

# HP Business Service Management

Pour les systèmes d'exploitation Windows® et Linux

Version du logiciel : 9.22

---

## Operations Manager i - Concepts

Date de publication du document : mai 2013

Date de lancement du logiciel : mai 2013



# Mentions légales

## Garantie

Les seules garanties applicables aux produits et services HP sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. HP ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

## Légende de restriction des droits

Logiciel confidentiel. Licence HP valide requise pour la détention, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

## Copyright

© Copyright 2008-2013 Hewlett-Packard Development Company, L.P.

## Marques

Adobe® est une marque d'Adobe Systems Incorporated.

Microsoft® et Windows® sont des marques déposées aux États-Unis de Microsoft Corporation.

UNIX® est une marque déposée de The Open Group.

## Mises à jour de la documentation

La page de titre du présent document contient les informations d'identifications suivantes :

- le numéro de version du logiciel ;
- la date de publication du document, qui change à chaque mise à jour de ce dernier ;
- la date de lancement du logiciel.

Pour obtenir les dernières mises à jour ou vérifier que vous disposez de l'édition la plus récente d'un document, accédez à la page :

**<http://h20230.www2.hp.com/selfsolve/manuals>**

Pour accéder à ce site, vous devez créer un compte HP Passport et vous connecter comme tel.

Pour obtenir un identifiant HP Passport, accédez à l'adresse :

**<http://h20229.www2.hp.com/passport-registration.html>**

Vous pouvez également cliquer sur le lien **New users - please register** dans la page de connexion de HP Passport.

En vous abonnant au service d'assistance du produit approprié, vous recevrez en outre les dernières mises à jour ou les nouvelles éditions. Pour plus d'informations, contactez votre revendeur HP.

## Assistance

Visitez le site d'assistance HP Software à l'adresse :

**<http://www.hp.com/go/hpsoftwaresupport>**

Ce site fournit les informations de contact et les détails sur les offres de produits, de services et d'assistance HP Software.

L'assistance en ligne de HP Software propose des fonctions de résolution autonome. Le site constitue un moyen efficace d'accéder aux outils interactifs d'assistance technique nécessaires à la gestion de votre activité. En tant que client privilégié de l'assistance, vous pouvez depuis ce site :

- rechercher des documents de connaissances présentant un réel intérêt ;
- soumettre et suivre des demandes d'assistance et des demandes d'améliorations ;
- télécharger des correctifs logiciels ;
- gérer des contrats d'assistance ;
- rechercher des contacts de l'assistance HP ;
- consulter les informations sur les services disponibles ;
- participer à des discussions avec d'autres utilisateurs d'un même logiciel ;
- rechercher des cours de formation sur les logiciels et vous y inscrire.

Pour accéder à la plupart des offres d'assistance, vous devez vous enregistrer en tant qu'utilisateur disposant d'un compte HP Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance. Pour obtenir un identifiant HP Passport, accédez à l'adresse suivante :

**<http://h20229.www2.hp.com/passport-registration.html>**

Les informations relatives aux niveaux d'accès sont détaillées à l'adresse suivante :

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

---

# Table des matières

Operations Manager i - Concepts .....	1
Table des matières .....	5
Bienvenue dans ce manuel .....	7
Structure du manuel .....	7
À qui s'adresse ce manuel ? .....	8
<b>Introduction à Gestion exploitations de BSM .....</b>	<b>9</b>
Structure des licences .....	9
Console de surveillance pour une solution BSM complète .....	10
Gestion consolidée des événements et des performances .....	13
Corrélation des événements .....	16
Corrélation des événements en fonction de la topologie .....	18
Résolution de problèmes structurée .....	19
Gestion du contenu avec les content packs .....	21
Architecture modulable avec plusieurs serveurs .....	24
Monitoring Automation .....	26
Engagement utilisateur .....	29
Interfaces d'intégration .....	30
Rôles utilisateur et responsabilités .....	30
<b>Flux de travail de l'opérateur .....</b>	<b>35</b>
L'environnement de l'opérateur .....	36
Autres rôles .....	39
<b>Flux de travail du développeur spécialisé dans la surveillance .....</b>	<b>41</b>
Analyse initiale .....	41
Définition de statuts d'indicateur .....	42
Autres tâches .....	42
Autres rôles .....	43
<b>Flux de travail de l'administrateur des systèmes informatiques .....</b>	<b>45</b>

Tâches d'installation et de configuration .....	45
Supervision de l'installation de BSM .....	46
Réglage des paramètres d'infrastructure .....	46
Configuration d'utilisateurs et de rôles utilisateur .....	46
Autres responsabilités .....	47
Tâches continues .....	47
Console de surveillance .....	47
Autres rôles .....	48
<b>Flux de travail de l'expert en applications .....</b>	<b>49</b>
Tâches d'installation et de configuration .....	49
Tâches continues .....	50
Autres rôles .....	50
<b>Synthèse .....</b>	<b>51</b>
<b>Index .....</b>	<b>53</b>

## Bienvenue dans ce manuel

Ce manuel est une introduction à Gestion exploitations de HP Business Service Management (BSM). Il décrit les principaux concepts sous-jacents de ce logiciel de gestion des performances et des événements complet, composant d'une solution HP Business Service Management (BSM).

**Remarque** : Gestion exploitations de BSM est disponible avec un système de déploiement HP Business Service Management (BSM) doté d'une licence Operations Manager *i* (OMi) active (voir « Introduction à Gestion exploitations de BSM », page 9).

Pour plus d'informations sur le déploiement de HP Business Service Management, voir le *manuel HP Business Service Management Deployment Guide*.

## Structure du manuel

Le présent manuel contient les informations suivantes :

- « Introduction à Gestion exploitations de BSM », page 9

Une présentation générale des fonctions les plus importantes vous aide à savoir comment utiliser Gestion exploitations de BSM pour améliorer les performances, la disponibilité et l'efficacité de votre environnement informatique.

- « Flux de travail de l'opérateur », page 35

Une description d'une journée type pour Dave, opérateur informatique, et de la manière dont il utilise la gestion des événements pour classer par ordre de priorité ses tâches quotidiennes.

- « Flux de travail du développeur spécialisé dans la surveillance », page 41

Une description du rôle de Mike, développeur informatique spécialisé dans la surveillance, et de la manière dont il surveille une nouvelle application.

- « Flux de travail de l'administrateur des systèmes informatiques », page 45

Une description du rôle de Matthew et de la manière dont il supervise l'environnement Gestion exploitations de BSM et configure l'infrastructure opérationnelle de manière à y intégrer l'ensemble des applications et serveurs de son domaine.

- « Flux de travail de l'expert en applications », page 49

Une description du rôle d'Alice et de la manière dont elle configure des solutions de surveillance génériques pour l'ensemble des applications et serveurs de son domaine.

## À qui s'adresse ce manuel ?

Vous devez lire ce manuel si vous êtes l'un des utilisateurs suivants :

- Un opérateur informatique
- Un spécialiste des bases de données, Exchange, SAP ou d'un autre domaine qui conçoit les scénarios de surveillance pour ces applications d'entreprise
- Un développeur informatique spécialisé dans la surveillance
- Un administrateur des systèmes informatiques
- Un administrateur des applications informatiques
- Si vous êtes un utilisateur de ce type, vous vous familiariserez avec BSM et les concepts fondamentaux de la surveillance et de la gestion d'entreprise.



# Introduction à Gestion exploitations de BSM

Ce chapitre présente brièvement Gestion exploitations de BSM et vous indique comment il peut vous aider à améliorer l'efficacité de vos services informatiques et de votre infrastructure.

Ce chapitre comprend une présentation architecturale et vous permet de comprendre de quelle manière Gestion exploitations de BSM s'intègre à une solution HP Business Service Management (BSM), à travers la description des concepts sous-jacents.

Contenu de ce chapitre :

- « Structure des licences », ci-dessous
- « Console de surveillance pour une solution BSM complète », page suivante
- « Gestion consolidée des événements et des performances », page 13
- « Résolution de problèmes structurée », page 19
- « Gestion du contenu avec les content packs », page 21
- « Architecture modulable avec plusieurs serveurs », page 24
- « Monitoring Automation », page 26
- « Interfaces d'intégration », page 30
- « Rôles utilisateur et responsabilités », page 30

## Structure des licences

Gestion exploitations de BSM est disponible avec un système de déploiement HP Business Service Management (BSM) doté d'une licence Operations Manager *i* (OMi) active.

Pour plus d'informations sur le déploiement, voir le manuel HP Business Service Management Deployment Guide.

La structure de licence Operations Manager *i* (OMi) est la suivante :

- **Fondations de Gestion des événements**

La licence Fondations de Gestion des événements est nécessaire pour la fonctionnalité Gestion exploitations de BSM.

- **Corrélation des événements en fonction de la topologie**

Ce type de licence est requis pour la fonction de corrélation des événements en fonction de la topologie (TBEC). Il repose sur la licence Fondations de Gestion des événements.

- **Connecteur cible**

Ce type de licence est nécessaire pour chaque système géré par une solution de gestion tierce (non HP), dans laquelle les événements sont consolidés dans Gestion exploitations de BSM. Il repose sur la licence Fondations de Gestion des événements.

- **Monitoring Automation**

Pour surveiller les applications directement à partir de HP Operations Manager i, une licence Monitoring Automation est requise. Monitoring Automation est disponible en deux versions :

- *Monitoring Automation for Servers*

La version Monitoring Automation for Servers a spécialement été mise au point pour les systèmes virtuels et physiques, et les applications centralisées du serveur. La licence Fondations de Gestion des événements d'OMi comprend la version Monitoring Automation for Servers.

- *HP Monitoring Automation for Composite Applications*

HP Monitoring Automation for Composite Applications offre davantage de fonctionnalités pour les centres de données dynamiques, comme la configuration de la surveillance en fonction de la topologie pour les applications hiérarchisées complexes, et adapte automatiquement la configuration de surveillance lors du réglage des paramètres ou des instances d'application, de manière à suivre l'évolution des besoins environnementaux ou professionnels. Vous pouvez acheter une licence HP Monitoring Automation for Composite Applications afin d'enrichir la gamme de solutions HP Operations Manager i.

- Gestion exploitations de BSM est le fondement de la gestion des événements pour une solution de surveillance BSM complète. En tant que trait d'union des exploitations, elle permet de regrouper toute la surveillance de l'infrastructure informatique dans une console centrale et d'associer les événements aux services informatiques qui dépendent de cette infrastructure. Les utilisateurs peuvent ainsi bénéficier d'un modèle commun structuré de gestion des événements qui applique les mêmes processus aussi bien à la gestion des services métier qu'à la gestion de l'infrastructure informatique.

## Console de surveillance pour une solution BSM complète

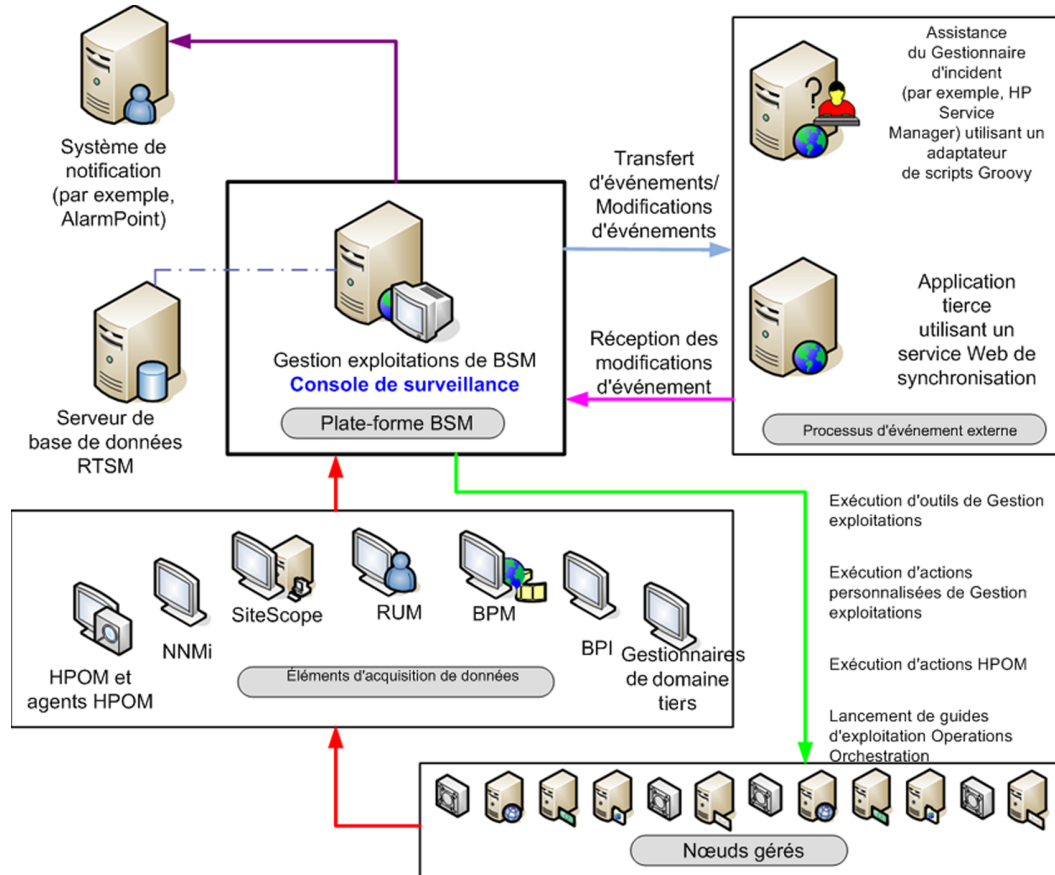
Gestion exploitations de BSM est le fondement de la gestion des événements pour une solution de surveillance BSM complète. En tant que trait d'union des exploitations, elle permet de regrouper toute la surveillance de l'infrastructure informatique dans une console centrale et d'associer les événements aux services informatiques qui dépendent de cette infrastructure. Les utilisateurs peuvent ainsi bénéficier d'un modèle commun structuré de gestion des événements qui applique les mêmes processus aussi bien à la gestion des services métier qu'à la gestion de l'infrastructure informatique.

Gestion exploitations de BSM relie la gestion de l'infrastructure à la gestion des applications et des services métier. Elle permet d'associer des événements des composants HP Business Service Management, tels que Business Process Monitor (BPM), Real User Monitor (RUM) et Gestion des contrats de service (SLM), aux événements des composants de gestion des exploitations de la solution BSM, tels que HP Operations Manager (HPOM) et HP Network Node Manager i (NNMi). Cette liaison permet de suivre l'ensemble des événements survenant dans votre environnement surveillé.

La [Figure 1](#), [page suivante](#) illustre un exemple de déploiement type dans lequel Gestion exploitations de BSM agit en tant que console de surveillance d'une solution BSM. Gestion exploitations de BSM permet la surveillance et l'intégration automatisées de plusieurs applications

externes, et s'exécute au sein de la plate-forme BSM à l'aide de la base de données RTSM (Run-Time Service Model) commune.

Figure 1 - Console de surveillance dans une solution BSM



Le partage du référentiel RTSM avec d'autres applications BSM confère un accès immédiat et à tout moment aux données les plus récentes stockées dans le référentiel RTSM. Les administrateurs des systèmes informatiques n'ont, par exemple, plus à réaliser des tâches supplémentaires afin de s'assurer de la pertinence des données de topologie dans le référentiel RTSM.

L'ensemble des ordres de gestion des événements et des performances émanant des serveurs, réseaux, applications, systèmes de stockage et autres silos informatiques de votre infrastructure sont regroupés dans un unique flux d'événements, sur une console d'événements centrale avancée. Cette console signale les alertes de surveillance à l'équipe d'opérateurs appropriée.

Vous pouvez ainsi rapidement identifier, surveiller, consigner et résoudre les problèmes de votre environnement informatique distribué. Ces fonctionnalités vous permettent d'améliorer les performances et la disponibilité de l'infrastructure et des services de votre environnement surveillé pour une plus grande efficacité et une excellente productivité au sein de votre activité. Gestion exploitations de BSM vous aide à identifier et à résoudre les problèmes associés aux événements avant qu'ils n'affectent la qualité de votre service métier. Il offre aux opérateurs les outils dont ils

ont besoin pour résoudre les problèmes sans requérir l'intervention d'un spécialiste du domaine, qui peut ainsi se concentrer sur les activités stratégiques de votre entreprise.

#### **Acquisition de données de plusieurs sources**

Vous pouvez constater dans la [Figure 1](#), [page précédente](#) que les événements, quelle que soit leur origine, sont traités et gérés de manière uniforme.

Exemples de sources d'événement :

- Composants de BSM :  
Les alertes BSM (alertes de statut d'élément de configuration, alertes de Convention de service et alertes en fonction des événements) peuvent également générer des événements dans Gestion exploitations de BSM. Par exemple, les opérateurs peuvent, à partir de composants d'Expérience utilisateur, collecter, afficher, corrélérer et gérer des événements générés par des alertes en fonction des événements. À noter que les alertes transférées à partir d'un composant d'Expérience utilisateur comme BPM ne sont pas rétrosynchronisées.
- Composants de BSM :
  - HP Operations Manager pour UNIX (HPOM pour UNIX) avec un serveur Operations Manager exécuté sur une plate-forme HP-UX, SPARC Solaris ou RHEL x64
  - HP Operations Manager pour Windows (HPOM pour Windows)
  - HP Network Node Manager i (NNMi)
  - Business Process Monitor (BPM)
  - Real User Monitor (RUM)
  - HP SiteScope
  - HP Systems Insight Manager

Les alertes BSM (alertes de statut d'élément de configuration, alertes de Convention de service et alertes en fonction des événements) peuvent également générer des événements dans Gestion exploitations de BSM. Par exemple, les opérateurs peuvent, à partir de composants d'Expérience utilisateur, collecter, afficher, corrélérer et gérer des événements générés par des alertes en fonction des événements. À noter que les alertes transférées à partir d'un composant d'Expérience utilisateur comme BPM ne sont pas rétrosynchronisées.

- Logiciels de gestion tiers, généralement utilisés pour surveiller des environnements spécifiques ou des paramètres spéciaux dont la surveillance n'est pas assurée par les composants d'autres solutions, comme Microsoft Systems Center Operations Manager ou Oracle Enterprise Manager. Les connecteurs permettant l'intégration de logiciels de gestion tiers, comme Microsoft SCOM, Nagios et IBM Tivoli, dans HP BSM sont également disponibles sur le portail HP Live Network (<https://hpln.hp.com>).

## Gestion consolidée des événements et des performances

La console de surveillance est le pôle de consolidation d'événements de tout type provenant de sources multiples sur une console centralisée. Les perspectives fournissent aux opérateurs différents niveaux d'informations concernant les événements dont ils sont responsables. Par exemple, la gestion globale des événements est réalisée dans la perspective Événement, tandis que la perspective Intégrité donne des informations supplémentaires sur les événements en rapport avec l'intégrité du service. Ces perspectives sont regroupées dans le navigateur d'événements.

### Informations sur l'événement

Les événements signalent des faits importants se produisant dans l'environnement informatique géré. Ils sont générés par les gestionnaires de domaine, transférés vers Gestion exploitations, puis

mappés aux éléments de configuration (CI) associés dans le référentiel RTSM. Ces événements sont affectés à des opérateurs à des fins de résolution. Dans le navigateur d'événements, les opérateurs bénéficient d'un aperçu complet de l'ensemble des événements actifs nécessitant une intervention. Ils peuvent se rendre compte de la gravité des événements, en voir le type et la catégorie, la source, ainsi que l'heure et l'emplacement, et visualiser l'élément de configuration concerné.

Les événements parcourent un cycle de vie, qui permet l'affichage et la surveillance rapides de leur statut. Le flux de travail d'un opérateur repose sur le cycle de vie d'un événement. L'état du cycle de vie d'un événement représente la progression de l'analyse du problème à l'origine de l'événement. Un opérateur affecté à un événement lance une analyse et tente de trouver une solution au problème sous-jacent de l'événement. Des experts peuvent ensuite examiner la solution suggérée, s'assurer qu'elle résout bien le problème à l'origine de l'événement et clôturer l'événement, ce qui met un terme à son cycle de vie.

Les opérateurs peuvent configurer le navigateur d'événements conformément aux exigences de leur flux de travail type. Le contenu du navigateur d'événements est filtré selon la vue ou l'élément de configuration sélectionné. Les opérateurs peuvent configurer de nouveaux filtres ou modifier des filtres existants, selon leurs besoins, afin d'afficher d'autres informations. Le filtrage du navigateur d'événements permet aux opérateurs de se concentrer sur les informations les plus utiles pour identifier les événements prioritaires, par exemple, et déterminer les événements requérant une intervention immédiate afin de limiter leur impact sur les services métier. Vous pouvez également configurer des utilisateurs et des groupes de sorte qu'ils voient uniquement les événements filtrés par vue associés à cet utilisateur ou à ce groupe,

Vous pouvez configurer des collecteurs de données HP ou tiers de manière à transférer les événements vers Gestion exploitations de BSM. Les événements sont synchronisés entre les serveurs. Par exemple, Gestion exploitations de BSM et HP Operations Manager (HPOM) synchronisent l'état des événements et des messages. Si un opérateur Gestion exploitations de BSM clôture un événement, une notification est automatiquement envoyée à HPOM. De la même manière, HPOM informe Gestion exploitations de BSM de l'acquittement des messages et Gestion exploitations de BSM met automatiquement à jour l'état du cycle de vie des événements correspondants en le définissant sur Clôturé.

Les opérateurs peuvent indiquer des informations supplémentaires sur les événements. Ils peuvent, par exemple, ajouter des annotations à l'événement afin de faciliter la résolution des problèmes ou de préciser les mesures déjà prises.

Les événements clôturés sont automatiquement déplacés vers le navigateur des événements clôturés. Les opérateurs peuvent accéder à cette liste d'événements clôturés et utiliser ces événements en guise de référence pour la résolution de problèmes similaires.

La console de surveillance peut transférer les événements nécessitant l'attention de spécialistes du domaine aux opérateurs appropriés. Par exemple, l'administrateur des systèmes informatiques peut configurer le système de manière à ce qu'il achemine les notifications vers les opérateurs et les escalade vers les opérateurs d'assistance appropriés qui peuvent se concentrer sur la gestion des événements escaladés et la résolution des problèmes sous-jacents.

### Tableaux de bord des événements

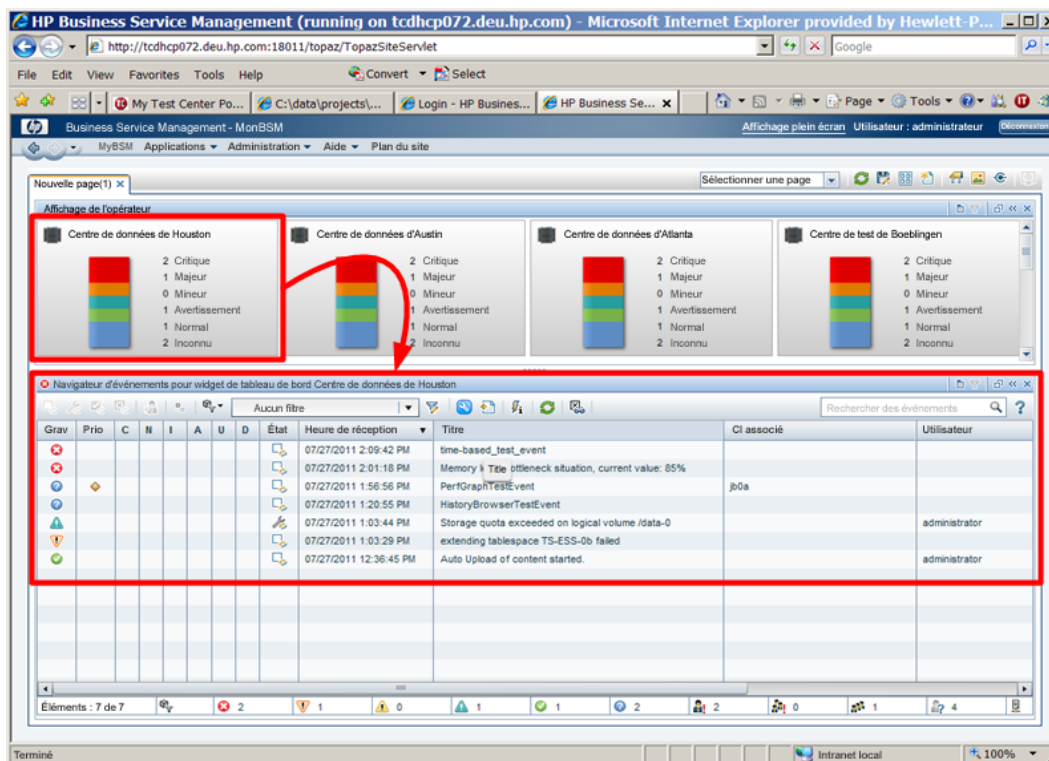
Les tableaux de bord des événements (voir [Figure 2, page suivante](#)) vous offrent un aperçu des événements de votre environnement surveillé. Ils vous permettent d'évaluer rapidement l'intégrité de l'environnement et d'identifier les zones requérant votre attention.

Les tableaux de bord des événements vous aident à :

- visualiser en un clin d'œil votre environnement surveillé
- repérer un point de départ pour les opérations de gestion quotidiennes
- appliquer rapidement des filtres d'événement au navigateur d'événements
- garder un œil sur l'environnement surveillé tout en travaillant sur un événement

Les tableaux de bord d'événements permettent d'afficher des informations de statut à l'aide de widgets utilisés comme unités élémentaires (les widgets STACK et PIE, par exemple). Chaque widget fait référence à un filtre d'événement, à une vue, ou aux deux, et ne présente que le statut des événements correspondant aux critères du filtre et associés aux éléments de configuration inclus dans la vue référencée, pour une personnalisation aisée.

**Figure 2 - Tableau de bord des événements**



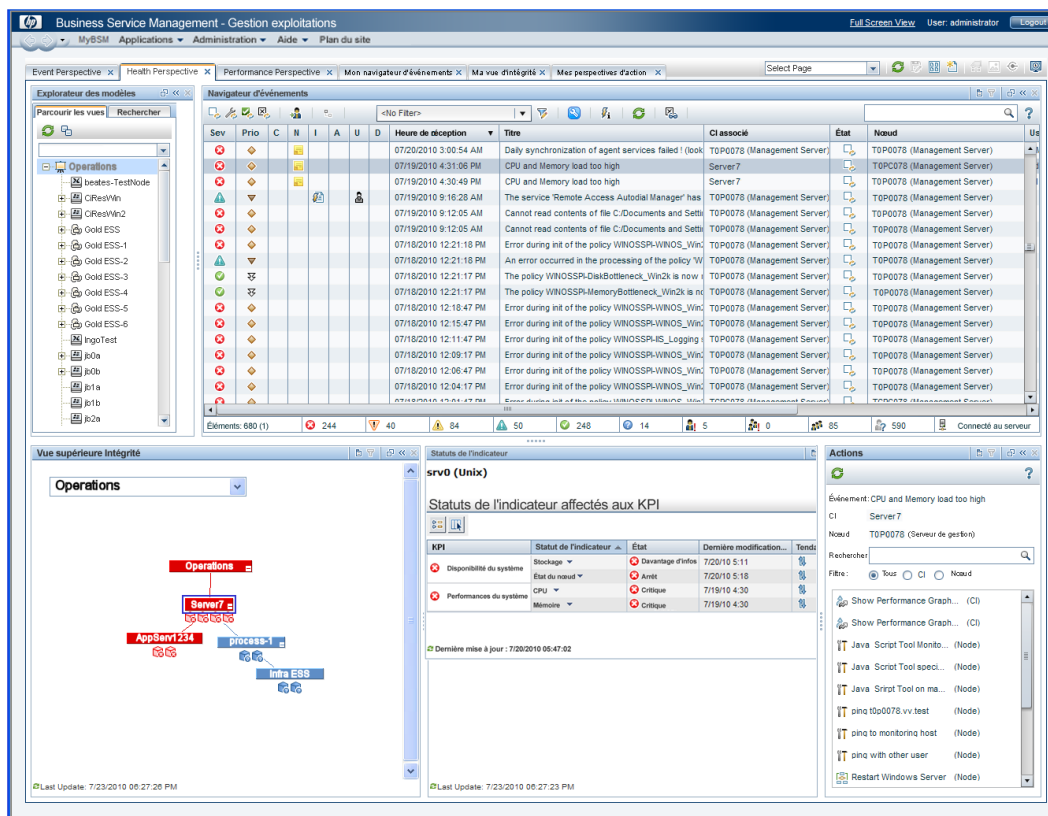
### Informations sur l'intégrité

Grâce aux données d'événement, vous pouvez voir, dans le navigateur d'événements, l'élément de configuration associé affecté par l'événement. En outre, les données sur l'intégrité BSM, telles que les indicateurs type événement (ITE), les statuts d'indicateur (SI) et les indicateurs de performance métiers (KPI), sont utilisées pour évaluer l'intégrité des éléments de configuration associés lors des événements.

Pour tout périphérique, comme un serveur, la gravité des problèmes directement associés au serveur est collectée et associée aux informations concernant les périphériques en lien avec le serveur. Les données combinées sont ensuite transmises à des règles de calcul qui évaluent et définissent les indicateurs de performance métiers reflétant globalement l'intégrité de l'objet.

La [Figure 3, page suivante](#) illustre une page Perspective Intégrité type. La vue supérieure Intégrité présente les relations existantes entre les objets associés à l'événement, de manière hiérarchique.

**Figure 3 - Perspective Intégrité avec les volets Vue supérieure Intégrité et Statuts de l'indicateur**



Vous pouvez voir le statut de l'intégrité d'un objet et les règles métier et indicateurs de performance métiers utilisés, et déterminer la manière dont le statut de l'intégrité de l'objet sélectionné affecte l'intégrité des objets associés. Par exemple, un utilisateur peut accéder à cette page pour vérifier l'intégrité des éléments de configuration voisins. Ces informations permettent à l'utilisateur de repérer les événements sur lesquels il doit se concentrer et de les classer par ordre de priorité de gestion afin d'optimiser la disponibilité des services métier et de limiter l'impact qu'ils pourraient avoir sur eux. Les utilisateurs peuvent également sélectionner des vues afin de n'afficher que les événements et éléments de configuration dont ils sont responsables.

Ils peuvent sélectionner le composant de leur choix et afficher l'état des statuts d'indicateur et indicateurs de performance métiers associés. Par exemple, un opérateur peut souhaiter afficher le statut de l'indicateur de performance métier Disponibilité d'un serveur particulier et l'état des statuts d'indicateur associés.

### Corrélation des événements

Dans un vaste environnement, l'un des défis les plus importants réside dans la gestion du grand nombre d'événements émanant de diverses sources. Dans ce foisonnement de données, l'objectif est d'identifier les événements ayant un fort impact sur les services métier. Par conséquent, bien qu'il soit essentiel de limiter le nombre d'événements apparaissant dans le navigateur d'événements, il est d'autant plus important de mettre en évidence les événements qui, s'ils ne sont pas gérés correctement, pourraient se solder par la violation des Conventions de service (SLA) et générer des incidents au sein de votre système d'assistance.



La corrélation des événements joue un rôle très important dans l'association de la gestion des services métier et de la gestion de l'infrastructure informatique. Vous pouvez ainsi remonter à la défaillance à l'origine de l'interruption d'un service de l'infrastructure informatique dont dépend le service.

Gestion exploitations de BSM corrèle automatiquement les événements de l'une des manières suivantes :

- Suppression des événements dupliqués
- Clôture automatique des événements associés
- Corrélation des événements en fonction du flux
- Corrélation des événements en fonction de la topologie

#### Suppression des événements dupliqués

Un nouvel événement peut être une copie d'un événement existant. Par exemple, en raison de problèmes d'instabilité du réseau, le même événement est envoyé deux fois par le gestionnaire de domaine source suite à la réception tardive de l'acquittement de la première instance de l'événement. Au fur et à mesure que les nouveaux événements sont reçus, ils sont vérifiés par rapport aux événements existants. Si des doublons sont détectés, de nouvelles informations, telles qu'une altération de la gravité, sont utilisées pour la mise à jour de l'événement existant et le nouvel événement est ignoré. Si la suppression des événements dupliqués est activée, les nouveaux événements qui sont des duplications d'événements existants ne sont pas retenus, et l'événement original est mis à jour.

L'avantage de la corrélation d'événements à l'aide de la suppression des événements dupliqués est la réduction du nombre d'événements affichés sur la console, sans perte d'informations importantes.

La suppression d'événements dupliqués peut générer des corrélations supplémentaires de l'événement original (en tant que cause ou en tant que symptôme). Lorsqu'une duplication est identifiée, la date et heure de l'événement original sont mises à jour à la date et heure de réception de la duplication. L'événement est alors corrélé de nouveau et peut donc être associé à d'autres événements qui n'étaient pas disponibles pour la corrélation au moment de la réception de l'événement original.

#### Clôture automatique des événements associés

Un nouvel événement peut automatiquement clôturer un ou plusieurs événements existants. Lorsqu'un nouvel événement arrive, une recherche est effectuée afin de constater la présence éventuelle d'événements associés. Certaines informations spécifiques contenues dans le nouvel événement sont utilisées pour mettre en correspondance le nouvel événement avec des événements existants. Le nouvel événement clôturé l'événement existant. Ce type de corrélation d'événements est similaire à la corrélation de messages correcte/incorrecte proposée par HP Operations Manager.

Par exemple, un événement existant peut être la notification d'un problème ou d'une condition anormale (événement néfaste) pour un périphérique particulier. Cet événement néfaste pourrait être la *faiblesse des performances de la requête SQL*. Imaginez qu'un nouvel événement corresponde à cet événement associé existant qui signale que la condition anormale n'existe plus (événement positif). Cet événement positif pourrait être la *puissance des performances de la requête SQL*. Ce nouvel événement (positif) clôturé l'événement associé (néfaste) existant.

Vous pouvez suivre les événements associés automatiquement clôturés dans l'historique des événements.

#### Corrélation des événements en fonction du flux

La corrélation des événements en fonction du flux (SBEC, Stream-based event correlation) utilise des règles et des filtres permettant d'identifier les événements ou associations d'événements se produisant fréquemment et simplifie la gestion de ces événements en identifiant automatiquement les événements à conserver, à supprimer ou nécessitant la génération d'un nouvel événement et sa présentation aux opérateurs.

Les types de règle de corrélation des événements en fonction du flux suivants peuvent être configurés :

- **Règles de répétition** : une répétition fréquente du même événement peut indiquer un problème nécessitant une attention particulière.
- **Règles de combinaison** : une association de différents événements se produisant simultanément ou dans un ordre particulier indique un problème et nécessite un traitement spécial.
- **Règles de périodicité manquante** : un événement se produisant de manière régulière est manquant, par exemple, un événement de pulsation régulier n'arrive pas au moment prévu.

#### Corrélation des événements en fonction de la topologie

Le processus de gestion des événements est simplifié par la consolidation, sur une console centrale, des événements émanant de l'ensemble des différentes sources, mais également par le classement des événements à l'aide de la corrélation des événements en fonction de la topologie (TBEC). Les dépendances entre événements sont analysées afin de déterminer si certains événements peuvent être expliqués par d'autres. Par exemple, supposons que vous disposiez d'un serveur de base de données (serveur de BD) exécuté sur un serveur (Serveur1). Si le CPU de Serveur1 est en permanence surchargé, l'événement obtenu, *Violation de la Convention de service pour le serveur de BD*, peut être expliqué par l'événement déclencheur *Serveur1 : CPU en permanence surchargé (100 % pendant plus de 10 minutes)*.

L'essentiel est d'identifier les événements déclencheurs sous-jacents responsables des autres événements de symptôme, de manière à pouvoir résoudre en priorité ces événements déclencheurs selon leur impact sur votre activité.

Si deux événements se produisent simultanément (dans un délai configurable), les règles de corrélation de l'événement en fonction de la topologie identifient un événement comme étant la cause et l'autre événement comme étant le symptôme. La gestion des événements en fonction d'une règle vous permet de gérer un grand nombre d'événements de symptôme (associés) semblables sur un vaste réseau.

Lorsqu'une association d'événements de cause et de symptôme se produit dans l'environnement surveillé, les événements corrélés sont signalés dans le navigateur d'événements. Vous pouvez configurer le navigateur d'événements de manière à afficher l'événement déclencheur et un aperçu distinct de l'ensemble des événements de symptôme. Vous pourrez ainsi explorer le processus de corrélation et parcourir la hiérarchie des événements corrélés.

Les événements peuvent également être corrélés dans plusieurs domaines techniques, tels que des bases de données, du matériel, des réseaux et des applications Web. Ce champ d'action complet vous permet de corréler des événements qui, à première vue, ne semblent avoir aucun

rapport. La fonctionnalité interdomaine accroît également la productivité en réduisant le nombre de tâches identiques effectuées par plusieurs opérateurs responsables de la surveillance de différents domaines techniques. Par exemple, afin d'éviter que les opérateurs des différents domaines techniques analysent tous séparément différents événements symptômes d'un unique événement déclencheur, vous pouvez corréler des événements en rapport avec des problèmes de base de données, de réseau et de stockage.

La corrélation des événements en fonction de la topologie offre un certain nombre d'avantages associés à la résolution d'événements complexes :

- Elle réduit le nombre d'événements affichés sur la console, sans ignorer ni perdre les données importantes qui permettent aux utilisateurs d'explorer la hiérarchie des événements associés.
- Elle prend en charge la corrélation d'événements de plusieurs domaines afin de simplifier l'analyse de la cause fondamentale des événements générateurs d'événements de symptôme.
- Les modifications apportées aux données topologiques ne nécessitent aucune modification des règles de corrélation.

### Suppression d'une tempête d'événements

Une tempête d'événements est un phénomène déclenché lorsqu'un problème survient sur un système géré et entraîne la génération d'un nombre anormalement élevé d'événements sur une courte période. Il est très probable que la cause fondamentale soit déjà connue et puisse être résolue. Cependant, des événements associés peuvent également être générés. Ces événements n'apportent aucune information utile, mais peuvent générer des charges considérablement plus importantes sur les serveurs exécutant Gestion exploitations. Afin d'éviter une telle situation, Gestion exploitations peut être configuré de manière à rechercher les tempêtes d'événements provenant de systèmes gérés et à ignorer tous les événements qui en découlent jusqu'à ce que la tempête d'événements d'un système particulier soit terminée.

Une tempête d'événements est détectée lorsque le nombre d'événements reçus sur une période de détection, suite à un problème rencontré par un système, dépasse le seuil configuré requis pour activer une condition de tempête d'événements.

Lorsqu'une tempête d'événements est détectée sur un système, les événements provenant de ce système sont ignorés jusqu'à ce que le nombre d'événements entrants revienne en dessous du seuil de fin de tempête d'événements. Vous pouvez configurer des règles d'exception pour sélectionner des événements provenant d'un système subissant une tempête d'événements et correspondant à un filtre. Vous pouvez ensuite les afficher dans le navigateur d'événements ou les clôturer (disponibles dans le navigateur d'événements sous Événements clôturés). L'événement de fin de tempête d'événements clôture automatiquement l'événement de début de tempête d'événements associé.

## Résolution de problèmes structurée

La console de surveillance centralisée rationalise l'ensemble du processus de gestion des événements. Avec des informations consolidées, centralisées, vous pouvez créer des processus cohérents, réutilisables et optimisés pour la réponse aux événements.

Vous pouvez traiter la plupart des événements se produisant dans votre environnement de manière très structurée. Pour gérer plus efficacement les événements en toute simplicité, vous pouvez avoir recours aux moyens suivants :

- **Outils**

Vous pouvez créer des outils pour aider les utilisateurs à réaliser les tâches courantes sur les éléments de configuration. Lorsque vous créez un outil, il est associé à un type d'élément de configuration et vous pouvez l'exécuter à partir de la console centralisée. Par exemple, vous pouvez exécuter un outil de commande pour vérifier le statut d'une instance de base de données Oracle. Cet outil est affecté au type d'élément de configuration Base de données Oracle. Si vous gérez plusieurs versions de bases de données Oracle, pour lesquelles l'outil nécessite différents paramètres et options afin de vérifier le statut des processus de la base de données Oracle, vous pouvez créer des copies de l'outil le plus approprié et les personnaliser selon chaque version de base de données Oracle à l'aide de la fonction Dupliquer. Chaque outil est ensuite associé à une version spécifique de base de données Oracle.

- **Actions personnalisées**

Pour automatiser la gestion de vos événements, vous pouvez créer des actions à exécuter sur des événements afin de faciliter la résolution des problèmes et d'améliorer l'efficacité et la productivité des opérateurs. Les administrateurs peuvent définir diverses actions personnalisées que l'opérateur pourra utiliser lors de la résolution de certains types d'événement. Des actions contextuelles et des outils propres à un contexte peuvent également être définis dans des circonstances particulières. Par exemple, vous pouvez créer un ensemble d'outils de diagnostic de base de données à des fins de résolution de problèmes de base de données.

Pour plus d'informations sur la définition et la création de scripts, y compris des exemples de script fournis avec le produit, voir le manuel *Operations Manager i Extensibility Guide*.

- **Actions HPOM**

Les événements reçus dans le navigateur d'événements à partir de HPOM peuvent contenir des actions associées à des événements, configurées dans HPOM. Si des actions associées à des événements existent, vous pouvez les exécuter à partir de la console Gestion exploitations de BSM. Les actions de HPOM peuvent être lancées par l'opérateur ou automatiquement exécutées lorsqu'un événement se produit.

Pour un aperçu complet des actions disponibles et pour plus d'informations sur leur exécution, voir l'aide en ligne Gestion exploitations de BSM.

- **Guides d'exploitation HP Operations Orchestration**

Si vous utilisez déjà HP Operations Orchestration (OO) pour automatiser les tâches des opérateurs pour l'analyse ou la résolution de problèmes, les guides d'exploitation OO peuvent être mappés à des types d'élément de configuration dans BSM. Vous pouvez lancer les guides d'exploitation OO dans un contexte d'événement à partir de la console Gestion exploitations de BSM.

Outre le lancement manuel des guides d'exploitation, il est également possible de configurer des règles afin d'exécuter automatiquement un guide d'exploitation ou une série de guides d'exploitation dans le contexte d'un événement.

Pour plus d'informations sur la manière d'exécuter des guides d'exploitation OO, voir l'aide en ligne Gestion exploitations de BSM.

- **Graphiques**

Les graphiques offrent des données supplémentaires permettant la visualisation et l'analyse des problèmes de performance et des tendances affectant l'élément de configuration touché par un événement ou l'un des éléments de configuration voisins. Les opérateurs peuvent même créer leurs propres graphiques.

Des processus de gestion des événements structurés sont déployés de manière à :

- Affecter automatiquement les événements entrants à des utilisateurs de groupes d'utilisateurs spécifiques. L'affectation automatique des événements accroît de manière significative l'efficacité de la gestion des événements et réduit le délai avant réponse à un événement. L'administrateur des systèmes informatiques peut configurer Gestion exploitations de BSM pour automatiquement affecter les événements entrants aux groupes d'opérateurs disponibles responsables de la résolution de ces événements, et ce, immédiatement.
- Lancer des actions sur les événements répondant à un ensemble défini de critères après un certain délai. Les règles d'automatisation des événements en fonction du temps comprennent trois principaux éléments :
  - Le filtre définissant les événements auxquels les règles d'automatisation des événements en fonction du temps doivent être appliquées.
  - La période définissant la durée d'un événement doit, en permanence, correspondre au filtre de la règle afin que les actions de la règle puissent être exécutées sur cet événement.
  - La liste d'actions à exécuter sur des événements correspondants. Les actions suivantes sont disponibles : réexécution d'actions automatiques sur les événements, modification des attributs d'événement, transfert d'événements aux serveurs externes, affectation d'événements aux utilisateurs et groupes, exécution de scripts et exécution de guides d'exploitation.
- Afficher et surveiller le statut des événements à l'aide de concepts de gestion de cycle de vie. Vous pouvez également voir qui est actuellement chargé de la résolution de l'événement, ainsi que l'ensemble des autres utilisateurs ayant déjà participé à la recherche d'une solution.
- Documenter la gestion et la résolution d'un événement. Vous pouvez annoter l'événement afin de décrire le processus de résolution du problème ou faire appel aux spécialistes du domaine en ajoutant des conseils aux événements, qui en facilitent la compréhension et précisent le problème sous-jacent.

## Gestion du contenu avec les content packs

Le contenu consiste en des informations que BSM utilise pour décrire et enrichir les objets ou les éléments de configuration surveillés dans votre environnement informatique. Ces objets peuvent être du matériel réseau, des systèmes d'exploitation, des applications, des services, des utilisateurs, etc. Le contenu est utilisé pour enrichir les données des éléments de configuration.

Les données des éléments de configuration propres à Gestion exploitations de BSM sont gérées dans des content packs. Vous pouvez observer du contenu sous la forme d'un ensemble de plusieurs content packs. Les content packs fournissent des règles et des outils préconfigurés (notamment, des guides d'exploitation), ainsi que d'autres éléments pour des applications et systèmes gérés spécifiques. Un content pack peut par conséquent contenir un aperçu de tout ou partie de votre contenu. Vous pouvez également utiliser des content packs pour échanger des données personnalisées entre différentes instances de BSM (entre des environnements de test et

de production, par exemple). Vous pouvez aussi partager du contenu entre différents content packs.

Les content packs contiennent généralement les éléments suivants :

- Règles de corrélation
- Règles de mappage pour la synchronisation de topologie
- Règles de mappage et définitions de statuts d'indicateur (SI)
- Règles de mappage et définitions d'indicateurs Type Événement (ITE)
- Règles et affectations d'indicateurs de performance métiers (KPI)
- Menus
- Mappages de vues
- Graphiques et affectations de graphique
- Outils
- Définitions de l'interface de traitement de l'événement (EPI) et scripts d'actions personnalisées
- Règles de transfert d'événements

Le contenu qui n'est pas propre à Gestion exploitations de BSM (comme des types d'élément de configuration supplémentaires) se trouve dans d'autres packs gérés séparément à l'aide d'outils spéciaux.

Deux types de content pack sont disponibles :

- Des content packs prêts à l'emploi pour compléter les données collectées par, par exemple, NNMi ou les Smart Plug-ins (SPI) HP Operations Manager.
- Des content packs personnalisés que vous développez afin de répondre aux exigences de vos propres applications et politiques de surveillance.

Généralement, le développeur spécialisé dans la surveillance crée des content packs personnalisés et l'administrateur des systèmes informatiques les déploie.

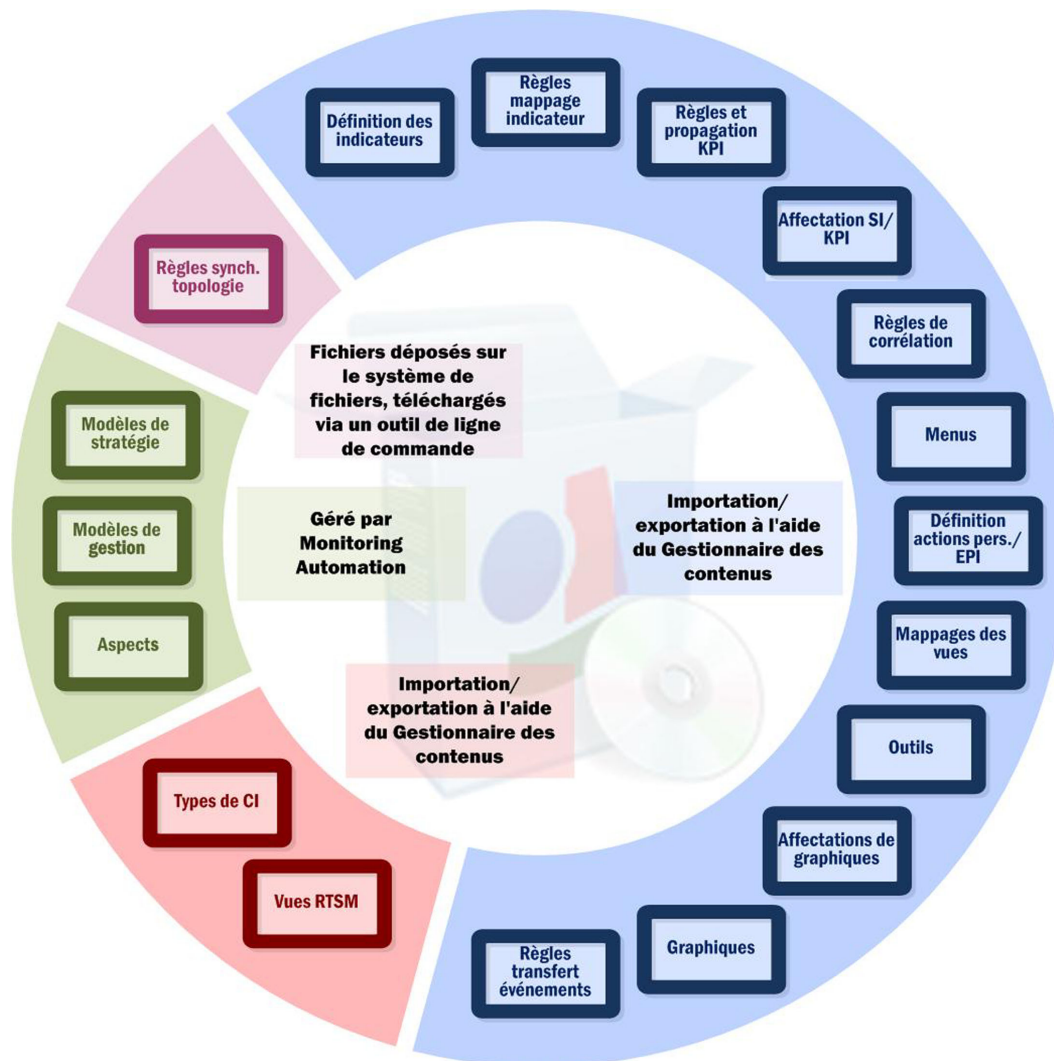
### Content packs prêts à l'emploi

Si l'administrateur système déploie les content packs HP Operations Manager, ces derniers fournissent les données de configuration nécessaires à la réception et au traitement des événements transférés depuis HP Operations Manager.

Si l'administrateur système installe le content pack dédié à la base de données Oracle, par exemple, ce dernier fournit à Gestion exploitations de BSM des informations sur la forme et le contenu des événements envoyés par le Smart Plug-in HP Operations Manager à destination des bases de données Oracle. Le content pack donne les règles, outils et définitions de graphique nécessaires à l'utilisation des données d'événement en vue d'évaluer l'intégrité des éléments de configuration associés au serveur Oracle ou de corréler des événements associés au serveur Oracle. Autre exemple, le content pack Infrastructure fournit les données de configuration, notamment les outils, nécessaires à l'intégration d'événements à partir de NNMi.

La [Figure 4, page suivante](#) donne un aperçu du contenu pouvant être inclus dans un ensemble de content packs.

Figure 4- Contenu pouvant être inclus dans un ensemble de content packs



### Outils de gestion du contenu

BSM dispose d'un ensemble d'outils facilitant la gestion du contenu. Vous pouvez également utiliser le Gestionnaire de contenu pour échanger du contenu entre les différents systèmes. Par exemple, vous pouvez préparer du contenu dans un environnement de test, puis transférer le contenu testé vers un environnement de production si les tests confirment que le contenu fonctionne comme prévu.

Les outils d'exportation et d'importation vous permettent d'échanger du contenu entre les différents systèmes de manière à ce que vous puissiez conserver des instantanés ou des images de sauvegarde du contenu développé et vous assurer que les différentes instances restent synchronisées et à jour.

## Architecture modulable avec plusieurs serveurs

Gestion exploitations de BSM vous permet de gérer des systèmes très étendus à partir d'un emplacement central. Dans un déploiement distribué, vous pouvez configurer votre environnement de manière hiérarchique. Vous pouvez ensuite étendre la responsabilité de la gestion sur plusieurs niveaux de gestion en fonction de critères, tels que l'expérience de l'opérateur, sa situation géographique, l'heure. Grâce à cette gestion souple, les opérateurs peuvent se concentrer sur les tâches correspondant à leurs compétences, tout en bénéficiant de l'assistance technique 24 heures sur 24 disponible automatiquement et à la demande.

Cette architecture modulable permet d'associer une ou plusieurs instances Gestion exploitations de BSM à une solution de gestion unique puissante spécialement paramétrée de manière à satisfaire aux exigences de votre structure organisationnelle. Par conséquent, vous pouvez configurer des serveurs de manière à transférer des événements vers d'autres serveurs de votre environnement.

Dans un environnement distribué, les serveurs hébergeant Gestion exploitations de BSM peuvent être configurés de manière à fonctionner avec d'autres systèmes, tels que des serveurs, mais également avec différents serveurs de gestion HPOM pour Windows et HPOM pour UNIX, d'autres serveurs BSM et même avec des gestionnaires de domaine tiers.

Dans un environnement distribué et hiérarchique de ce type, vous pouvez configurer Gestion exploitations de BSM de manière à :

- Être le pivot central des événements ou le gestionnaire des gestionnaire de l'ensemble de l'environnement, au sommet de la hiérarchie.
- Utiliser d'autres produits HP, tels que NNMI et HP SiteScope.
- Travailler avec des gestionnaires de domaine tiers, tels que Microsoft Systems Center Operations Manager.

Vous pouvez configurer les serveurs hébergeant Gestion exploitations de BSM de manière à :

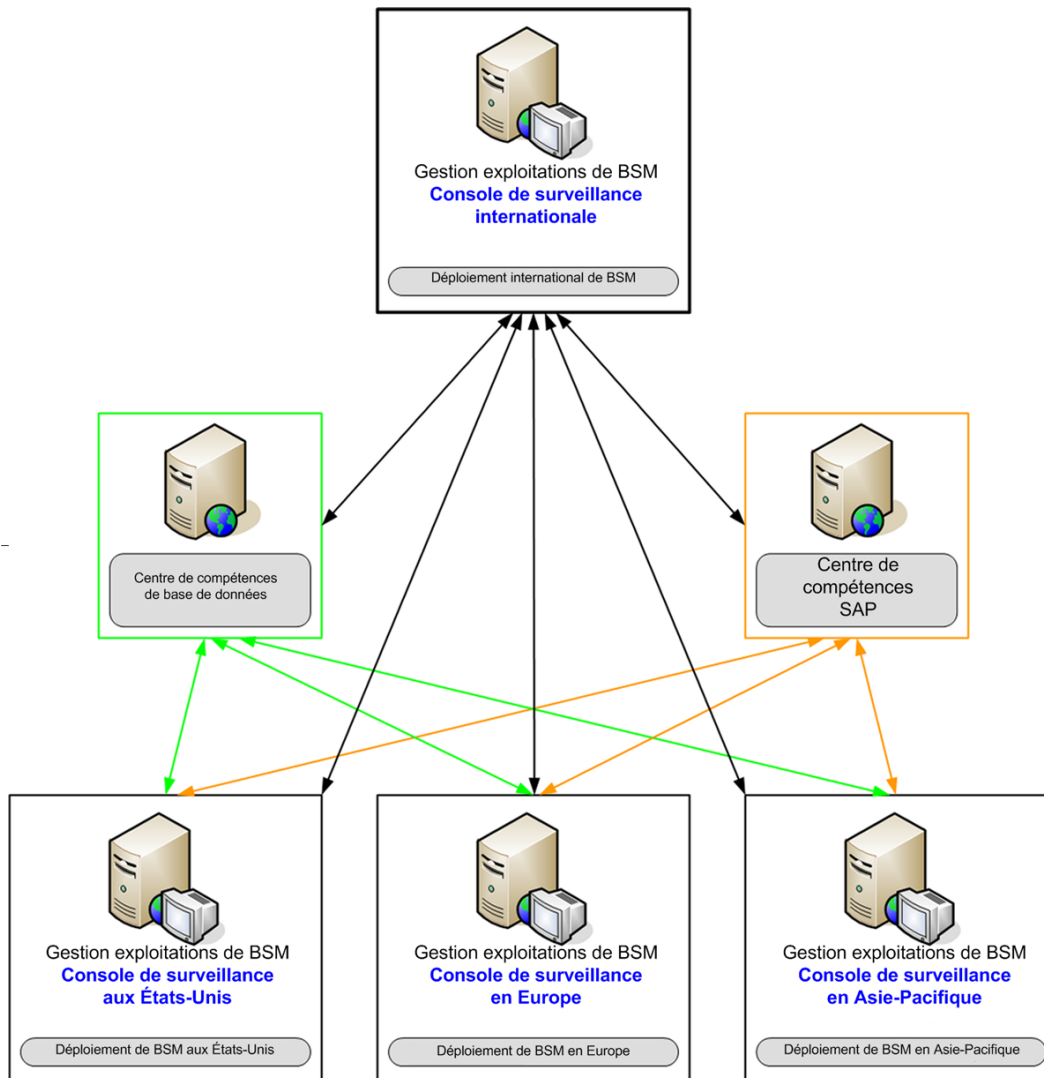
- Transférer des événements vers d'autres serveurs hébergeant Gestion exploitations de BSM et maintenir la synchronisation de ces événements sur les différents serveurs.
- Recevoir des messages transférés à partir de différents serveurs de gestion HPOM pour Windows et HPOM pour UNIX et maintenir la synchronisation de ces messages sur les différents serveurs hébergeant Gestion exploitations de BSM et les serveurs de gestion HPOM.
- Recevoir des événements transférés à partir d'un serveur BSM recevant des alertes de composants BSM, tels que HP Business Process Monitor (BPM).

### Déploiement Manager-of-Managers (MoM)

La [Figure 5](#), [page suivante](#) donne un exemple d'un environnement distribué hiérarchique avec un serveur central hébergeant Gestion exploitations de BSM et gérant d'autres serveurs régionaux hébergeant eux-mêmes Gestion exploitations de BSM selon une méthode souple de gestion sur serveur.



**Figure 5 - Déploiement de type Manager-of-Managers (MoM)**



Dans cet exemple, le déploiement de serveurs régionaux BSM en Europe, BSM aux États-Unis et BSM en Asie-Pacifique gère différentes régions. Gestion exploitations de BSM hébergé sur le déploiement international du serveur BSM est au sommet de la hiérarchie et gère les serveurs régionaux. Il centralise les événements ou agit en qualité de responsable des responsables de l'environnement complet. Il représente une console de surveillance internationale. Les serveurs régionaux peuvent également agir en tant que responsables des responsables des systèmes subordonnés de leur propre région afin de créer un environnement régional surveillé. Il est possible de présenter la gestion d'environnements surveillés de manière hiérarchique.

Si vous travaillez au sein d'une grande entreprise dotée de plusieurs serveurs de gestion répartis sur un large secteur, il est possible que vous ne disposiez pas localement des connaissances spécialisées nécessaires à la compréhension d'un point particulier. Par exemple, votre organisation dispose peut-être d'un centre de compétences responsable SAP. Un autre centre d'expertise peut, quant à lui, être responsable de la gestion des bases de données.

Une hiérarchie des centres de compétences répartit la responsabilité des éléments de configuration au sein de l'environnement surveillé. Les serveurs régionaux ne sont pas uniquement responsables des éléments de configuration.

Bien au contraire, les événements concernant des points particuliers sont dédiés à un serveur de centres de compétences disposant du savoir-faire nécessaire à la résolution de problèmes semblables pour tous les éléments de configuration de l'environnement surveillé.

Dans un environnement distribué, l'administrateur des systèmes informatiques peut configurer des serveurs régionaux de manière à transférer certains messages à d'autres serveurs du réseau. Ce même administrateur système peut configurer des serveurs régionaux de manière à transférer des événements vers n'importe quel serveur du réseau, où qu'il soit, en fonction des attributs des événements.

Dans la [Figure 5 , page précédente](#), l'ensemble des serveurs régionaux (BSM en Europe, BSM aux États-Unis et BSM en Asie-Pacifique) transfèrent l'ensemble des événements associés à la base de données au serveur du centre de compétences sur les bases de données et l'ensemble des événements associés à des systèmes SAP au serveur du centre de compétences SAP.

Dans ce cas, la console de surveillance synchronise les actions d'événement (par exemple, une résolution, une affectation, un changement de gravité) des serveurs régionaux et des centres de compétences. Ceci garantit la synchronisation permanente de l'état des événements dans l'environnement d'entreprise.

## Monitoring Automation

La surveillance consiste à générer des événements en cas de comportement inattendu d'un élément de configuration. Ces événements peuvent notamment être déclenchés par :

- Le dépassement d'un certain seuil par une valeur surveillée. Exemple : l'espace disque utilisé sur une base de données dépasse une limite prédéfinie de 90 %.
- Le retrait d'un nœud du réseau. Exemple : une coupure de courant entraîne l'arrêt d'un serveur qui ne peut alors plus être atteint.

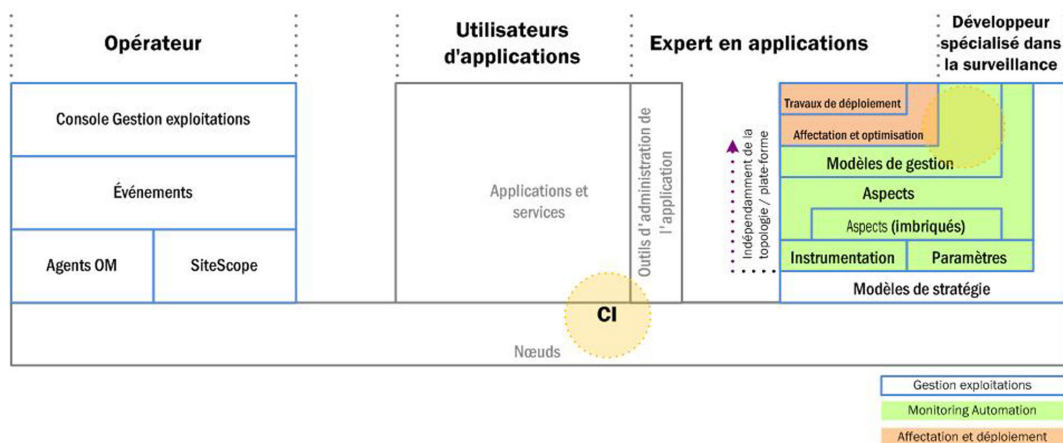
Monitoring Automation offre une solution de gestion complète d'applications ou de services et vous permet ainsi de créer une solution de gestion pour l'ensemble des éléments de configuration (CI) comprenant ces applications ou services. Cette solution peut être conçue de manière à répondre dynamiquement à l'évolution de la topologie, pour une solution de surveillance indépendante du matériel et de la plate-forme d'exécution de l'application ou du service concerné.

Familiarisez-vous avec la terminologie et l'architecture sous-jacentes de Monitoring Automation afin d'en comprendre parfaitement le fonctionnement. Reportez-vous aux piles illustrées à la [Figure 6 , page suivante](#). La base de la pile représente les éléments de configuration à surveiller. Les éléments de configuration peuvent être des éléments réseau tels que des ordinateurs, des applications ou des ensembles d'applications offrant un service. L'accès aux éléments de configuration s'effectue de l'une des manières suivantes :

- Les utilisateurs interagissent avec les éléments de configuration ne faisant l'objet d'aucune surveillance, comme le suggère la section centrale de la [Figure 6 , page suivante](#).
- Gestion exploitations surveille les éléments de configuration selon la structure de surveillance standard illustrée dans la section gauche de la [Figure 6 , page suivante](#).

- Un développeur spécialisé dans la surveillance configure des solutions de surveillance de la manière indiquée dans la section droite de la [Figure 6](#), ci-dessous.
- Un expert en applications lance le processus de surveillance après avoir affiné la configuration paramétrée par le développeur spécialisé en surveillance. Il inspecte les travaux de déploiement et utilise les outils d'administration propres à chaque application afin d'appliquer les mesures nécessaires sur les événements transmis par l'opérateur.

**Figure 6 - Piles de Gestion exploitations**



Monitoring Automation offre plusieurs fonctions de création de solutions de surveillance flexibles. La section suivante détaille chaque fonction ou terme illustré dans la [Figure 6](#), ci dessus, de manière à vous éclairer sur les principes fondamentaux de l'application. L'explication fournie suit l'ordre des couches de la pile de configuration, de bas en haut.

### Nœud

Un nœud est un élément physique accessible sur le réseau.

### Élément de configuration (CI)

Un élément de configuration est un nœud, ou une application ou des services exécutés sur un nœud. Les éléments de configuration constituent l'objet de surveillance actuel de Gestion exploitations. Les événements sont toujours associés à des éléments de configuration.

### Modèles de stratégie

Les modèles de stratégie conditionnent les objets de la surveillance ainsi que le mode de surveillance. Il convient de noter que les modèles de stratégie sont subordonnés à la plate-forme utilisée.

Avant Monitoring Automation, l'ensemble des configurations étaient réalisées par le biais de stratégies et de modèles de stratégie. Cette procédure impliquait la modification des valeurs des modèles de stratégie de l'élément de configuration, conformément auxquels ce dernier était surveillé, à chaque changement de plate-forme, de topologie ou de stratégie de surveillance qu'il subissait.

### Paramètres et instrumentation

Monitoring Automation introduit des paramètres. Chaque paramètre correspond à un paramètre de surveillance pour un attribut d'élément de configuration dans le modèle de stratégie. La modification de la valeur d'un paramètre déclenche un changement dans le comportement de la surveillance. Il est par conséquent inutile de modifier manuellement les valeurs figées dans le code d'un modèle de stratégie. Le concept de valeurs par défaut en cascade représente l'une des caractéristiques essentielles de Monitoring Automation. L'idée est que le développeur spécialisé en surveillance ou l'expert en applications utilise autant de valeurs par défaut que possible à un certain niveau, lesquelles servent ensuite de référence pour la surveillance. Au niveau immédiatement supérieur, un sous-ensemble de ces valeurs peut être remplacé en cas de nécessité pour la tâche de surveillance considérée, sans pour cela qu'il faille redéfinir chaque valeur à remplacer relevant déjà du paramètre de référence.

Les fonctions suivantes des paramètres offrent une plus grande souplesse :

- Les valeurs de paramètre conditionnel permettent l'utilisation d'un même paramètre dans plusieurs modèles de stratégie, pour des solutions de surveillance indépendantes du matériel et des plates-formes mis en œuvre.
- Les paramètres de même valeur peuvent être regroupés sous un paramètre unique. Il devient par conséquent inutile de saisir plusieurs fois la même valeur.

L'instrumentation comprend les scripts et programmes exécutés par HP Operations Agent, tels que définis dans les stratégies mises en œuvre pour les nœuds gérés disposant de l'agent.

#### Aspects

Les modèles de stratégie et l'instrumentation devant déclencher un certain comportement au niveau de l'application ou du service à surveiller sont regroupés sous différents aspects. Au niveau de l'aspect, les développeurs rationalisent la configuration de la manière suivante :

- Ils regroupent les paramètres de même fonction sous un paramètre unique.
- Ils peuvent imbriquer des aspects de manière à regrouper les aspects présentant le même comportement, mais étant définis dans différents modèles de stratégie, sous un aspect unique. Chaque aspect imbriqué peut être associé à une condition de déploiement indiquant à Gestion exploitations quel aspect imbriqué utiliser dans quel environnement. Ceci permet à n'importe quel élément de configuration du type d'élément de configuration cible d'utiliser le même aspect, indépendamment de la plate-forme mise en œuvre.
- Ils définissent les valeurs par défaut au niveau de l'aspect, conformément aux stratégies de surveillance de la société.

#### Modèle de gestion

Un modèle de gestion associe tous les aspects nécessaires à la surveillance d'une application ou d'un service composite. La configuration d'un modèle de gestion comprend la topologie de l'application composite et les aspects à surveiller. En outre, le développeur remplace, au niveau du modèle de gestion, les valeurs par défaut à l'échelle de la société, s'il s'agit d'une exigence de l'application à surveiller.

Le développeur transmet le modèle de gestion terminé à l'expert en applications, qui l'utilise pour lancer la surveillance de l'application cible.

#### Optimisation, affectation et déploiement

Avant de lancer la surveillance, l'expert en applications peut souhaiter remplacer certaines valeurs par défaut configurées par le développeur spécialisé dans la surveillance afin de prendre en compte

les exigences de surveillance propres à la situation qui se présente à lui. C'est ce que l'on appelle l'optimisation.

La configuration de surveillance représentée par un aspect est définie en qualité de type d'élément de configuration. Pour que Gestion exploitations soit en mesure de lancer la surveillance, ce type d'élément de configuration doit être mis en correspondance avec une instance d'élément de configuration réelle découverte par le processus de découverte de topologie. Ce processus de mise en correspondance est appelé "affectation" et peut être réalisé de l'une des manières suivantes :

- Affectation manuelle d'un modèle de gestion. L'expert en applications relie le modèle de gestion à une instance de CI du CI racine du modèle de gestion.
- Affectation manuelle d'un aspect. L'expert en applications relie l'aspect à une instance de CI du type de CI cible de l'aspect.
- Affectation automatique. Si l'expert en applications définit les affectations automatiques d'un modèle de gestion ou d'un aspect, Gestion exploitations affecte dynamiquement des aspects aux instances de CI appropriées, dès leur découverte.

Une fois l'affectation terminée, la solution de surveillance est déployée lors de la même phase. Au cours de la surveillance, l'expert en applications peut garder un œil sur les travaux de déploiement afin de s'assurer que le processus de surveillance se déroule comme prévu ou d'acquérir des informations relatives aux événements signalés par un opérateur.

## Engagement utilisateur

La fonction Engagement utilisateur innovante applique une dynamique de jeu afin de stimuler davantage les utilisateurs de Gestion exploitations. Pour cela, elle propose des défis d'amélioration des activités, optimise les performances de la console de surveillance et consolide le savoir-faire des utilisateurs. La progression favorable des différentes activités est récompensée par des badges et la notification en temps réel des excellentes performances, ce qui apporte une motivation supplémentaire et facilite l'utilisation de Gestion exploitations, pour une meilleure performance des utilisateurs dans leurs tâches quotidiennes. Une chronologie est mise à la disposition des utilisateurs afin que chacun d'entre eux puisse visualiser ses progrès et le nombre de badges reçus. La quasi-totalité des utilisateurs est séduite par au moins un des types de défis intégrés à la dynamique de jeu (réalisation d'une tâche, compétition, statut et clôture), attrait dont Engagement utilisateur tire toute sa puissance.

La définition des objectifs commerciaux que les utilisateurs de Gestion exploitations doivent atteindre et leur récompense pour la réalisation des tâches souhaitées leur permettent de maîtriser les compétences les plus appropriées et d'effectuer les tâches les plus importantes, tout en les incitant à s'engager davantage et à prendre plus de plaisir dans leurs tâches quotidiennes. Les utilisateurs peuvent suivre le résultat de leurs efforts dans les barres de progression et mapper la progression de leurs tâches et défis dans le tableau de bord. La réalisation de chaque nouvelle activité peut être accompagnée d'une notification contextuelle immédiate de bonnes performances.

Engagement utilisateur fait appel à la motivation intrinsèque afin d'aider les utilisateurs de Gestion exploitations à atteindre les objectifs définis, sans leur apporter des avantages extérieurs, qui sont généralement acceptés uniquement afin de procurer un bienfait éphémère. Les gens souhaitent naturellement réussir et être considérés comme brillants. Engagement utilisateur fournit le cadre nécessaire à une simplification de l'utilisation de Gestion exploitations et à une optimisation des tâches quotidiennes. En saluant les résultats des utilisateurs, cet outil leur permet de prendre plus de plaisir et de s'impliquer davantage dans leur travail.

Les administrateurs Engagement utilisateur peuvent sélectionner, configurer et mettre en place des activités intégrées adaptées aux besoins des différents utilisateurs de Gestion exploitations. Les utilisateurs peuvent procéder aux activités de premier niveau et, une fois ces activités terminées, ils sont invités à tenter de réaliser les activités du niveau suivant. Ils bénéficient ainsi d'une meilleure perception de leurs résultats et des progrès réalisés.

## Interfaces d'intégration

Plusieurs interfaces sont fournies pour l'intégration à d'autres applications, ainsi que la modification et la personnalisation du processus de gestion des événements. Par exemple :

- Pour modifier et améliorer les événements au cours de leur traitement, une interface de traitement des événements permet l'intégration de scripts de traitement des événements au sein d'un pipeline de traitement des événements. Ceci vous permet d'enrichir les événements :
  - Au cours de leur traitement, par exemple, en ajoutant des informations utilisées lors de la résolution des éléments de configuration et des indicateurs Type Événement ou en influençant la manière dont sont gérés les événements dupliqués.
  - Pour fournir davantage d'informations une fois le traitement des événements terminés, par exemple, des informations supplémentaires concernant les éléments de configuration des bases de données d'actifs ou des informations utiles pour la résolution de problèmes, telles qu'une URL d'exploration ou un lien vers une base de connaissances externe.
- Pour intégrer des événements dans d'autres applications, une interface de service Web d'événement permet aux développeurs et aux intégrateurs d'automatiser les fonctions de l'opérateur et la détection des modifications subies par les événements. La plupart des opérations réalisables sur la console par un opérateur lors du traitement des événements peuvent être effectuées automatiquement pour plus d'efficacité. Cette interface offre également une assistance aux abonnements par l'intermédiaire du fil Atom.
- Pour synchroniser des événements entre Gestion exploitations de BSM et une application de traitement des événements externe, Gestion exploitations de BSM offre une interface de service Web de synchronisation des événements. Cas typique d'utilisation : la synchronisation d'événements entre Gestion exploitations de BSM et un gestionnaire des incidents, comme Service Manager.
- Pour s'intégrer directement à d'autres gestionnaires de domaine, tels que Microsoft Systems Center Operations Manager, BSM propose HP BSM Integration Adapter.

Le manuel *Operations Manager i Extensibility Guide* disponible dans la bibliothèque de documentation HP Business Service Management décrit ces interfaces et fournit les informations dont les développeurs de contenu et les intégrateurs ont besoin pour personnaliser et enrichir la fonctionnalité de Gestion exploitations de BSM.

## Rôles utilisateur et responsabilités

L'installation, la configuration et l'exécution de la console de surveillance nécessitent une équipe de personnes dotées de compétences spécifiques et jouissant d'une bonne connaissance du domaine. Chaque rôle présente un ensemble de responsabilités et de tâches différent.

- L'opérateur est le gestionnaire pratique des événements et la personne chargée de résoudre les problèmes.

- Le développeur spécialisé dans la surveillance connaît suffisamment bien le produit de surveillance et l'application pour développer lui-même la solution de surveillance. Il décide des systèmes à surveiller et des niveaux de performance appropriés.
- L'administrateur des systèmes informatiques installe et configure les processus de gestion des événements et de surveillance. Son champ d'action est très vaste. Il peut ajouter des utilisateurs au domaine de gestion des utilisateurs BSM conformément aux exigences locales. Il peut octroyer des autorisations et limiter l'accès aux interfaces utilisateur administratives, catégories d'outils et actions personnalisées. Il peut définir des droits et autorisations pour chaque utilisateur ou pour différents types d'utilisateur. Il peut également activer ou désactiver l'accès à des événements affectés à d'autres utilisateurs. Par exemple, il peut autoriser les utilisateurs à visualiser les événements qui ne leur sont pas affectés, mais leur refuser le droit d'y apporter des modifications.
- L'expert en applications sait tout d'une application ou d'un service spécifique. Elle gère l'équipement impliqué dans le fonctionnement de l'application et en résout les problèmes éventuellement indiqués par les événements de surveillance.


Vous trouverez les intitulés fréquemment utilisés pour ces rôles utilisateur, ainsi qu'une synthèse de leurs responsabilités, dans le [Tableau 1 , page suivante](#). Après nous être familiarisés avec Gestion exploitations de BSM, nous allons suivre, dans les prochains chapitres, certains utilisateurs types afin de voir la manière dont ils gèrent leur journée de travail et effectuent leurs tâches. Dans le chapitre suivant, nous détaillerons les responsabilités de Dave au quotidien, l'opérateur d'un environnement d'entreprise utilisant Gestion exploitations de BSM en tant que console de surveillance.

**Tableau 1 - Rôles utilisateur**

Intitulé du poste	Autres intitulés	Responsabilités
<p>Opérateur</p>  <p>Dave</p>	<ul style="list-style-type: none"> <li>Opérateur de domaine</li> <li>Opérateur informatique</li> </ul>	<p>Surveille quotidiennement les événements qui lui ont été affectés ou qui ont été affectés à son groupe de travail.</p> <p>Effectue des opérations de routine n'ayant aucun rapport avec Gestion exploitations de BSM sur les applications, systèmes et réseaux dont il est responsable.</p> <p>Résout les problèmes et événements susceptibles de causer des incidents.</p>
<p>Développeur spécialisé dans la surveillance</p>  <p>Mike</p>	<ul style="list-style-type: none"> <li>Spécialiste de domaine</li> <li>Développeur informatique spécialisé dans la surveillance</li> <li>Expert en applications, réseaux ou dans d'autres domaines spécialisés</li> </ul>	<ul style="list-style-type: none"> <li>Personnalise la manière dont Gestion exploitations de BSM surveille un domaine.</li> <li>Configure les modèles de gestion, les aspects et les modèles de stratégie pour Monitoring Automation.</li> </ul>
<p>Administrateur</p>  <p>Matthew</p>	<ul style="list-style-type: none"> <li>Administrateur système</li> <li>Administrateur des systèmes informatiques</li> <li>Administrateur Gestion exploitations de BSM</li> <li>Concepteur de systèmes</li> </ul>	<p>Supervise l'environnement Gestion exploitations de BSM et l'affectation des tâches.</p> <p>Intègre Gestion exploitations de BSM dans d'autres outils et processus.</p>



**Tableau 1 - Rôles utilisateur, suite**

Intitulé du poste	Autres intitulés	Responsabilités
<p>Expert en applications</p>  <p>Alice</p>	<ul style="list-style-type: none"><li>• Experte spécialisée dans une certaine application ou dans un certain service</li><li>• Administrateur d'applications</li></ul>	<p>Adapte une solution de surveillance à l'environnement spécifique de son application ou service, et affecte des modèles de gestion ou des aspects à des nœuds du système.</p> <p>Déploie la solution de surveillance et s'assure que la surveillance fonctionne correctement.</p>



## Flux de travail de l'opérateur



Nous avons rencontré Dave dans le chapitre « Introduction à Gestion exploitations de BSM ». Dave est l'opérateur responsable de la gestion quotidienne des événements dans un déploiement BSM. "Opérateur" est généralement un poste de débutant dans l'environnement informatique d'une entreprise, mais Dave possède diverses compétences qu'il exploite à son poste. Il maîtrise en effet de nombreuses technologies dans l'environnement Gestion exploitations de BSM.

Le planning de Dave n'est pas fixe puisqu'il est souvent appelé lorsque des problèmes surviennent. Il peut les résoudre en personne ou se connecter à distance afin de garantir le travail ininterrompu de sa communauté d'utilisateurs. L'interface utilisateur Gestion exploitations de BSM lui permet de surveiller les événements qui se produisent dans son domaine de n'importe quel endroit, tant qu'il dispose d'un accès réseau.

Dave doit maîtriser la gestion des événements et l'ensemble des outils associés à l'intégrité à sa disposition. Des outils, des commandes configurables, des scripts et des liens vers d'autres informations sont à la disposition des opérateurs comme Dave pour leur faciliter la résolution et la clôture de différents types d'événement se produisant dans l'environnement d'exploitation.

La console de surveillance permet à Dave de voir immédiatement les alertes et événements affectant son domaine. Il peut se concentrer sur la gestion de ses événements et la résolution automatique des problèmes sous-jacents à l'aide des outils appropriés.

Dave aide l'entreprise à maximiser ses profits en classant les événements par ordre de priorité dans son domaine, en fonction de leur impact sur les services métier et leur continuité. Dave doit résoudre les problèmes mineurs avant qu'ils ne deviennent des problèmes plus importants susceptibles de détériorer la qualité des services métier pris en charge.

Son expérience des technologies sous-jacentes peut l'aider à corréler des événements se produisant dans différents domaines techniques, tels que des bases de données, du matériel, un réseau et des applications Web. Il surveille ces technologies disparates afin de minimiser l'impact d'une défaillance dans un secteur, susceptible de limiter le niveau de réponse du système dans un autre secteur. Remédier aux problèmes avant qu'ils ne s'aggravent améliore la productivité de l'entreprise en minimisant l'effet cascade d'un événement critique non identifié.

Si Dave ne parvient pas à résoudre un problème, il peut l'escalader en transférant l'événement vers une application de traitement des événements externe. Généralement, ce transfert inclut également la propriété de l'événement vers, par exemple, un opérateur d'assistance ou un expert en applications.

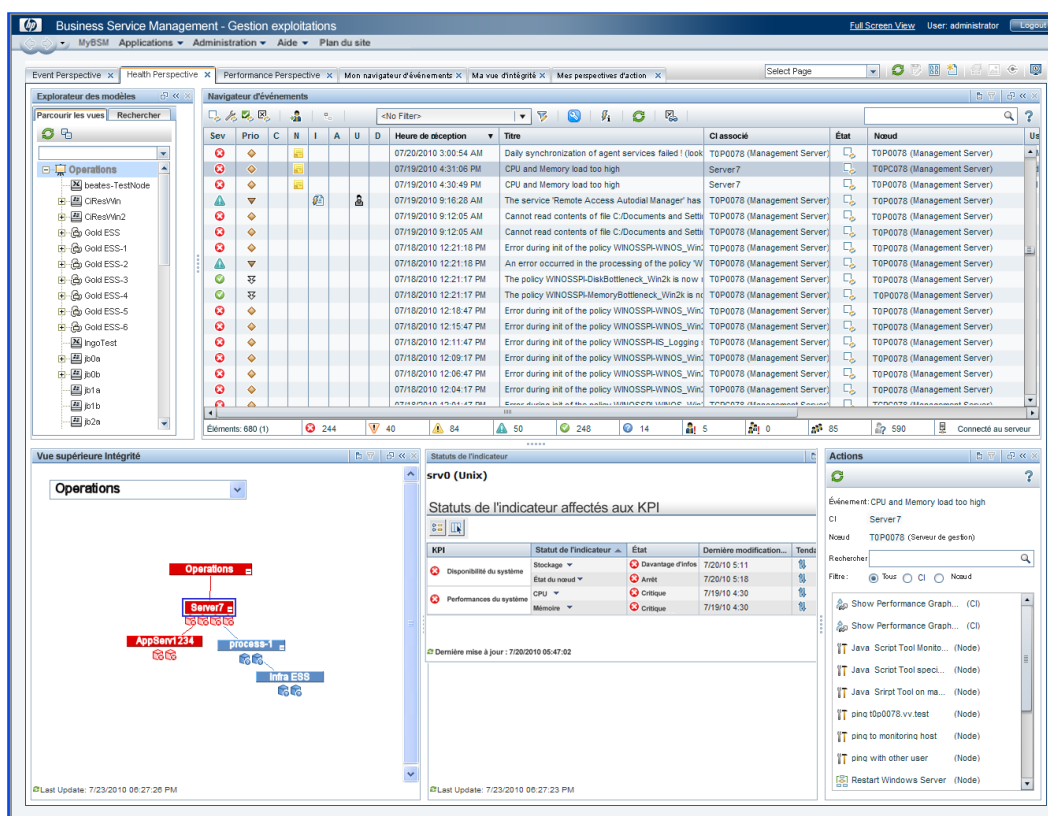
## L'environnement de l'opérateur

L'administrateur système détermine les événements que chaque opérateur peut afficher ou modifier en définissant des rôles utilisateur et en affectant des droits d'utilisateur. Dave peut voir les événements qui lui ont été affectés, ainsi que les autres événements qu'il est autorisé à voir, dans une vue interdomaine. Par exemple, il est responsable du maintien du serveur de messagerie électronique de l'entreprise, mais il peut être en mesure de voir les événements affectés à un autre opérateur.

### Perspective Intégrité

La Figure 7, ci-dessous illustre l'onglet Perspective Intégrité qui comporte cinq volets affichant différentes vues du système. Chaque jour, Dave commence par ouvrir la perspective Intégrité.

Figure 7 - Perspective Intégrité



Les cinq volets offrent une vue globale des événements du domaine de Dave :

- L'explorateur des modèles permet à Dave de sélectionner une vue et un secteur dont il sera responsable. La vue présente les relations parent-enfant des éléments de configuration.
- Le navigateur d'événements répertorie l'ensemble des événements associés et les informations correspondantes dans une vue tabulaire.
- La vue supérieure Intégrité d'un événement sélectionné présente les indicateurs de performance métiers (KPI) de l'élément de configuration associé à l'événement et les éléments de

configuration dans son voisinage.

- Le volet Statuts de l'indicateur fournit des informations détaillées sur le statut d'un élément de configuration sélectionné dans le volet Vue supérieure Intégrité. Cette vue donne des informations sur les performances, les indicateurs de performance métiers Disponibilité et tout statut de l'indicateur pertinent pour l'élément de configuration sélectionné.
- Le volet Actions permet d'afficher les actions qui sont disponibles pour l'événement sélectionné, ses CI associés ou le nœud hôte du CI. Les actions incluent des outils, des guides d'exploitation, des actions personnalisées et des graphiques de performance.

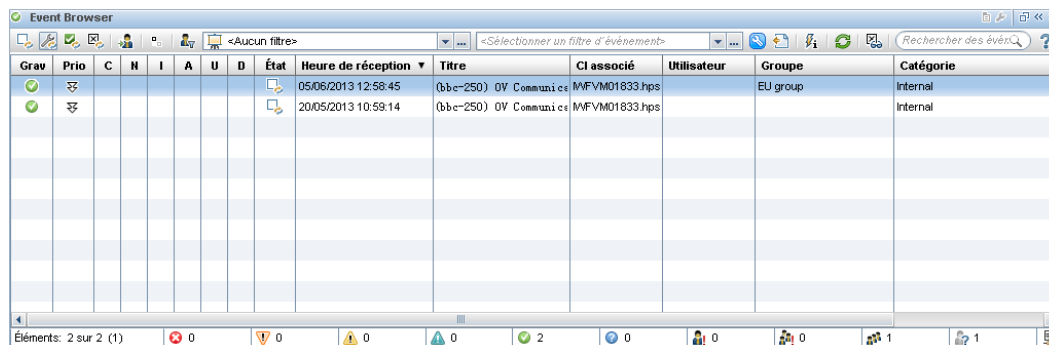
## Navigateur d'événements

Le navigateur d'événements est la première zone observée par Dave. Il peut y voir :

- Une liste des événements actifs classés par ordre de priorité.
- Les événements qui lui ont été affectés.
- Des informations sur les événements irrésolus et non affectés.
- Des détails, classés sous différents onglets, qui indiquent le nombre d'événements critiques, majeurs, mineurs, normaux ou dont le statut est Inconnu ou Avertissement.

La [Figure 8](#), ci-dessous présente une vue globale type des informations relatives aux événements, organisées dans le volet Navigateur d'événements.

**Figure 8 - Navigateur d'événements**



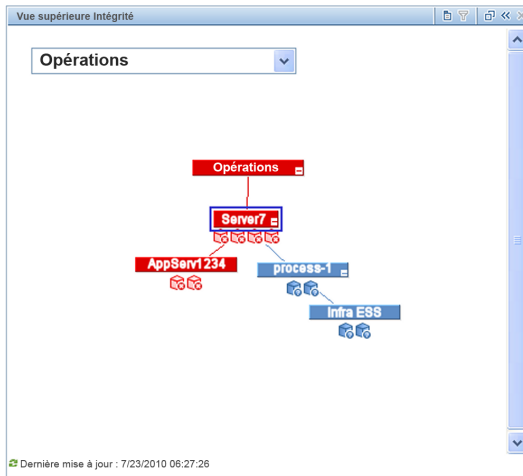
Grav	Prio	C	H	I	A	U	D	État	Heure de réception	Titre	CI associé	Utilisateur	Groupe	Catégorie
✓	☞								05/06/2013 12:58:45	(bb-c-250) 0V Communics	MFVVM01833.hps		EU group	Internal
✓	☞								20/05/2013 10:59:14	(bb-c-250) 0V Communics	MFVVM01833.hps			Internal

Dave utilise des filtres pour observer des événements de vues prêtes à l'emploi. Il peut également personnaliser son espace de travail en définissant différents filtres et onglets. Par exemple, il peut utiliser une combinaison de gravité et priorité afin de repérer les événements nécessitant une intervention immédiate. La première tâche est de déterminer les événements d'importance capitale à examiner en priorité.

## Vue supérieure Intégrité

Lorsque Dave sélectionne un événement à analyser, la vue supérieure Intégrité est mise à jour de manière à afficher davantage d'informations sur l'élément de configuration associé. Par exemple, supposons que l'événement soit déclenché par le dépassement d'un quota de stockage sur un serveur associé. La vue supérieure Intégrité présente la vue topologique du serveur concerné. Dave peut le sélectionner dans cette vue afin d'obtenir plus d'informations. La [Figure 7](#), page 32 illustre une vue supérieure Intégrité type de services métier et éléments de configuration.

**Figure 9 - Vue supérieure Intégrité**



Pour chaque nœud de la vue supérieure Intégrité, il peut utiliser un menu contextuel afin d'obtenir des informations sur l'impact métier. Par exemple, s'il choisit Server7, il peut voir les services métier ou Conventions de service (SLA) susceptibles d'être affectés par un événement ou une interruption. La vue supérieure Intégrité permet à un opérateur de voir l'intégrité de n'importe quel élément de configuration du diagramme de topologie. L'examen des éléments de configuration situés en amont et en aval peut fournir d'autres indices susceptibles de faciliter l'identification du problème.

La prochaine étape est l'analyse de l'origine du problème à l'aide du volet Statuts de l'indicateur.

### Volet Statut de l'indicateur

Lorsque Dave sélectionne l'élément de configuration affecté dans la vue supérieure Intégrité, le volet Statuts de l'indicateur est mis à jour de manière à afficher davantage d'informations sur cet élément de configuration. La colonne des tendances, illustrée dans la [Figure 10](#), ci-dessous, indique si le statut actuel est une amélioration ou une aggravation des précédents statuts d'indicateur.

**Figure 10— Volet Statuts de l'indicateur**

KPI	Statut de l'indicateur	État	Dernière modification...	Tendance
Disponibilité du système	Stockage	Davantage d'infos	7/20/10 5:11	↕
	État du nœud	Arrêt	7/20/10 5:18	↕
Performances du système	CPU	Critique	7/19/10 4:30	↕
	Mémoire	Critique	7/19/10 4:30	↕

Cette vue détaillée peut indiquer s'il n'existe qu'un seul problème sous-jacent ou une variété de facteurs ayant contribué à l'événement critique. Ces informations permettent à Dave de prendre

rapidement sa décision concernant la suite des opérations. Lorsqu'il prend une mesure, les autres opérateurs voient qu'il travaille sur ce problème et peuvent se concentrer sur d'autres événements critiques.

Dave peut également utiliser des graphiques de performance et d'autres outils pour résoudre ce problème.

### Autres outils

Les détails d'un événement peuvent contenir des instructions. Dave peut sélectionner l'onglet **Informations supplémentaires**, qui peut contenir des remarques ou des conseils sur la résolution du problème. Cet onglet peut comprendre un outil de diagnostic ou un script que Dave peut exécuter pour analyser les performances des éléments de configuration en détail, ou encore des journaux associés comportant des messages d'erreur informatifs.

Dave dispose de graphiques de performance qui constituent d'utiles outils d'analyse. Par exemple, si un événement lié aux performances d'une base de données se produit, Dave peut cliquer à l'aide du bouton droit de la souris sur l'événement et sélectionner **Afficher > Graphiques de performance (voisinage)**. Les graphiques de performance sont affichés pour l'élément de configuration affecté par l'événement et pour ses éléments de configuration voisins, tels que le serveur d'applications affecté. Ces graphiques présentent non seulement les informations relatives aux performances au moment de l'événement, mais également les informations relatives aux performances à un moment antérieur.

**Remarque** : Les outils de Gestion exploitations de BSM ne se limitent pas à la résolution d'événements. Dave peut également lancer des outils uniquement pour réaliser ses tâches quotidiennes.

### Résolution

Il existe de nombreuses manières de résoudre un problème. Dans le cadre de notre exemple, il est suggéré à Dave d'exécuter un outil à partir du menu **Lancer**. Dans le navigateur d'événements, Dave clique avec le bouton droit de la souris sur l'événement et sélectionne **Lancer > Outils > Réparer le système de fichiers (CI)**. Dès que l'outil a terminé, le problème est résolu et l'événement disparaît de la liste. Si le problème n'est pas résolu, Dave peut accéder aux guides d'exploitation associés dans le volet Actions. Les guides d'exploitation sont des scripts qui exécutent un processus en plusieurs étapes afin de résoudre le problème.

## Autres rôles

L'opérateur compte sur l'expertise de deux autres rôles clés :

- Le développeur spécialisé dans la surveillance  
Voir le « Flux de travail du développeur spécialisé dans la surveillance » , page 41
- L'administrateur système  
Voir le « Flux de travail de l'administrateur des systèmes informatiques » , page 45





## Flux de travail du développeur spécialisé dans la surveillance



Mike est un développeur de Gestion exploitations de BSM spécialisé dans la surveillance. Son objectif principal est de personnaliser Gestion exploitations de BSM afin de répondre à des exigences professionnelles spécifiques.

Généralement, Mike intègre de nouvelles applications et de nouveaux éléments de configuration dans le processus de surveillance. Pour créer un environnement de surveillance pour applications et services composites satisfaisant aux normes de la société, Mike configure des éléments de Monitoring Automation, tels que des modèles de gestion et des aspects. Il personnalise les modèles de stratégie et les associe aux modèles de gestion et aux aspects afin de mettre en application les détails de la surveillance. Il assure également l'indépendance des solutions de surveillance par rapport aux instances et plates-formes en procédant à des affectations automatiques et au déploiement conditionnel d'aspects.

Par exemple, il doit définir la surveillance d'un groupe de serveurs prenant en charge le protocole FTP. Ces serveurs prennent en charge les services métier critiques en permettant aux services internes d'envoyer et de recevoir des blocs de données volumineux.

Dans un premier temps, le service des paies, par exemple, transmettra, à partir de ce serveur, les informations de versement des salaires aux employés au service des paies de l'entreprise. Le service des paies renverra les rapports récapitulatifs internes, les rapports gouvernementaux requis qui doivent être archivés et redistribués aux organismes gouvernementaux appropriés, et fournira tout autre document ayant trait aux paies.

Mike doit définir la manière dont doivent être gérés les serveurs FTP afin d'en assurer l'intégrité en toutes circonstances, mais aussi afin qu'ils puissent traiter les demandes, et permettre de télécharger dans un environnement sécurisé à partir du FTP. Si les serveurs sont indisponibles, des délais ne seront pas respectés et, dans les cas extrêmes, une interruption pourrait entraîner des amendes pour manquement à des exigences gouvernementales.

### Analyse initiale

Les premiers points auxquels Mike doit penser sont les indicateurs de performance métiers et les statuts d'indicateur pour les serveurs FTP. Principales questions auxquelles répondre :

- Si la disponibilité et les performances des applications sont importantes, comment doit-il mesurer ces indicateurs de performance métiers ?

- Quelles Conventions de service (SLA) peuvent être violées si les seuils de disponibilité et de performance du serveur FTP ne sont pas atteints ?

L'organisation informatique n'est pas seulement responsable de la disponibilité de ce serveur et de ses applications résidentes. Elle doit également s'assurer que l'ensemble des ressources associées fonctionnent conformément aux attentes des utilisateurs. Mike doit prendre en compte l'ensemble de ces informations lors de la sélection des indicateurs de performance métiers et de la définition des principaux statuts d'indicateur.

## Définition de statuts d'indicateur

Quels sont les indicateurs de performance métiers que le processus de surveillance doit mesurer ?

Comment doivent-ils être rapportés aux propriétaires du service métier utilisant le serveur FTP ?

Mike se concentre sur la définition des statuts d'indicateur prenant en charge les indicateurs de performance métiers sélectionnés. Par exemple, les statuts d'indicateur pour la disponibilité des applications d'un serveur FTP Windows peuvent comprendre des métriques de service Windows signalant les éléments suivants :

- Nombre de connexions de tous types émanant du service
- Nombre d'octets transférés par seconde
- Temps de réponse du serveur

Mike doit configurer le processus de surveillance, créer la stratégie de surveillance et déterminer la manière d'en indiquer le statut.

Par chance, il dispose de plusieurs applications HP prenant en charge ces tâches. Son expérience de ces applications et les connaissances générales qu'il possède en la matière lui permettent de choisir la meilleure solution pour réaliser ces tâches. Par exemple, il peut choisir la stratégie d'un agent HP Operations Manager, HP SiteScope ou un autre outil de surveillance HP. Le statut de l'indicateur qu'il sélectionne, quel qu'il soit, doit disposer d'un outil de prise en charge capable d'en indiquer l'état.

## Autres tâches

Mike réalise différentes tâches pour optimiser le processus de maintenance de l'intégrité et de surveillance pour le serveur FTP. Il peut, par conséquent, effectuer au moins une des tâches suivantes :

- Créer des graphiques synthétisant les métriques collectées pour le serveur FTP et les affecter au type d'élément de configuration Serveur FTP afin qu'ils apparaissent automatiquement.
- Créer des outils Gestion exploitations de BSM pour redémarrer le serveur FTP.
- Créer plusieurs guides d'exploitation opérationnels. Par exemple, Mike pourrait créer un guide d'exploitation permettant la suppression des fichiers obsolètes du serveur FTP.
- Créer des content packs contenant les composants de surveillance.
- Créer des règles de corrélation en vue de mapper certains problèmes de disque identifiés à certains problèmes de serveur FTP.

Le rôle de Mike est important. Il envisage les métriques qui seront nécessaires et la manière dont elles seront capturées, et définit les processus associés pour la collecte de données et la résolution de problèmes.

## Autres rôles

Mike, le développeur spécialisé dans la surveillance, intègre de nouvelles applications et de nouveaux éléments de configuration dans le processus de surveillance. Ceux-ci sont configurés par Matthew, l'administrateur des systèmes informatiques, afin que les opérateurs, Dave et ses collègues, puissent s'en servir. Il met également au point des solutions de gestion à l'attention d'Alice, l'expert en applications, et ses collègues.

Pour plus d'informations sur ces autres rôles, voir :

- L'administrateur système

Voir le « Flux de travail de l'administrateur des systèmes informatiques », page 45

- L'opérateur

Voir le « Flux de travail de l'opérateur », page 35

- L'expert en applications

Voir le « Flux de travail de l'expert en applications », page 49



# Flux de travail de l'administrateur des systèmes informatiques



Dans le chapitre « [Introduction à Gestion exploitations de BSM](#) », nous nous sommes familiarisés avec le concept d'une console de surveillance. Gestion exploitations de BSM est la console de surveillance permettant d'obtenir une solution de surveillance BSM complète. Il offre un emplacement centralisé pour la gestion des événements et des performances. Cette console de surveillance permet une gestion consolidée des opérations de l'environnement BSM.

Dans le chapitre « [Flux de travail de l'opérateur](#) », nous avons appris que la console de surveillance offre une vue complète de l'ensemble des événements d'exploitation, permettant une intervention immédiate si nécessaire. Pour un fonctionnement efficace de la console de surveillance, une personne doit se charger de sa configuration et de son optimisation. C'est le rôle de Matthew en tant qu'administrateur des systèmes informatiques.

Matthew conçoit un environnement de surveillance efficace pour le personnel dédié aux opérations et agit donc en arrière-plan. Son rôle consiste à assurer la maintenance continue de cet environnement, à gérer les utilisateurs et les rôles utilisateur et à chercher à optimiser le processus de surveillance. Il conçoit le système d'exploitation et met en place les processus auxquels les autres membres de l'organisation doivent chaque jour se conformer. La création de scripts et l'automatisation d'autant de processus que possible sont sa spécialité.

Matthew doit bien connaître l'environnement d'exploitation, comprendre les dépendances existantes entre les différentes applications et configurer un environnement aussi efficace que possible.

## Tâches d'installation et de configuration

Matthew dispose des connaissances générales nécessaires à l'installation et à la configuration de Gestion exploitations de BSM et de Monitoring Automation. Dans un cas simple, il pourrait y avoir une instance de Monitoring Automation for Servers installée avec la licence Fondations de Gestion des événements d'Operations Manager i. Dans un cas complexe, il pourrait y avoir plusieurs instances d'Operations Manager i et de Gestion exploitations de BSM dans un environnement distribué de type Manager-of-Managers (voir « [Introduction à Gestion exploitations de BSM](#) », page 9). Lors d'un déploiement de type Manager-of-Managers, une intégration parfaite dans ces environnements requiert que Matthew intègre les flux HP Operations Orchestration, les incidents HP Network Node Manager i (NNMi) et les événements Business Process Monitor.

Matthew active également le processus de surveillance en installant les outils de surveillance nécessaires, notamment Operation Agent et Sitescope.

Matthew installe et gère des content packs, qui contiennent les définitions utilisées par les stratégies de surveillance, tels que les content packs pour Monitoring Automation.

Si nécessaire, Matthew installe HP BSM Integration Adapter afin de faciliter l'intégration de gestionnaires de domaine tiers, tels que Microsoft System Center Operations Manager (SCION).

Matthew a les responsabilités suivantes :

- Supervision de l'installation de BSM
- Paramétrage de l'environnement
- Réglage des paramètres d'infrastructure
- Configuration d'utilisateurs et de rôles utilisateur

#### Supervision de l'installation de BSM

Matthew est spécialiste du domaine et possède une certaine expérience de la gestion opérationnelle. Il sait comment installer les composants de BSM, notamment Gestion exploitations, et bien les configurer. Il conçoit et supervise le processus d'installation de bout en bout des composants de BSM requis et décide des applications à intégrer dans BSM. Parmi ces applications peuvent se trouver d'autres solutions d'entreprise HP et applications tierces, telles que Microsoft SCOM.

La complexité de son travail réside dans l'intégration de plusieurs applications métier d'entreprise et d'infrastructure selon les principes de l'Information Technology Infrastructure Library (ITIL®). Son objectif est d'installer et de configurer des applications autonomes travaillant parfaitement ensemble. Chacune fonctionne séparément mais communique efficacement avec les autres applications.

#### Paramétrage de l'environnement

Matthew configure l'ensemble des serveurs connectés. Il définit ensuite des règles de transfert des événements et des notifications, et choisit les destinataires des notifications d'événement. Dans certains cas, la réponse à un événement est l'utilisation des scripts personnalisés identifiés ou créés par Matthew. Enfin, il conçoit le processus d'affectation de nouveaux événements à une communauté d'utilisateurs spécifique. Il s'agit de filtres basés sur une règle permettant de s'assurer que Gestion exploitations de BSM affecte automatiquement chaque événement au groupe ou à l'individu approprié.

#### Réglage des paramètres d'infrastructure

Ces paramètres font appel à de nombreuses compétences. Si Matthew modifie un paramètre, il doit en saisir l'impact sur l'environnement d'exploitation. Par exemple, s'il limite les informations fournies dans le journal d'audit, des détails de certains événements peuvent être omis. D'autres paramètres décrivent différents aspects de l'environnement (tels que le serveur de certificat SSL), la manière dont les événements associés sont gérés et la gestion des événements dupliqués.

#### Configuration d'utilisateurs et de rôles utilisateur

Matthew est responsable de la définition des rôles utilisateur, ainsi que des droits et limites associés à ces rôles. Un rôle utilisateur permet d'affecter globalement les mêmes droits à des utilisateurs, plutôt que de configurer chaque autorisation séparément. Si un nouvel opérateur ou un nouveau développeur spécialisé dans la surveillance rejoint l'entreprise, Matthew l'ajoute au

système et lui affecte l'un de ses rôles utilisateur prédéfinis afin de lui octroyer automatiquement les mêmes droits et limites qui touchent les autres utilisateurs ayant ce rôle.

## Autres responsabilités

L'administrateur des systèmes informatiques a d'autres responsabilités, parmi lesquelles :

- Choisir les scripts EPI (interface de traitement de l'événement) à exécuter à des moments prédéfinis
- Définir des actions personnalisées

## Tâches continues

Une fois l'installation et la configuration initiales réalisées, les bénéficiaires du système sont les opérateurs dont la tâche est de gérer les événements qu'ils surveillent. Matthew fournit à Dave, l'opérateur, un environnement qui simplifie ses tâches quotidiennes et lui permet de réagir aux événements critiques aussi rapidement et efficacement que possible.

Une fois la configuration initiale effectuée, la maintenance est automatique jusqu'à ce qu'un utilisateur en demande la modification. La plupart des environnements doivent également évoluer afin de satisfaire à de nouvelles demandes. Mike, le développeur spécialisé dans la surveillance, peut envoyer de nouveaux content packs ou des contenus packs mis à jour à Matthew pour qu'il les installe. En réponse à la croissance de l'entreprise, Matthew doit ajouter des utilisateurs et affecter à chacun d'entre eux le rôle utilisateur et les autorisations appropriés.

Matthew peut également constater au cours de ses opérations quotidiennes qu'il doit réviser certains de ses modèles d'origine pour le transfert d'événements et les notifications. À chaque nouvelle situation, Matthew décide s'il est nécessaire d'utiliser des scripts existants ou de créer des modèles de réponse. Le paramétrage de l'environnement optimise cette opération et la surveillance.

## Console de surveillance

Le regroupement de l'ensemble des opérations d'une infrastructure, y compris les applications, les serveurs dédiés et les logiciels et matériel associés, sous un même parapluie informatique permet de satisfaire aux objectifs de contrat de service des entreprises. Le rôle de Matthew est de configurer cet environnement hautes performances et d'utiliser Gestion exploitations de BSM comme console de surveillance. L'ensemble des composants travaillent de concert pour fournir les services métier internes nécessaires aux employés et les services de portail ou autre disponibilité applicative aux abonnés externes. Imaginez un environnement bancaire international disposant d'un ensemble de serveurs, d'applications, d'éléments de configuration et autres, garantissant une réponse de 99,999 %. Ce type d'engagement nécessite le type d'environnement d'exploitation bien conçu que Matthew propose.

## Autres rôles

Matthew, l'administrateur des systèmes informatiques, configure et optimise la console de surveillance, y compris le contenu développé par Mike, le développeur spécialisé dans la surveillance, à des fins d'utilisation par les opérateurs, Dave et ses collègues.

Pour plus d'informations sur ces autres rôles, voir :

- Le développeur spécialisé dans la surveillance

Voir le « Flux de travail du développeur spécialisé dans la surveillance », page 41

- L'opérateur

Voir le « Flux de travail de l'opérateur », page 35



## Flux de travail de l'expert en applications



Dans le chapitre « Introduction à Gestion exploitations de BSM », nous nous sommes familiarisés avec le concept d'une console de surveillance. Gestion exploitations de BSM est la console de surveillance permettant d'obtenir une solution de surveillance BSM complète. Il offre un emplacement centralisé pour la gestion des événements et des performances. Cette console de surveillance permet une gestion consolidée des opérations de l'environnement BSM.

Nous avons également vu comment Monitoring Automation aidait à créer des solutions de surveillance flexibles pour les applications et les services.

Dans le « Flux de travail du développeur spécialisé dans la surveillance », nous avons rencontré Mike, qui conçoit des solutions de surveillance conformes aux stratégies de la société, relatives aux éléments à surveiller et à la manière dont ils doivent l'être.

Alice est l'expert en applications spécialisée dans une application ou un service spécifique. Elle est la spécialiste des systèmes sur lesquels les applications sont exécutées et connaît parfaitement les rouages de l'application qu'elle maîtrise. Alice est responsable du déploiement du modèle de gestion développé par Mike en vue de surveiller l'instance réelle de l'application dont elle est en charge.

### Tâches d'installation et de configuration

Avant de lancer la surveillance de son système, Alice règle les valeurs sur lesquelles l'application sera surveillée. Les valeurs configurées dans le modèle de gestion de Mike, le développeur spécialisé dans la surveillance, reflètent les normes de la société en matière de surveillance des applications de même type que l'application d'Alice. Il est possible qu'Alice ait besoin de modifier certaines de ces valeurs afin de répondre aux besoins de l'instance d'une application particulière dont elle est en charge.

Une fois le modèle de gestion affiné, elle l'affecte et le déploie.

- Gestion exploitations découvre des instances des types d'élément de configuration de la vue de topologie configurée dans le modèle de gestion. Alice n'a plus qu'à définir les affectations automatiques réalisables pour le modèle de gestion. Une fois la configuration des affectations automatiques pour le modèle de gestion terminée, Gestion exploitations met en correspondance les types d'élément de configuration du modèle de gestion avec les instances d'élément de configuration découvertes, puis déploie les aspects nécessaires à leur surveillance automatique.
- Si un contrôle renforcé est nécessaire, Alice peut affecter manuellement le modèle de gestion ou

l'aspect aux éléments de configuration découverts. Gestion exploitations déploie ensuite ces aspects dans le modèle de gestion.

## Tâches continues

Au cours de la surveillance, Alice vérifie de temps en temps les travaux de déploiement concernant son application afin de s'assurer que le processus de surveillance fonctionne comme prévu.

Si son application génère des événements, Alice peut y remédier en exécutant des outils d'administration propres à son application à partir de la console OMi.

## Autres rôles

Alice, l'expert en applications, règle et lance le processus de surveillance de l'instance de l'application dont elle est responsable à l'aide du modèle de gestion mis au point par Mike, le développeur spécialisé dans la surveillance. Le processus de surveillance génère des événements traités par Dave, l'opérateur.

Pour plus d'informations sur ces autres rôles, voir :

- Le développeur spécialisé dans la surveillance

Voir le « Flux de travail du développeur spécialisé dans la surveillance » , page 41

- L'opérateur

Voir le « Flux de travail de l'opérateur » , page 35

## Synthèse

Après vous être familiarisé avec les différents utilisateurs chargés de l'installation, de la configuration et de la gestion des opérations quotidiennes de Gestion exploitations de BSM, vous constaterez que le fonctionnement optimal d'une infrastructure repose sur une multitude de compétences. Vous pouvez revêtir l'un des rôles décrits dans le présent manuel. Quel qu'il soit, vous pouvez, avec votre groupe de travail, faire la différence en termes de qualité fournie aux abonnés internes.



---

# Index

- A**
- Actions 20
  - Affectation
    - Affectation 28, 49
    - Affectation automatique 28-29, 41
  - Aspect 28
- C**
- Configuration 46
  - Console de surveillance 10, 19, 26, 30, 47
  - Content pack 21, 42, 46
- D**
- Déploiement
    - Déploiement 27, 49
    - Travaux de déploiement 27, 29, 50
- E**
- Engagement utilisateur 29
- G**
- Gestion des événements 10, 18, 30-31, 35
    - Corrélation des événements 17
    - Cycle de vie des événements 14
    - Mappage de l'événement 21
    - Navigateur d'événements 37
    - Suppression d'une tempête d'événements 19
    - Suppression des événements dupliqués 17
    - Synchronisation des événements 30
    - Tableau de bord des événements 14
  - Graphiques 20
  - Guides d'exploitation 20, 42
- I**
- Installation 46
  - Instrumentation 27
  - Intégration 10, 30, 41
- L**
- Licences 9
- M**
- Manager-of-Managers 25
  - Modèle de gestion 28
  - Modèle de stratégie 27
  - Monitoring Automation 26, 46, 49
- O**
- Optimisation 28, 46, 49
  - Outils 20, 39, 42
- P**
- Paramètre 27
- R**
- Règles 21, 42
- S**
- Solution entreprise 24, 26, 41
  - Statut de l'indicateur 15, 36, 38, 42
- T**
- Topologie
    - Synchronisation 22

