

IBM Defense Operations Platform
Version 1.6

*IBM Defense Operations Platform
Documentation produit*

IBM

IBM Defense Operations Platform
Version 1.6

*IBM Defense Operations Platform
Documentation produit*

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 207.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.can.ibm.com> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex*

La présente édition s'applique à IBM Defense Operations Platform version 1.6.0, et à toutes les modifications et versions suivantes sauf indication contraire dans les nouvelles éditions.

© Copyright IBM Corporation 2011, 2013.

Table des matières

Figures	vii
--------------------------	------------

Avis aux lecteurs canadiens.	ix
---	-----------

Chapitre 1. Présentation de la solution . 1

Editions d'IBM Defense Operations Platform.	1
Nouveautés de la version 1.6	2
Services système IBM Defense Operations Platform	3
Serveurs IBM Defense Operations Platform dans Field Edition	4
Serveurs IBM Defense Operations Platform dans Command Center Edition	6
Configuration matérielle requise pour IBM Defense Operations Platform pour Field Edition	8
Configuration matérielle requise pour IBM Defense Operations Platform dans Command Center Edition.	10
Configuration des logiciels prérequis	11

Chapitre 2. Installation et configuration 13

Serveur d'installation	13
Listes de contrôle d'installation	13
Liste de contrôle - installation de IBM Defense Operations Platform Field Edition	13
Liste de contrôle - installation de IBM Defense Operations Platform Command Center Edition	14
Utilisation des fichiers de démarrage pour préparer Red Hat Enterprise Linux	15
Préparation des serveurs	16
Configuration du réseau TCP/IP	16
Désactivation des paramètres de sécurité	21
Configuration des services SSH.	22
Installation des packages Linux pour Field Edition	22
Installation des packages Linux pour Command Center Edition	25
Définition d'exigences de pré-installation supplémentaires	30
Préparation des serveurs pour Command Center Edition	30
Préparation du serveur d'installation	31
Fichiers de propriétés de la topologie.	32
Personnalisation des propriétés d'installation	32
Informations sur le serveur cible pour Field Edition	33
Informations sur le serveur cible pour Command Center Edition	34
Informations sur les services d'annuaire	36
Suffixe LDAP.	36
Domaine LTPA (Lightweight Third-Party Authentication)	37
Propriétés de groupement	37
Informations sur les mots de passe pour Field Edition	38
Informations sur les mots de passe pour Command Center Edition	40

Propriétés Cyber Hygiene	43
Exécution du programme d'installation de ligne de commande Field Edition	43
Exécution du programme d'installation de ligne de commande Command Center Edition.	45
Vérification de l'installation avant la configuration de post installation	47
Configuration de post-installation d'IBM Defense Operations Platform	48
Configuration des services de collaboration pour IPv6	48
Configuration de la connexion unique pour les services de collaboration	48
Définition du délai d'expiration de session	50
Configuration d'un serveur LDAP de services de collaboration secondaire dans Command Center Edition	51
Configuration d'autres relations de gestionnaires de grappes dans Command Center Edition	52
Configuration du système NFS externe facultatif dans Command Center Edition.	52
Configuration du nom d'hôte de l'outil d'administration Web Tivoli Directory Server	53
Activation de la journalisation Tivoli Directory Server	53
Suppression des fichiers d'installation du système de production	54
Vérification de l'installation	54
Installation d'IBM Defense Operations Platform Workbench Edition	55

Chapitre 3. Gestion de la solution . . . 57

Accès aux consoles d'administration IBM Defense Operations Platform	57
Démarrage, arrêt et interrogation du statut dans Field Edition	57
Démarrage des composants dans Field Edition	58
Arrêt des composants dans Field Edition	59
Interrogation du statut des composants dans Field Edition	60
Obtention de l'aide pour l'outil de contrôle de plateforme dans Field Edition	61
Démarrage, arrêt, gestion et interrogation du statut dans Command Center Edition.	62
Démarrage des composants dans Command Center Edition	63
Arrêt des composants dans Command Center Edition	64
Interrogation du statut des composants dans un environnement Command Center Edition	65
Gestion des composants HADR dans Command Center Edition	66
Montage et démontage manuels du répertoire WebSphere Message Broker	67

Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition	68	Test Base de données (DB2 Instance - Applications) [2]	113
Détermination du statut des services et composants		Identification des problèmes	113
IBM Defense Operations Platform	69	Test Base de données (DB2 Instance - Directory Server)	115
Utilisation de l'outil de vérification du système	69	Identification des problèmes	115
Test Serveur d'applications (REST BPM_DE.AppTarget.BPMNode1.0).	70	Test Base de données (DB2 Instance - Directory Server) [1]	116
Identification des problèmes	70	Identification des problèmes	116
Test Serveur d'applications (REST IopServer1)	72	Test Base de données (DB2 Instance - Directory Server) [2]	117
Identification des problèmes	73	Identification des problèmes	117
Test Serveur d'applications (REST IopServer2)	75	Test Base de données (DB2 Instance - Logiciel intermédiaire)	118
Identification des problèmes	75	Identification des problèmes	119
Test Serveur d'applications (REST isim1).	78	Test Base de données (DB2 Instance - Logiciel intermédiaire) [1]	120
Identification des problèmes	78	Identification des problèmes	120
Test Serveur d'applications (REST odmServer1)	80	Test Base de données (DB2 Instance - Logiciel intermédiaire) [2]	121
Identification des problèmes	80	Identification des problèmes	121
Test Serveur d'applications (REST odmdc1).	83	Test Base de données (System Verification Check Scheduler)	122
Identification des problèmes	83	Identification des problèmes	122
Test Serveur d'applications (REST STProxyServer1).	85	Test Decision Management (Console Decision Center de WebSphere Operational Decision Management)	124
Identification des problèmes	85	Identification des problèmes	124
Test Serveur d'applications (REST WebSphere_Portal)	88	Test Decision Management (console Rule Execution Server de WebSphere Operational Decision Management)	125
Identification des problèmes	88	Identification des problèmes	125
Test Serveur d'applications (REST WebSphere_Portal_PortalNode2)	91	Test Répertoire (Tivoli Directory Server)	126
Identification des problèmes	91	Identification des problèmes	126
Test Serveur d'applications (REST WSRServer1)	93	Test Répertoire (Tivoli Directory Server) [1]	128
Identification des problèmes	93	Identification des problèmes	128
Test Serveur d'applications (REST WorklightServer1)	96	Test Répertoire (Tivoli Directory Server) [2]	130
Identification des problèmes	96	Identification des problèmes	130
Test Serveur d'applications (REST WorklightServer2)	98	Test Répertoire (Console Tivoli Directory Server)	132
Identification des problèmes	99	Identification des problèmes	132
Test Serveur d'applications (Console d'administration de WebSphere Application Server version 7)	101	Test Répertoire (Tivoli Directory Server Proxy)	134
Identification des problèmes	101	Identification des problèmes	134
Test Serveur d'applications (Console d'administration de WebSphere Application Server version 8)	102	Test Répertoire (WebSphere Service Registry and Repository)	137
Identification des problèmes	102	Identification des problèmes	137
Test Serveur d'applications (Console d'administration de WebSphere Application Server version 8.5).	104	Test Messagerie (vérification de l'installation de Message Broker)	139
Identification des problèmes	104	Identification des problèmes	139
Test Collaboration (Console Lotus Domino)	105	Test Messagerie (vérification de l'installation de Message Broker) [1]	141
Identification des problèmes	105	Identification des problèmes	141
Test Collaboration (Console Lotus Sametime)	107	Test Messagerie (vérification de l'installation de Message Broker) [2]	143
Identification des problèmes	107	Identification des problèmes	143
Test Collaboration (Console de proxy Lotus Sametime)	108	Test Mobile (console IBM Worklight)	145
Identification des problèmes	108	Identification des problèmes	145
Test Base de données (DB2 Instance - Applications)	111	Test Mobile (console IBM Worklight)[1].	147
Identification des problèmes	111	Identification des problèmes	147
Test Base de données (DB2 Instance - Applications) [1]	112	Test Mobile (console IBM Worklight)[2].	149
Identification des problèmes	112	Identification des problèmes	150
		Test Surveillance (Netcool Omnibus)	152

Identification des problèmes	152
Test Surveillance (Tivoli Enterprise Monitoring Server)	153
Identification des problèmes	153
Test Surveillance (Tivoli Enterprise Portal Server)	155
Identification des problèmes	155
Test Surveillance (Tivoli Integrated Portal/Netcool).	156
Identification des problèmes	157
Test Gestion des mots de passe (Tivoli Directory Integrator)	158
Identification des problèmes	158
Test Portail (console WebSphere Portal via le serveur Web)	159
Identification des problèmes	160
Test Portail (console WebSphere Portal via le serveur Web) [1]	162
Identification des problèmes	162
Test Portail (console WebSphere Portal via le serveur Web) [2]	164
Identification des problèmes	164
Test Portail (console WebSphere Portal).	166
Identification des problèmes	166
Test Portail (console WebSphere Portal) [1]	169
Identification des problèmes	169
Test Portail (console WebSphere Portal) [2]	171
Identification des problèmes	171
Test Process Management (Console Business Process Manager - Business Space)	173
Identification des problèmes	173
Test Gestion de processus (Console Business Process Manager)	176
Identification des problèmes	176
Test Sécurité (console d'administration IBM Security Identity Manager)	177
Identification des problèmes	177
Test Sécurité (console IBM Security Identity Manager).	179
Identification des problèmes	179
Test Sécurité (console en libre service IBM Security Identity Manager)	182
Identification des problèmes	182
Test Sécurité (WebSEAL) [1]	185

Identification des problèmes	185
Test Sécurité (WebSEAL) [2]	186
Identification des problèmes	186
Consignation et analyse des données d'utilisation	188
Journaux d'analyse d'utilisation	188
Exécution de l'outil d'analyse d'utilisation	189
Modification du mot de passe d'installation	190
Modification du mot de passe de topologie	190
Mise à jour du jeton LTPA pour la connexion unique	191
Définition du délai d'expiration de session	192
Définition du délai d'expiration de LTPA	193

Chapitre 4. Traitement des incidents et support 195

Echec du lancement d'IBM Installation Manager	195
Les composants WebSphere ne démarrent pas	195
Impossible de démarrer le serveur LDAP à l'aide de Tivoli Directory Server Web Administration Tool	196

Chapitre 5. Référence 199

Produits et composants installés avec IBM Defense Operations Platform Field Edition	199
Produits et composants installés avec IBM Defense Operations Platform Command Center Edition	199
Ports utilisés par les serveurs Command Center Edition	201
Ports utilisés par les serveurs Field Edition	202
Processus en cours d'exécution dans le compte superutilisateur	202
Accessibilité	203
Mention de droits d'auteur et marques	204
Mention de droits d'auteur	204
Marques	204
Considérations relatives aux règles de confidentialité	204

Remarques 207

Marques	209
-------------------	-----

Index 211

Figures

1. Composants Field Edition.	58	2. Composants Command Center Edition	62
--------------------------------------	----	--------------------------------------	----

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. Présentation de la solution

IBM® Defense Operations Platform est une plateforme interopérable destinée aux organisations militaires et aux Forces Armées.

A travers le monde, les Forces Armées doivent s'adapter à des menaces de plus en plus dynamiques et complexes, tout en étant limitées en termes de ressources. Les organisations militaires sont passées du concept d'opérations en réseau (NCO - Network Centric Operations) au concept d'avantage décisif au combat. Désormais, les responsables militaires s'attachent plus à l'exécution qu'à la gestion réseau. Cette nouvelle tendance favorise l'acquisition de capacités embarquées d'installation rapide. Elles permettent d'augmenter la coordination et le partage d'informations entre les différents services militaires en présence, et avec un vaste réseau de partenaires au sein de la coalition, de fournisseurs et d'organismes externes.

La technologie utilisée par l'Armée doit constituer une aide à la prise de décisions affectant la vie et le bien-être de millions de personnes. Les services du secteur de la Défense sont continuellement à la recherche de nouvelles fonctions capables de réduire les risques encourus. Les innovations technologiques offrent de nouvelles opportunités, mais le déploiement de ces innovations n'a pas été une tâche facile. Du prototype au déploiement réel, plusieurs années peuvent s'écouler. Dans le même temps, la technologie évolue et se développe sur plusieurs générations. Les services de Défense peuvent ainsi manquer d'intéressantes opportunités de réduction des risques pendant ce laps de temps. Dans la course aux nouvelles fonctions demandées sans répit par les utilisateurs, il est souvent inévitable d'opérer certains compromis à un niveau des composants d'applications. Avec des milliers d'applications déployées, il existe fréquemment des milliers de solutions de remplacement au niveau des interactions des utilisateurs avec les informations logicielles et de stockage. Or, une plateforme standard ne permet pas de résoudre un grand nombre de ces difficultés.

A l'heure actuelle, les systèmes militaires sont souvent en silos, et il est difficile de bénéficier de fonctions totalement intégrées. L'interopérabilité doit être réalisée entre les systèmes, au lieu d'être intégrée. Bien sûr, la technologie permet de résoudre les problèmes d'interopérabilité, mais la création d'un environnement technique fiable et sécurisé dans lequel les technologies fonctionnent bien est un processus complexe, onéreux et très consommateur de main d'oeuvre. Un seul changement au niveau d'un noeud est susceptible de rompre l'interopérabilité. La complexité et le coût élevé de ces environnements hétérogènes et personnalisés peuvent constituer des facteurs clés ralentissant la mise à disposition de nouvelles capacités de missions aux Forces Armées.

IBM Defense Operations Platform offre une plateforme interopérable qui diminue considérablement les temps de déploiement des capacités requises pour les missions. Les packages intégrés incluent supports, scripts et instructions détaillées de configuration pour centres de commande, déploiements sur le terrain et mobiles. Grâce à ces packages prédéfinis et pré-testés, l'installation d'IBM Defense Operations Platform ne prend qu'un jour ou deux. Une implémentation rapide dans divers environnements militaires permet aux utilisateurs militaires de se concentrer sur leurs capacités de missions. En effet, l'utilisation d'une plateforme interopérable permet d'éliminer les problèmes de disparité, de duplication et autres problèmes généralement rencontrés en cas d'intégration verticale classique.

IBM Defense Operations Platform s'appuie sur un modèle de sécurité unifié qui offre une approche rigoureuse et cohérente au sein d'une infrastructure de sécurité globale.

Editions d'IBM Defense Operations Platform

IBM Defense Operations Platform a été conçu en vue d'un fonctionnement au sein d'une entreprise de défense. Il existe trois éditions déployables de la plateforme.

Chacune de ces éditions est exécutée au sein du même environnement IBM Defense Operations Platform, ce qui permet le déploiement rapide de nouvelles capacités (ou de capacités mises à jour) et garantit l'intégrité des communications. IBM Defense Operations Platform a été conçu de façon à fournir un grand nombre de services réutilisables à architecture SOA (Service Oriented Architecture) du secteur de la Défense (OTAN, par exemple, ou encore normes applicables au sein du Ministère de la Défense) ; cette plateforme peut être totalement intégrée aux nouveaux systèmes ou aux systèmes existants compatibles.

Command Center Edition

Command Center Edition est particulièrement destiné aux unités dotées d'importantes capacités d'infrastructure (départements exécutifs, bases d'opérations avancées ou navires de défense, par exemple).

Field Edition

Field Edition est particulièrement destiné aux unités en transit (navires de taille réduite, véhicules terrestres, postes de commande mobiles et embarqués, par exemple).

Mobile Edition

Mobile Edition est particulièrement destiné aux soldats, pour permettre un accès mobile (installations de véhicules tactiques, ordinateurs portables et PDA (Personal Digital Assistance), par exemple).

Workbench Edition

Workbench Edition fournit un ensemble d'outils pour concevoir, mettre au point, implémenter, construire, tester, déployer et gérer des fonctions de mission telles que des applications et des services sur Command Center Edition, Field Edition et Mobile Edition. Grâce à ces outils, Workbench Edition fournit un environnement de développement permettant rapidement de créer, déployer et gérer des fonctions de mission.

Workbench Edition requiert Command Center Edition en tant qu'environnement d'exécution de développement.

Editions mises à jour (IBM Defense Operations Platform 1.6)

La version IBM Defense Operations Platform 1.6 contient des mises à jour de Command Center Edition, Field Edition, et Workbench Edition. Aucune mise à jour n'est fournie pour Mobile Edition.

Nouveautés de la version 1.6

IBM Defense Operations Platform 1.6 offre un support de plateforme actualisé et contient des outils supplémentaires.

Outre la mise à jour des produits dans les versions actuelles, IBM Defense Operations Platform offre trois nouveaux outils :

Outil de contrôle de plateforme

L'outil de contrôle de plateforme permet à un administrateur de démarrer, d'arrêter et d'interroger le statut des services et des composants IBM Defense Operations Platform à l'aide d'un seul outil. L'administrateur n'a pas besoin de connaître les différents services d'administration fournis par les produits accompagnant IBM Defense Operations Platform. La syntaxe de l'outil de contrôle de plateforme est similaire pour tous les produits IBM Defense Operations Platform.

Outil de gestion des mots de passe

IBM Defense Operations Platform contient une version de IBM Security Identity Manager qui permet aux utilisateurs et aux administrateurs de gérer les ID utilisateurs et les ID d'applications.

Cet outil est fourni pour faciliter la gestion des mots de passe et pour permettre la création et la gestion des comptes utilisateurs sur plusieurs systèmes. Il offre également des capacités d'audit. Par exemple, l'outil de gestion des mots de passe permet aux administrateurs de changer facilement les mots de passe des administrateurs ou des comptes d'administration requis par les produits sous-jacents d'IBM Defense Operations Platform.

Outil d'analyse d'utilisation

IBM Defense Operations Platform consigne les données d'utilisation qui peuvent ensuite être traitées à l'aide d'une application d'analyse d'utilisation.

Services système IBM Defense Operations Platform

Les serveurs IBM Defense Operations Platform proposent de nombreux services.

Services d'analyse

Fournit des services d'analyse de données, de présentation et de génération de rapports.

Services d'assurance qualité d'applications

Fournit des services de gouvernance, d'automatisation et de collaboration applicables aux informations de projets et aux mises à jour de statuts lors du cycle de vie de développement.

Services de développement et de conception d'applications

Fournit des services destinés à la gestion des éléments de travail, activités de projets, tableaux de bord et rapports d'avancement, planifications, contrôles des sources et configurations logicielles.

Services de gestion et de déploiement d'applications

Fournit des services destinés à la gestion et au déploiement de logiciels.

Services d'application

Fournit des services Java™ Enterprise Edition qui prennent en charge la solution.

Services d'authentification et d'autorisation

Fournit des services d'authentification et d'autorisation à la solution, aux applications, et à d'autres services.

Services de surveillance des activités métier

Services qui fournissent l'agrégation, l'analyse et la présentation des informations sur les activités et les processus métier en temps réel.

Services de collaboration

Fournit des services qui permettent la collaboration en temps réel pour les utilisateurs et les applications.

Services de configuration

Services qui gèrent la configuration du produit, notamment l'inventaire et la gestion des changements.

Services de base de données

Fournit les services de base de données pour la solution et les applications.

Services de gestion des identités

Fournit des services pour gérer les ID utilisateur final et application IBM Defense Operations Platform.

Services d'installation

Fournit des services pour installer IBM Defense Operations Platform.

Services de messagerie

Fournit des services de messagerie et de flux de travaux.

Services mobiles

Fournit des services permettant d'activer les utilisateurs nomades.

Services de gestion des mots de passe

Fournit des services pour gérer les mots de passe de la solution.

Services de gestion de plateforme

Fournit des services de gestion d'exécution comprenant la capacité de démarrer, d'arrêter, et d'interroger le statut de services et de composants IBM Defense Operations Platform.

Services d'utilisation de plateforme

Fournit des services pour analyser l'utilisation de la solution.

Services de procédure standard d'exploitation

Fournit des services de gestion du traitement des procédures standard d'exploitation.

Services d'analyse de l'utilisation

Ces services permettent la consignation des données d'utilisation comme la connexion, la déconnexion de l'utilisateur, le délai d'attente et les incidents de connexion.

Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe

Permet la synchronisation de mots de passe. Les changements de mot de passe sont alors interceptés au niveau des noeuds finals et réacheminés vers les services de gestion des identités.

Services d'interface utilisateur

Services qui prennent en charge l'interaction d'utilisateur avec le produit.

Services d'annuaire utilisateur et d'intégration d'annuaire utilisateur

Fournit un mappage entre les noms d'utilisateur et de groupe et des valeurs, ainsi que l'intégration avec des annuaires supplémentaires.

Services Web

Fournit HTTP, HTTPS et d'autres services Web à la solution.

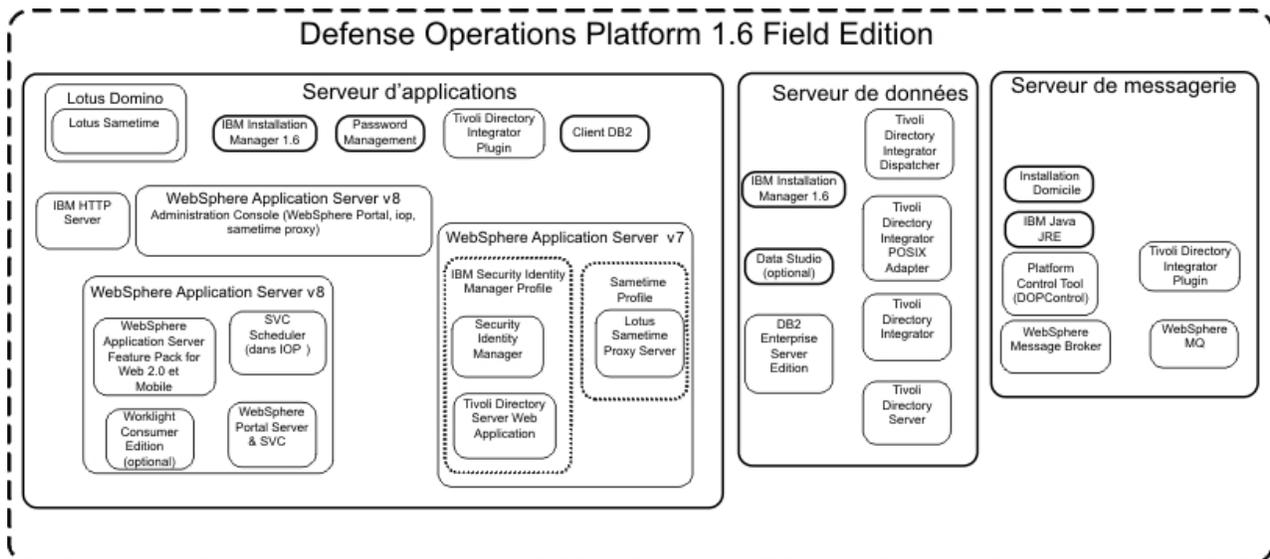
Le service suivant n'est disponible que si l'outil Data Studio facultatif est installé.

Services de conception de données

Fournit des fonctions de conception de données aux générateurs d'application.

Serveurs IBM Defense Operations Platform dans Field Edition

IBM Defense Operations Platform est installé sur trois serveurs dans Field Edition.



Serveur d'applications

Ce serveur fournit les services suivants :

- Services d'application
- Services de surveillance des activités métier
- Services d'interface utilisateur
- Services de collaboration
- Services mobiles
- Services de gestion des identités
- Services d'authentification
- Services de gestion des mots de passe
- Services d'utilisation de plateforme
- Services d'indicateurs clés de performance
- Services de versement d'événement
- Services de procédure standard d'exploitation
- Services d'analyse de l'utilisation
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe

Serveur de données

Ce serveur fournit les services suivants :

- Services de base de données
- Services de conception de données
- Services d'annuaire utilisateur
- Services d'intégration d'annuaire utilisateur
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe

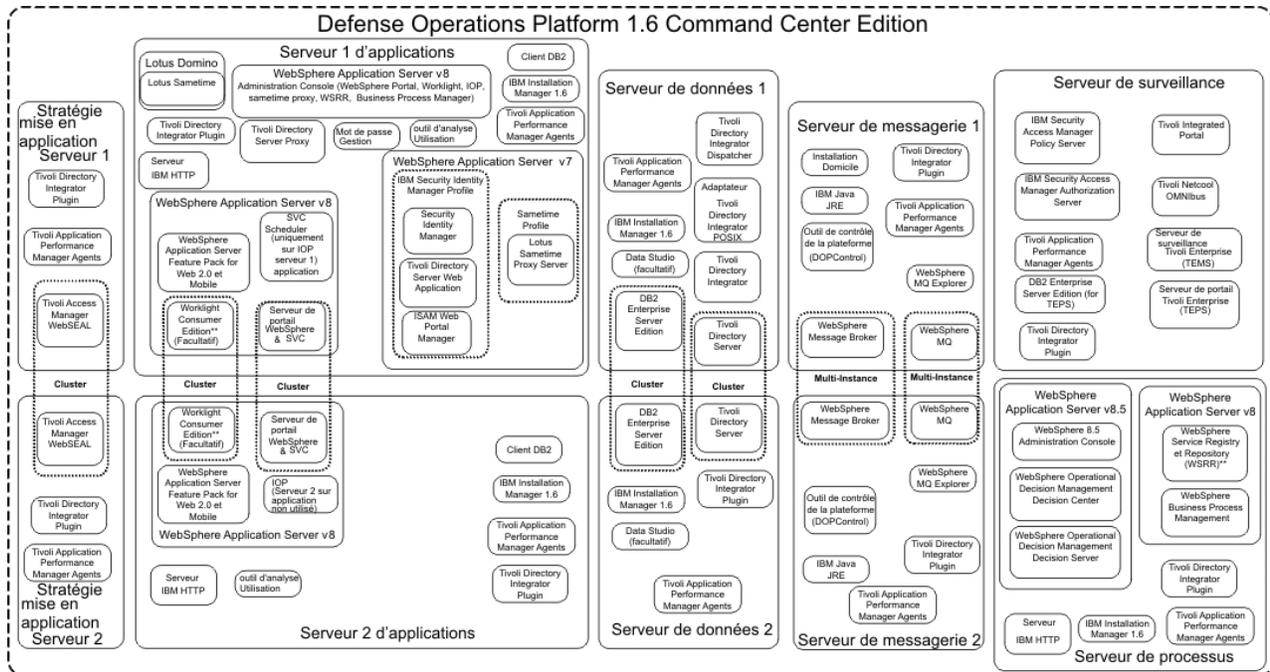
Serveur de messagerie

Ce serveur fournit les services suivants :

- Services d'installation
- Services de messagerie
- Services d'analyse
- Services de gestion de plateforme
- Services de messagerie
- Services de génération de rapports
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe

Serveurs IBM Defense Operations Platform dans Command Center Edition

IBM Defense Operations Platform est installé sur dix serveurs dans Command Center Edition.



Serveur d'applications 1

Ce serveur fournit les services suivants :

- Services d'application
- Services de surveillance des activités métier
- Services d'interface utilisateur
- Services de collaboration
- Services mobiles
- Services de gestion des identités
- Services d'authentification
- Services de gestion des mots de passe
- Services d'utilisation de plateforme
- Services d'indicateurs clés de performance
- Services de versement d'événement
- Services de procédure standard d'exploitation
- Services d'analyse de l'utilisation
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur d'applications 2

Ce serveur fournit les services suivants :

- Services d'application
- Services de surveillance des activités métier
- Services d'interface utilisateur

- Services mobiles
- Services d'authentification
- Services d'utilisation de plateforme
- Services d'indicateurs clés de performance
- Services de versement d'événement
- Services de procédure standard d'exploitation
- Services d'analyse de l'utilisation
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur de données 1

Ce serveur fournit les services suivants :

- Services de base de données
- Services de conception de données
- Services d'annuaire utilisateur
- Services d'intégration d'annuaire utilisateur
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur de données 2

Ce serveur fournit les services suivants :

- Services de base de données
- Services de conception de données
- Services d'annuaire utilisateur
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur de messagerie 1

Ce serveur fournit les services suivants :

- Services d'installation
- Services de messagerie
- Services d'analyse
- Services de gestion de plateforme
- Services de génération de rapports
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur de messagerie 2

Ce serveur fournit les services suivants :

- Services d'installation
- Services de messagerie
- Services d'analyse
- Services de gestion de plateforme
- Services de génération de rapports
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur d'application des règles 1

Ce serveur fournit les services suivants :

- Services du proxy inverse

- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur d'application des règles 2

Ce serveur fournit les services suivants :

- Services du proxy inverse
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services de l'agent de surveillance

Serveur de surveillance

Ce serveur fournit les services suivants :

- Services de surveillance des processus
- Services de gestion des événements
- Services de surveillance système
- Services d'entreprise de gestion système
- Services d'entreprise d'administration de gestion système
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services serveur de règles Access Manager
- Services serveur d'autorisations Access Manager
- Services de l'agent de surveillance
- Services de base de données

Serveur de processus

Ce serveur fournit les services suivants :

- Services de workflow de processus
- Services de gestion des tâches humaines
- Services de centre opérationnel de décisions
- Services serveur de centre opérationnel de décisions
- Intégration d'annuaire utilisateur - services du plug-in de synchronisation de mots de passe
- Services proxy d'annuaire d'utilisateurs
- Services de gestion des processus métier
- Services de référentiel et de registre de services
- Services de l'agent de surveillance

Configuration matérielle requise pour IBM Defense Operations Platform pour Field Edition

Trois serveurs conformes à la configuration minimale requise sont nécessaires pour installer IBM Defense Operations Platform Field Edition. Le serveur de messagerie sert également de serveur d'installation.

Le serveur doit être doté de processeurs Intel x86-64 ou AMD x86-64.

La configuration minimale requise pour les serveurs utilisés par IBM Defense Operations Platform est décrite dans le tableau 1. L'espace disque minimal recommandé n'inclut pas l'espace pour les partitions d'amorçage et de permutation. Ces répertoires doivent être définis avant d'installer IBM Defense Operations Platform.

Tableau 1. Configuration matérielle minimale requise

Modèle	Serveur d'applications	Serveur de messagerie	Serveur de données
Unités centrales	4	4	4

Tableau 1. Configuration matérielle minimale requise (suite)

Modèle	Serveur d'applications	Serveur de messagerie	Serveur de données
Mémoire	14 Go	8 Go	8 Go
Adaptateurs de réseau	1	1	1
Espace disque	93 Go	93 Go	115 Go
Espace disque supplémentaire requis pendant l'installation	90 Go	37 Go (139 Go si le support de téléchargement doit être stocké sur le serveur)	17 Go

Pour des utilisations de développement et hors environnements de production, en cas d'utilisation peu intensive, la mémoire serveur de messagerie peut être de 4 Go et la mémoire serveur de données peut être de 6 Go.

La configuration minimale requise pour les répertoires sur chaque serveur, à l'exclusion de l'espace requis pour les partitions d'amorçage et de permutation, est présentée dans le tableau 2.

Tableau 2. Espace minimal requis pour chaque répertoire

Répertoire	Espace minimal	Remarques
/	8 go	
/opt	32 Go	
/usr	8 go	
/home	5 Go	
/tmp	12 Go	
/chroot	1 Go	
/datahome	22 Go	Requis uniquement sur serveur de données.
/loghome	8 go	
/installMedia	17 Go, 37 Go, ou 90 Go	<p>Ce répertoire peut porter un autre nom. Toutefois, s'il porte un autre nom, il doit être défini dans le fichier de propriétés d'installation. Ce répertoire peut être supprimé après l'installation.</p> <p>La quantité d'espace requise dépend du serveur.</p> <ul style="list-style-type: none"> • Serveur de données : 17 Go • Serveur de messagerie : 37 Go • Serveur d'applications : 90 Go
/distributionMedia	102 Go	Ce répertoire peut porter un autre nom. Toutefois, s'il porte un autre nom, il doit être défini dans le fichier de propriétés d'installation. Ce répertoire n'est obligatoire que sur le serveur d'installation
/var	8 go	
/SWAP	8 go	

Configuration matérielle requise pour IBM Defense Operations Platform dans Command Center Edition

Dix serveurs conformes à la configuration minimale requise sont nécessaires pour installer IBM Defense Operations Platform Command Center Edition. Le Serveur de messagerie 1 sert également de serveur d'installation.

Le serveur doit être doté de processeurs Intel x86-64 ou AMD x86-64.

La configuration minimale requise pour les serveurs utilisés par IBM Defense Operations Platform est décrite dans le tableau 3. L'espace disque minimal recommandé n'inclut pas l'espace pour les partitions d'amorçage et de permutation.

Important : La configuration du serveur de données 1 et du serveur de données 2 doivent être virtuellement identiques. La configuration inclut le matériel, le niveau du système d'exploitation et les modules de correction, les périphériques réseau, et les versions de base de données. Le fait de rendre ces serveurs aussi identiques que possible favorisera le bon fonctionnement d'un procédé de reprise en ligne de la base de données en cas de besoin.

Tableau 3. Configuration matérielle minimale requise

Modèle	Serveur d'applications 1	Serveur d'applications 2	Serveur de messagerie 1	Serveur de messagerie 2	Serveur de données 1	Serveur de données 2	Serveur d'application des règles 1	Serveur d'application des règles 2	Serveur de surveillance	Serveur de processus
Unités centrales	4	4	4	4	4	4	1	1	4	4
Mémoire	14 Go	14 Go	8 Go	8 Go	10 Go	10 Go	1 Go	1 Go	8 Go	8 Go
Adaptateurs de réseau	1	1	1	1	1	1	1	1	1	1
Espace disque	103 Go	93 Go	115 Go	115 Go	115 Go	115 Go	63 Go	63 Go	93 Go	93 Go
Espace disque supplémentaire requis pendant l'installation	95 Go	70 Go	37 Go (182 Go si le support de téléchargement doit être stocké sur le serveur)	37 Go	27 Go	27 Go	27 Go	27 Go	85 Go	90 Go

La configuration minimale requise pour les répertoires sur chaque serveur, à l'exclusion de l'espace requis pour les partitions d'amorçage et de permutation, est présentée dans le tableau 4.

Tableau 4. Espace minimal requis pour chaque répertoire

Répertoire	Espace minimal	Remarques
/	8 Go	
/opt	32 Go	
/usr	8 Go	
/home	5 Go	
/tmp	12 Go	
/chroot	1 Go	
/datahome	22 Go, 10 Go	Requis uniquement sur le serveur d'applications 1 (10 Go), serveur d'applications 2 (10 Go), serveur de messagerie 1 (22 Go), serveur de messagerie 2 (22 Go), serveur de données 1 (22 Go), serveur de données 2 (22 Go).
/loghome	8 Go	

Tableau 4. Espace minimal requis pour chaque répertoire (suite)

Répertoire	Espace minimal	Remarques
/installMedia	90 Go, 85 Go, 37 Go, 27 Go, 95 Go, 70 Go	<p>Ce répertoire peut porter un autre nom. Toutefois, si le répertoire porte un autre nom, il doit être défini dans le fichier de propriétés d'installation. Ce répertoire peut être supprimé après l'installation.</p> <p>La quantité d'espace requise dépend du serveur.</p> <ul style="list-style-type: none"> • Serveur de processus: 90Go • Serveur de surveillance: 85 Go • Serveur de données : 27 Go • Serveur d'application des règles : 27 Go • Serveur de messagerie : 37 Go • Serveur d'applications 1: 95 Go • Serveur d'applications 2 : 70 Go
/distributionMedia	142 Go	Ce répertoire peut porter un autre nom. Toutefois, si le répertoire porte un autre nom, il doit être défini dans le fichier de propriétés d'installation. Ce répertoire n'est obligatoire que sur le serveur d'installation
/var	8 Go	
/SWAP	8 Go	

Par ailleurs, une infrastructure à équilibrage de charge est requise pour la connexion au serveur d'application des règles.

Configuration des logiciels prérequis

Avant d'installer IBM Defense Operations Platform, vous devez avoir installé les logiciels appropriés sur tous les serveurs.

IBM Defense Operations Platform nécessite Red Hat Enterprise Server Linux version 6 (6.3 ou supérieure). Des packages RPM Linux spécifiques doivent être installés dans le cadre de la procédure de préparation des serveurs.

Un poste de travail avec Windows est également nécessaire pour configurer la connexion unique pour les services de collaboration.

Il est recommandé de n'installer sur les serveurs que les logiciels prérequis. Toute installation d'IBM Defense Operations Platform effectuée sur les serveurs doit être supprimée avant d'installer IBM Defense Operations Platform.

Tâches associées:

«Installation des packages Linux pour Field Edition», à la page 22

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

«Installation des packages Linux pour Command Center Edition», à la page 25

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

«Configuration de la connexion unique pour les services de collaboration», à la page 48

Importez le jeton LTPA SSO WebSphere Portal sur le serveur d'applications pour permettre aux utilisateurs d'accéder aux services de collaboration sans avoir à saisir à nouveau leurs données d'identification.

Chapitre 2. Installation et configuration

IBM Defense Operations Platform fournit des options d'installation permettant d'installer l'environnement du produit et l'application. Après avoir installé IBM Defense Operations Platform, plusieurs étapes de configuration supplémentaires sont requises.

Serveur d'installation

Le serveur utilisé lors de l'installation de l'IBM Defense Operations Platform dépend de l'environnement dans lequel IBM Defense Operations Platform est installé pour Command Center Edition ou Field Edition.

Pour Field Edition, le serveur d'installation est serveur de messagerie.

Pour Command Center Edition, le serveur d'installation est le serveur de messagerie 1.

Listes de contrôle d'installation

Des listes de contrôle sont disponibles pour les options d'installation d'IBM Defense Operations Platform. Ces listes fournissent un aperçu des étapes d'installation et permettent d'en suivre la progression.

Liste de contrôle - installation de IBM Defense Operations Platform Field Edition

Utilisez cette liste de contrôle pour suivre les étapes d'installation de IBM Defense Operations Platform Field Edition.

Procédure

- 1. Examinez la note technique sur la planification de la maintenance préventive d'IBM Defense Operations Platform afin d'identifier les changements apportés à la documentation du produit qui pourraient affecter l'installation et l'utilisation d'IBM Defense Operations Platform.
- 2. Vérifiez que vous disposez du matériel nécessaire.
- 3. Vérifiez que les logiciels requis sont bien installés sur le matériel.
- 4. Facultatif : Utilisez le fichier de démarrage pour préparer Red Hat Enterprise Linux sur les serveurs. La préparation du système d'exploitation peut également être faite manuellement dans le cadre des étapes de la procédure de préparation des serveurs.
- 5. Préparez les serveurs.
 - a. Configurez la mise en réseau TCP/IP.
 - b. Désactivez les paramètres de sécurité.
 - c. Configurez les services SSH.
 - d. Installez les packages Linux obligatoires.
 - e. Définissez d'autres exigences de préinstallation.
 - f. Préparez le serveur d'installation
- 6. Vérifiez et personnalisez les propriétés d'installation, si nécessaire.
- 7. Définissez la topologie de l'installation en éditant le fichier de propriétés de la topologie.
- 8. Exécutez le programme d'installation de ligne de commande.

Important : Vérifiez que vous enregistrez le mot de passe d'installation. Toutes les tâches relatives à l'installation nécessitent le mot de passe d'installation. Le mot de passe d'installation est également le mot de passe de topologie initial nécessaire lors de l'exécution de l'outil de gestion

des mots de passe et deoutil de contrôle de plateforme. Le mot de passe de topologie peut être modifié. Le mot de passe de topologie et d'installation par défaut est ibmdop16.

- ___ 9. Vérifiez l'installation avant de configurer IBM Defense Operations Platform.
- ___ 10. Configurez IBM Defense Operations Platform.
 - ___ a. Configurez la connexion unique pour les services de collaboration.
 - ___ b. Configurez le nom d'hôte de l'outil d'administration Web Tivoli Directory Server
 - ___ c. Facultatif : Activez la journalisation Tivoli Directory Server
 - ___ d. Facultatif : Configurez le délai d'attente de session.
 - ___ e. Facultatif : Configurez le délai d'attente LTPA.
- ___ 11. Vérifiez que IBM Defense Operations Platform est correctement installé.
- ___ 12. Installez toutes les autres applications.

Résultats

L'architecture d'IBM Defense Operations Platform est installée et prête à l'utilisation.

Liste de contrôle - installation de IBM Defense Operations Platform Command Center Edition

Utilisez cette liste de contrôle pour suivre les étapes d'installation de IBM Defense Operations Platform Command Center Edition.

Procédure

- ___ 1. Examinez la note technique sur la planification de la maintenance préventive d'IBM Defense Operations Platform afin d'identifier les changements apportés à la documentation du produit qui pourraient affecter l'installation et l'utilisation d'IBM Defense Operations Platform.
- ___ 2. Vérifiez que vous disposez du matériel nécessaire.
- ___ 3. Vérifiez que les logiciels requis sont bien installés sur le matériel.
- ___ 4. Facultatif : Utilisez le fichier de démarrage pour préparer Red Hat Enterprise Linux sur les serveurs. La préparation du système d'exploitation peut également être faite manuellement dans le cadre des étapes de la procédure de préparation des serveurs.
- ___ 5. Préparez les serveurs.
 - a. Configurez la mise en réseau TCP/IP.
 - b. Désactivez les paramètres de sécurité.
 - c. Configurez les services SSH.
 - d. Installez les packages Linux obligatoires.
 - e. Définissez d'autres exigences de préinstallation.
 - f. Préparez les serveurs en vue de leur exécution dans un environnement à haute disponibilité.
 - g. Préparez le serveur d'installation
- ___ 6. Vérifiez et personnalisez les propriétés d'installation, si nécessaire.
- ___ 7. Définissez la topologie de l'installation en éditant le fichier de propriétés de la topologie.
- ___ 8. Exécutez le programme d'installation de ligne de commande.

Important : Vérifiez que vous enregistrez le mot de passe d'installation. Toutes les tâches relatives à l'installation nécessitent le mot de passe d'installation. Le mot de passe d'installation est également le mot de passe de topologie initial nécessaire lors de l'exécution de l'outil de gestion des mots de passe et deoutil de contrôle de plateforme. Le mot de passe de topologie peut être modifié. Le mot de passe de topologie et d'installation par défaut est ibmdop16.

- ___ 9. Vérifiez l'installation avant de configurer IBM Defense Operations Platform.
- ___ 10. Configurez IBM Defense Operations Platform.

- __ a. Configurez la connexion unique pour les services de collaboration.
 - __ b. Configurez les relations des gestionnaires de grappes supplémentaires.
 - __ c. Facultatif : Configurez le délai d'attente de session.
 - __ d. Facultatif : Configurez le délai d'attente LTPA.
 - __ e. Facultatif : Configurez un système de fichiers NFS externe facultatif.
- __ 11. Vérifiez que IBM Defense Operations Platform est correctement installé.
- __ 12. Installez toutes les autres applications.

Résultats

L'architecture d'IBM Defense Operations Platform est installée et prête à l'utilisation.

Utilisation des fichiers de démarrage pour préparer Red Hat Enterprise Linux

IBM Defense Operations Platform inclut un exemple de fichier de démarrage Red Hat Enterprise Linux V6 pour préparer le système d'exploitation pour les serveurs virtuels ou matériels.

Pourquoi et quand exécuter cette tâche

La configuration requise pour le serveur IBM Defense Operations Platform suppose que l'option d'installation minimale est sélectionnée au cours de l'installation de Red Hat Enterprise Linux. L'option minimale fournit uniquement les packages @core et @server-policy qui sont essentiels pour exécuter Red Hat Enterprise Linux. Les packages @core et @server-policy fournissent les packages RPM Linux requis pour un dispositif de serveur ou de bureau à fonction unique et maximisent les performances et la sécurité pour l'installation. Les fichiers de démarrage inclus avec IBM Defense Operations Platform comprennent tous les packages requis pour IBM Defense Operations Platform et peuvent être utilisés pour préparer les serveurs en vue de l'installation.

Les fichiers de démarrage peuvent être trouvés dans le répertoire /rhel-kickstart sur le support d'installation.

Les fichiers de démarrage fournis pour Field Edition sont :

- d2_ks-dopmsg-min.cfg - fichier de démarrage pour le serveur de messagerie
- d2_ks-dopapp-min.cfg - fichier de démarrage pour le serveur d'applications
- d2_ks-dopdb-min.cfg - fichier de démarrage pour le serveur de données

Les fichiers de démarrage fournis pour Command Center Edition sont :

- d1_ks-dopmsg1-min.cfg - fichier de démarrage pour le serveur de messagerie 1
- d1_ks-dopmsg2-min.cfg - fichier de démarrage pour le serveur de messagerie 2
- d1_ks-dopapp1-min.cfg - fichier de démarrage pour le serveur d'applications 1
- d1_ks-dopapp2-min.cfg - fichier de démarrage pour le serveur d'applications 2
- d1_ks-dopdb1-min.cfg - fichier de démarrage pour le serveur de données 1
- d1_ks-dopdb2-min.cfg - fichier de démarrage pour le serveur de données 2
- d1_ks-dopdmz1-min.cfg - fichier de démarrage pour le serveur d'application des règles 1
- d1_ks-dopdmz2-min.cfg - fichier de démarrage pour le serveur d'application des règles 2
- d1_ks-doppro-min.cfg - fichier de démarrage pour le serveur de processus
- d1_ks-dopmon-min.cfg - fichier de démarrage pour le serveur de surveillance

Procédure

Installez chaque fichier de démarrage.

1. Editez le fichier de démarrage.
 2. Définissez la valeur `lang` sur la langue utilisée pour votre installation. La valeur par défaut est `en_US.UTF-8`.
 3. Définissez la valeur `rootpw` sur le mot de passe `root` du système. La valeur par défaut est `ibmdop16`.
 4. Définissez la valeur `timezone` sur le fuseau horaire correspondant à votre installation. La valeur par défaut est `America/New_York`.
 5. Modifiez l'information `network` pour le système cible. La valeur par défaut est différente pour chaque serveur.
 6. Facultatif : Modifiez l'agencement de partition du système de fichiers. Dans la configuration par défaut, toutes les partitions du système de fichiers sont créées sur un disque.
- Utilisez le fichier de démarrage pour configurer le serveur ou la machine virtuelle.
7. Terminez les étapes de pré-installation dans le fichier de démarrage.
 8. Utilisez le fichier de démarrage pour installer et configurer Red Hat Enterprise Linux sur le serveur matériel ou la machine virtuelle.
 9. Terminez les étapes de post-installation dans le fichier de démarrage.
 10. Créez une image instantanée de la machine virtuelle ou une sauvegarde du serveur matériel.

Que faire ensuite

Une fois que le système d'exploitation est configuré sur tous les serveurs matériels ou machines virtuelles à l'aide des fichiers de démarrage, continuez les autres étapes de préparation des serveurs. Les fichiers de démarrage installent les packages Linux requis ; ces étapes peuvent donc être ignorées. Une fois que les serveurs sont préparés, installez IBM Defense Operations Platform.

Tâches associées:

«Préparation des serveurs»

Avant d'installer IBM Defense Operations Platform, tous les serveurs doivent être correctement préparés, sinon l'installation échouera. L'étape de pré-contrôle vérifiera que la plupart de ces exigences ont été mises en oeuvre pour l'ensemble des serveurs.

«Installation des packages Linux pour Field Edition», à la page 22

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

«Installation des packages Linux pour Command Center Edition», à la page 25

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

Préparation des serveurs

Avant d'installer IBM Defense Operations Platform, tous les serveurs doivent être correctement préparés, sinon l'installation échouera. L'étape de pré-contrôle vérifiera que la plupart de ces exigences ont été mises en oeuvre pour l'ensemble des serveurs.

Pourquoi et quand exécuter cette tâche

Dans un environnement virtuel, l'utilisation d'un modèle pour ces étapes peut vous aider à réduire le temps de configuration. Suivez les étapes de chaque section pour chaque serveur ou créez un modèle RHEL en suivant ces étapes.

Configuration du réseau TCP/IP

Avant d'installer IBM Defense Operations Platform, le réseau TCP/IP doit être configuré sur les serveurs.

Pourquoi et quand exécuter cette tâche

Si vous installez IBM Defense Operations Platform Command Center Edition, vous devez utiliser IPv4. Le groupement de serveurs à haute disponibilité ne prend pas en charge IPv6.

Les réseaux IPv6 sont pris en charge par IBM Defense Operations Platform Field Edition, mais les réseaux IPv4 doivent également être installés et configurés. Il est inutile d'affecter des adresses IPv4 aux serveurs, mais l'adresse de bouclage IPv4 (127.0.0.1) doit être activée et le nom d'hôte localhost doit résoudre l'adresse 127.0.0.1.

Les changements de configuration sont présentés dans le tableau 5, à la page 18. Configurez la gestion réseau TCP/IP sur le IBM Defense Operations Platform serveur d'installation et sur les serveurs cible en éditant les fichiers de configuration réseau Linux. Les notes de configuration présentées dans le tableau 5, à la page 18 sont données à titre informatif uniquement. Toute configuration réseau conforme à la configuration requise décrite précédemment devrait fonctionner.

Tableau 5. Instructions de configuration TCP/IP

Fichier	Remarques
/etc/hosts	<p>Le fichier hosts résout les noms TCP/IP en adresses IP. Si la configuration ne comporte pas de serveur DNS, tous les serveurs et leurs adresses IP, noms d'hôte abrégés et noms qualifiés complets doivent être définis dans ce fichier. Les adresses de bouclage locales et les noms d'hôte doivent également y être définis.</p> <p>Si un serveur DNS est utilisé, les hôtes qui sont résolus par ce système DNS n'ont pas besoin de figurer dans ce fichier.</p> <p>Important : Lors de l'utilisation d'IPv4, l'adresse de bouclage locale 127.0.0.1 doit être mappée aux noms d'hôte localhost et localhost.localdomain.</p> <p>Voici un exemple de fichier /etc/hosts utilisant des adresses IPv4.</p> <pre># local loopback definitions -- do not remove # or alter these! 127.0.0.1 localhost.localdomain localhost # use the following if IPv6 is enabled in your # network definitions ::1 localhost6.localdomain localhost6 # target runtime servers for the Field Edition 192.168.0.211 dopapp.dop16.com dopapp 192.168.0.212 dopdb.dop16.com dopdb 192.168.0.213 dopmsg.ioc16.com dopmsg # target runtime servers for the # Command Center Edition 192.168.0.214 doppel1.dop16.com doppel1 192.168.0.215 doppel2.dop16.com doppel2 192.168.0.216 dopapp1.dop16.com dopapp1 192.168.0.217 dopapp2.dop16.com dopapp2 192.168.0.218 dopdb1.dop16.com dopdb1 192.168.0.219 dopdb2.dop16.com dopdb2 192.168.0.220 dopana1.dop16.com dopana1 192.168.0.221 dopana2.dop16.com dopana2 192.168.0.222 dopmon.dop16.com dopmon 192.168.0.223 doppro.dop16.com doppro</pre> <p>Utilisez la notation d'adresse IPv6 pour affecter des adresses IPv6 statiques.</p> <p>Les adresses IPv6 et IPv4 peuvent être définies sur le même serveur.</p>

Tableau 5. Instructions de configuration TCP/IP (suite)

Fichier	Remarques
/etc/sysconfig/network-scripts/ifcfg- <i>nom_adaptateur</i>	<p>Le fichier <i>ifcfg-nom_adaptateur</i> définit les paramètres réseau de base pour l'adaptateur de réseau indiqué. Le nom Linux affecté à l'adaptateur de réseau est indiqué par <i>nom_adaptateur</i>. La valeur standard pour <i>nom_adaptateur</i> est <i>eth0</i>, mais elle peut être différente pour votre environnement.</p> <p>Pour le réseau IPv4, les paramètres suivants doivent être définis.</p> <p>IPADDR Indiquez l'adresse IP IPv4 du serveur en cours de configuration.</p> <p>NETMASK Indiquez le masque de réseau IPv4 du serveur en cours de configuration.</p> <p>GATEWAY Indiquez l'adresse IP IPv4 par défaut du serveur en cours de configuration.</p> <p>BOOTPROTO Si l'adressage IP statique est utilisé, indiquez <i>none</i>.</p> <p>NM_CONTROLLED Indiquez <i>no</i> pour désactiver le service de gestion des réseaux et l'empêcher de modifier le fichier <i>ifcfg-nom_adaptateur</i>.</p> <p>ONBOOT Indiquez <i>yes</i> pour démarrer l'adaptateur automatiquement.</p> <p>IPV6INIT Indiquez <i>yes</i> si l'adaptateur doit utiliser le réseau IPv6.</p> <p>IPV6ADDR Indiquez l'adresse IP IPv6 du serveur si <i>IPV6INIT=yes</i> est spécifié.</p> <p>IPV6_DEFAULTGW Indiquez l'adresse IP de passerelle du réseau IPv6 du serveur si <i>IPV6INIT=yes</i> est spécifié.</p>

Tableau 5. Instructions de configuration TCP/IP (suite)

Fichier	Remarques
/etc/sysconfig/network	<p>Le fichier network spécifie des paramètres réseau généraux.</p> <p>Pour les réseaux IPv4, les paramètres suivants doivent être définis :</p> <p>NETWORKING Indiquez <code>yes</code> pour activer les réseaux IPv4.</p> <p>NETWORKING_IPV6 Indiquez <code>yes</code> si les réseaux IPv6 sont également souhaités.</p> <p>HOSTNAME Indiquez le nom d'hôte abrégé du serveur.</p> <p>Les changements de configuration du nom d'hôte effectués en éditant le fichier /etc/sysconfig/network ne s'appliqueront pas tant que le serveur n'est pas redémarré. Si le redémarrage n'est pas souhaité, modifiez le nom d'hôte de la session shell en exécutant la commande <code>hostname nouveau_nom_hôte</code>. Par exemple, pour modifier le nom d'hôte du serveur en <code>dopweb</code>, exécutez la commande <code>hostname dopweb</code>.</p>
/etc/resolv.conf	<p>Le fichier resolv.conf permet de définir des serveurs DNS pour le réseau et un domaine de recherche par défaut. Si les serveurs DNS ne sont pas utilisés, ce fichier doit être vide. Si les deux serveurs DNS et /etc/hosts sont utilisés, la priorité de fichier est spécifiée dans le fichier /etc/nsswitch.conf.</p> <p>Si un serveur DNS est utilisé, le fichier resolv.conf doit contenir les lignes suivantes :</p> <pre>search domain_name nameserver first_DNS_server nameserver second_DNS_server</pre> <p>Exemple :</p> <pre>search yourcompany.com nameserver 10.75.20.10 nameserver 10.75.20.11</pre> <p>La valeur <code>search</code> indique le domaine de recherche par défaut. La première valeur <code>nameserver</code> correspond à l'adresse IP du serveur DNS. La seconde valeur <code>nameserver</code> peut être utilisée pour indiquer un serveur DNS secondaire. La seconde spécification <code>nameserver</code> est facultative.</p>

Procédure

1. Définissez un nom qualifié complet et un nom d'hôte abrégé en utilisant un serveur DNS ou le fichier /etc/hosts. Les noms d'hôte doivent résoudre l'adresse IP correcte sur chaque serveur.

Le nom d'hôte qualifié complet de chaque serveur doit comporter au moins trois composantes. Par exemple : `myhost.mydomain.com`, où le domaine de niveau supérieur est un domaine de haut niveau Internet standard.

Important : Les noms d'hôte abrégés et les noms d'hôte qualifiés complets doivent être indiqués dans la casse correcte. Par exemple, MyCompany.MyDomain.com n'est pas équivalent à mycompany.mydomain.com.

2. (Pour Command Center Edition uniquement) Assurez-vous que le HOSTNAME défini dans /etc/sysconfig/network est défini sur le nom d'hôte abrégé et non pas sur le nom d'hôte qualifié complet. Par exemple, définissez HOSTNAME=xyz au lieu de HOSTNAME=xyz.yourco.com.
3. Vérifiez que le nom d'hôte, le nom d'hôte qualifié complet et les noms de domaine sont configurés sur tous les serveurs. Les serveurs sont correctement configurés si les tests suivants réussissent.
 - a. La commande **hostname -s** renvoie le nom d'hôte abrégé défini pour le serveur.
 - b. La commande **hostname -f** renvoie le domaine et le nom d'hôte complets pour le serveur.
 - c. La commande **hostname -d** renvoie le nom de domaine du serveur.
 - d. Les résultats d'une commande **ping** ou d'une commande **ping6** pour les environnements IPV6, avec le nom d'hôte abrégé pour chaque serveur indiquent que le serveur est accessible.
 - e. Les résultats d'une commande **ping** ou d'une commande **ping6** pour les environnements IPV6, avec le nom complet pour chaque serveur indiquent que le serveur est accessible.
4. Activez l'adressage de bouclage local pour chaque serveur dans le fichier /etc/hosts.
5. Vérifiez l'adressage de bouclage local. Les serveurs sont correctement configurés si les tests suivants réussissent.
 - a. La commande **ping -n hôtelocal** renvoie l'adresse 127.0.0.1.
 - b. La commande **ping -n hôtelocal.domainelocal** renvoie l'adresse 127.0.0.1.
 - c. La commande **ping6 -n hôtelocal6** dans un environnement IPV6 renvoie l'adresse ::1.
 - d. La commande **ping6 -n hôtelocal6.domainelocal6** dans un environnement IPV6 renvoie l'adresse ::1.
6. Ajoutez ou mettez à jour le paramètre **net.ipv4.tcp_fin_timeout=15** dans le fichier/etc/sysctl.conf pour les serveurs suivants.

Pour le Command Center Edition

- Serveur d'applications
- Serveur de messagerie
- Serveur de données
- Serveur d'application des règles
- Serveur de processus
- Serveur de surveillance

Pour le Field Edition

- Serveur d'applications
- Serveur de messagerie
- Serveur de données

Redémarrez le serveur après avoir modifié le fichier /etc/sysctl.conf.

Si cette étape n'est pas effectuée lorsque les serveurs sont préparés, le programme d'installation d'IBM Defense Operations Platform corrigera le paramètre pour l'ensemble des serveurs.

Désactivation des paramètres de sécurité

Avant d'installer IBM Defense Operations Platform, certains paramètres de sécurité doivent être désactivés. Ils peuvent être réactivés après l'installation de IBM Defense Operations Platform.

Pourquoi et quand exécuter cette tâche

Si les étapes suivantes ne sont pas effectuées avant l'installation d'IBM Defense Operations Platform, le programme d'installation désactivera tous les pare-feux. SELinux sera également désactivé, à moins qu'il

ne soit défini sur le mode "permissif". S'il est défini sur "permissif", le paramètre sera conservé. Dans tous les cas, l'installation se poursuivra normalement.

Procédure

1. Désactivez SELinux (Security Application Linux) en éditant le fichier `/etc/selinux/config` et en remplaçant `SELINUX` par `désactivé`. Après avoir modifié la configuration, redémarrez le serveur.
2. Désactivez tous les pare-feux Linux.

Configuration des services SSH

Avant d'installer IBM Defense Operations Platform, les services SSH doivent être configurés sur les serveurs. Le service doit être activé pour la connexion root associée à l'authentification par mot de passe.

Pourquoi et quand exécuter cette tâche

Le port TCP/IP 22 doit être configuré dans le système d'exploitation comme un port d'accès SSH disponible pour l'utilisation lors du processus d'installation. Le numéro de port TCP/IP d'accès SSH à l'outil de contrôle de plateforme est spécifié dans le fichier de propriétés de la topologie. Seul l'outil de contrôle de plateforme utilise le port configuré.

Procédure

1. Editez le fichier `/etc/ssh/sshd_config`.
2. Vérifiez que les lignes suivantes sont spécifiées comme suit. Aucun signe `#` ne doit se trouver au début de ces lignes.
`PermitRootLogin yes`
`PasswordAuthentication yes`
3. Enregistrez le fichier modifié.
4. Démarrez ou redémarrez le service `sshd` sur chaque serveur en exécutant la commande **`service sshd restart`**.

Installation des packages Linux pour Field Edition

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

Pourquoi et quand exécuter cette tâche

La configuration requise pour le package Linux suppose que l'option Minimale a été sélectionnée au cours de l'installation de Red Hat. L'option Minimale fournit uniquement les package `@core` et `@server-policy` qui sont essentiels pour exécuter Red Hat Enterprise Linux. Une installation minimale fournit la base pour un dispositif de serveur ou de bureau à fonction unique et maximise les performances et la sécurité pour l'installation.

Les packages Linux répertoriés dans le tableau ci-dessous doivent être installés sur les serveurs IBM Defense Operations Platform. Ces packages sont disponibles à partir de Red Hat.

Tableau 6. Packages Linux requis pour les serveurs IBM Defense Operations Platform

Serveur d'applications	Serveur de messagerie	Serveur de données
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64

Procédure

1. Tous les packages Linux requis peuvent être installés sur tous les serveurs, ou seuls les packages requis pour chaque serveur peuvent être installés.

- Pour installer tous les packages sur tous les serveurs, exécutez les commandes suivantes sur chaque serveur. Chaque commande **yum** doit être spécifiée sur une seule ligne.

```

yum install -y audit-libs.i686 audit-libs.x86_64 bc.x86_64
compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
compat-glibc-headers.x86_64 compat-libstdc++i686
compat-libstdc++x86_64 dos2unix.x86_64 elfutils.x86_64
elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64
gettext.x86_64
gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64
libaio.i686
libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 libXft.i686
libXft.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.i686
libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 libXtst.i686
libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
pam.i686 pam-devel.i686 redhat-lsb.x86_64 rpm-build.x86_64
unzip.x86_64 xorg-x11-xauth.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64 xulrunner.x86_64
zip.x86_64
    
```

```

yum -y update
    
```

- Pour installer uniquement les packages requis par chaque serveur, exécutez les commandes suivantes. Chaque commande **yum** doit être spécifiée sur une seule ligne.

Sur le serveur d'applications :

```

yum install -y bc.x86_64 compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64
compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64
elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64
glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686
gtk2-engines.x86_64 libaio.i686
ksh.x86_64libaio.x86_64 libgcc.i686
libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
rpm-build.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64

```

```

yum -y update

```

Sur le serveur de messagerie :

```

yum install -y compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64
elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64
gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64
gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64
ksh.x86_64 expect.x86_64
libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686
libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686
openmotif22.x86_64 openssh-clients.x86_64 redhat-lsb.x86_64
rpm-build.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64

```

```

yum -y update

```

Sur le serveur de données :

```

yum install -y audit-libs.i686 audit-libs.x86_64
compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64
gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686
libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openssh-clients.x86_64 pam.i686 pam-devel.i686 unzip.x86_64
xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64
zip.x86_64 xulrunner.x86_64 expect.x86_64

```

```

yum -y update

```

2. Facultatif : Installez les packages Linux pour le système X-Window sur le serveur d'applications. Ces packages sont requis si l'outil de gestion des mots de passe sera utilisé.

a. Installez les packages pour le bureau GNOME ou KDE.

Pour installer le bureau GNOME, exécutez :

```

yum -y groupinstall "X Window System" Desktop

```

Pour installer le bureau KDE, exécutez :

```

yum -y groupinstall "X Window System" "KDE Desktop"

```

b. Exécutez yum -y update

c. Démarrez le bureau en exécutant init 5. Pour que le bureau graphique soit défini comme le bureau par défaut, procédez comme suit.

1) Éditez le fichier /etc/inittab.

2) Modifiez la valeur de la propriété initdefault de 3 à5. La ligne mise à jour doit être la suivante :

```

id:5:initdefault:

```

3) Sauvegardez les modifications.

4) Redémarrez le serveur.

3. Facultatif : Si le IBM Defense Operations Platform doit être utilisé en chinois, japonais ou coréen, exécutez la commande appropriée.

Langue	Commande
Chinois	yum install -y "@Chinese Support"
Français	yum install -y "@French Support"

Information associée:

 <http://www.redhat.com/>

Installation des packages Linux pour Command Center Edition

Avant d'installer IBM Defense Operations Platform, les packages Linux doivent être installés sur les serveurs.

Pourquoi et quand exécuter cette tâche

La configuration requise pour le package Linux suppose que l'option Minimale a été sélectionnée au cours de l'installation de Red Hat. L'option Minimale fournit uniquement les package @core et @server-policy qui sont essentiels pour exécuter Red Hat Enterprise Linux. Une installation minimale fournit la base pour un dispositif de serveur ou de bureau à fonction unique et maximise les performances et la sécurité pour l'installation.

Les packages Linux répertoriés dans le tableau ci-dessous doivent être installés sur les serveurs IBM Defense Operations Platform. Ces packages sont disponibles à partir de Red Hat.

Tableau 7. Packages Linux requis pour les serveurs IBM Defense Operations Platform principaux

Serveur d'applications 1	Serveur de messagerie 1	Serveur de données 1	Serveur d'application des règles 1
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++x86_64 ksh.x86_64 libstdc++i686 libstdc++x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++x86_64 ksh.x86_64 libstdc++i686 libstdc++x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64 libstdc++x86_64 xulrunner.x86_64	compat-db.i686 compat-db.x86_64 compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 libstdc++.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64

Tableau 8. Packages Linux requis pour les serveurs IBM Defense Operations Platform de secours

Serveur d'applications 2	Serveur de messagerie 2	Serveur de données 2	Serveur d'application des règles 2
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++x86_64 ksh.x86_64 libstdc++i686 libstdc++x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++x86_64 ksh.x86_64 libstdc++i686 libstdc++x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64 elfutils.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64 libstdc++x86_64 xulrunner.x86_64	compat-db.i686 compat-db.x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686 libgcc.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64

Tableau 9. Packages Linux requis pour les serveurs de surveillance et de processus IBM Defense Operations Platform

Serveur de surveillance	Serveur de processus
audit-libs.i686	bc.x86_64
audit-libs.x86_64	compat-db.i686
bc.x86_64	compat-db.x86_64
compat-db.i686	compat-glibc.x86_64
compat-db.x86_64	compat-glibc-headers.x86_64
compat-glibc.x86_64	compat-libstdc++i686
compat-glibc-headers.x86_64	compat-libstdc++x86_64
compat-libstdc++i686	dos2unix.x86_64
compat-libstdc++x86_64	elfutils.x86_64
dos2unix.x86_64	elfutils-libs.i686
elfutils.x86_64	elfutils-libs.x86_64
elfutils-libs.i686	expect.x86_64
elfutils-libs.x86_64	gettext.x86_64
expect.x86_64	gettext-libs.x86_64
gettext.x86_64	glibc.i686
gettext-libs.x86_64	glibc.x86_64
glibc.i686	gtk2.i686
glibc.x86_64	gtk2.x86_64
gtk2.i686	gtk2-engines.i686
gtk2.x86_64	gtk2-engines.x86_64
gtk2-engines.i686	ksh.x86_64
gtk2-engines.x86_64	libaio.i686
ksh.x86_64	libaio.x86_64
libaio.i686	libgcc.i686
libaio.x86_64	libgcc.x86_64
libgcc.i686	libstdc++i686
libgcc.x86_64	libstdc++x86_64
libstdc++i686	libXmu.i686
libstdc++x86_64	libXmu.x86_64
libstdc++.i686	libXp.i686
libXft.i686	libXpm.i686
libXft.x86_64	libXpm.x86_64
libXmu.i686	libXtst.i686
libXmu.x86_64	libXtst.x86_64
libXp.i686	nfs-utils.x86_64
libXpm.i686	nfs-utils-lib.x86_64
libXpm.x86_64	nss-softoken-freebl.i686
libXpm-devel.i686	nss-softoken-freebl.x86_64
libXpm-devel.x86_64	ntp.x86_64
libXtst.i686	openmotif22.i686
libXtst.x86_64	openmotif22.x86_64
nfs-utils.x86_64	openssh-clients.x86_64
nfs-utils-lib.x86_64	pam.i686
nss-softoken-freebl.i686	pam_passwdqc.x86_64
nss-softoken-freebl.x86_64	pam-devel.i686
ntp.x86_64	redhat-lsb.x86_64
openmotif22.i686	rpm-build.x86_64
openmotif22.x86_64	tcsh.x86_64
openssh-clients.x86_64	unzip.x86_64
pam.i686	xorg-x11-xauth.x86_64
pam_passwdqc.x86_64	zip.x86_64
pam-devel.i686	zlib.i686
redhat-lsb.x86_64	zlib.x86_64
rpm-build.x86_64	
tcsh.x86_64	
unzip.x86_64	
xorg-x11-xauth.x86_64	
zip.x86_64	
zlib.i686	
zlib.x86_64	

Procédure

1. Tous les packages Linux requis peuvent être installés sur tous les serveurs, ou seuls les packages requis pour chaque serveur peuvent être installés.

- Pour installer tous les packages sur tous les serveurs, exécutez les commandes suivantes sur chaque serveur. Chaque commande **yum** doit être spécifiée sur une seule ligne.

```
yum install -y audit-libs.i686 audit-libs.x86_64 bc.x86_64 compat-db.i686
compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686
compat-libstdc++x86_64 compat-libstdc++x86_64 dos2unix.x86_64 elfutils.x86_64
elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686
glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.i686_64
ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 libstdc++x86_64
libXft.i686 libXft.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64
libXpm-devel.i686 libXpm-devel.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64
nfs-utils-lib.x86_64 nss-softoken-freebl.i686 nss-softoken-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686
pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64
xorg-x11-xauth.x86_64 xulrunner.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
```

```
yum -y update
```

- Pour installer uniquement les packages requis par chaque serveur, exécutez les commandes suivantes. Chaque commande **yum** doit être spécifiée sur une seule ligne.

Sous serveur d'applications 1 et serveur d'applications 2 :

```
yum install -y compat-libstdc++x86_64 ksh.i686_64 libstdc++i686 libstdc++x86_64 expect.x86_64
yum install -y bc.x86_64 compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64
compat-libstdc++i686 dos2unix.x86_64 elfutils.x86_64
elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64
glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686
gtk2-engines.x86_64 libaio.i686
ksh.x86_64libaio.x86_64 libgcc.i686
libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
rpm-build.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64
```

```
yum -y update
```

Sous serveur de messagerie 1 et serveur de messagerie 2 :

```
yum install -y compat-libstdc++x86_64 expect.x86_64
ksh.x86_64 libstdc++i686 libstdc++x86_64 expect.x86_64
yum install -y compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
compat-glibc-headers.x86_64 compat-libstdc++i686 dos2unix.x86_64
elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64
gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64
gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64
ksh.x86_64 expect.x86_64
libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686
libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686
openmotif22.x86_64 openssh-clients.x86_64 redhat-lsb.x86_64
rpm-build.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64
```

```
yum -y update
```

Sous serveur de données 1 et serveur de données 2 :

```
yum install -y libstdc++x86_64 xulrunner.x86_64 expect.x86_64
yum install -y audit-libs.i686 audit-libs.x86_64
compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64
gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686
libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openssh-clients.x86_64 pam.i686 pam-devel.i686 unzip.x86_64
xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64
zip.x86_64 xulrunner.x86_64 expect.x86_64
```

```
yum -y update
```

Sous serveur d'application des règles 1 et serveur d'application des règles 2

```
yum install -y compat-db.i686 compat-db.x86_64 dos2unix.x86_64
elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64
gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686
libgcc.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64
libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686
nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64
rpm-build.x86_64 unzip.x86_64 zlib.i686
zlib.x86_64 pam_passwdqc.x86_64 tcsh.x86_64
```

```
yum -y update
```

Sur le serveur de surveillance :

```
yum install audit-libs.i686 audit-libs.x86_64 bc.x86_64
compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++i686
compat-libstdc++x86_64
dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686
elfutils-libs.x86_64 expect.x86_64 gettext.x86_64
gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
gtk2-engines.i686 gtk2-engines.x86_64
ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64
libstdc++i686 libstdc++x86_64
libstdc++.i686 libXft.i686 libXft.x86_64 libXmu.i686 libXmu.x86_64
libXp.i686 libXpm.i686 libXpm.x86_64
libXpm-devel.i686 li Xpm-devel.x86_64 libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64
openssh-clients. 86_64 pam.i686 pam_passwdqc.x86_64 pam-devel.i686
redhat-lsb.x86_64 rpm-build.x86_64
tcsh.x86_64 unzip.x86_64 xorg-x11-xauth.x86_64 zip.x86_64zlib.i686
zlib.x86_64
```

```
yum -y update
```

Sur le serveur de processus :

```
yum install bc.x86_64 compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64
compat-libstdc++i686 compat-libstdc++x86_64 dos2unix.x86_64
elfutils.x86_64 elfutils-libs.i686
elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64
gtk2.i686 gtk2.x86_64 gtk2-engines.i686
gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686
libgcc.x86_64 libstdc++i686
libstdc++x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
pam_passwdqc.x86_64 rpm-build.x86_64
tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
```

```
yum -y update
```

2. Facultatif : Installez les packages Linux pour le système X-Window sur le serveur d'applications. Ces packages sont requis si l'outil de gestion des mots de passe sera utilisé.

a. Installez les packages pour le bureau GNOME ou KDE.

Pour installer le bureau GNOME, exécutez :

```
yum -y groupinstall "X Window System" Desktop
```

Pour installer le bureau KDE, exécutez :

```
yum -y groupinstall "X Window System" "KDE Desktop"
```

b. Exécutez `yum -y update`

c. Démarrez le bureau en exécutant `init 5`. Pour que le bureau graphique soit défini comme le bureau par défaut, procédez comme suit.

1) Éditez le fichier `/etc/inittab`.

2) Modifiez la valeur de la propriété `initdefault` de 3 à 5. La ligne mise à jour doit être la suivante :

```
id:5:initdefault:
```

3) Sauvegardez les modifications.

4) Redémarrez le serveur.

3. Facultatif : Si le IBM Defense Operations Platform doit être utilisé en chinois, japonais ou coréen, exécutez la commande appropriée.

Langue	Commande
Chinois	<code>yum install -y "@Chinese Support"</code>
Français	<code>yum install -y "@French Support"</code>

Information associée:

 <http://www.redhat.com/>

Définition d'exigences de pré-installation supplémentaires

Avant d'installer IBM Defense Operations Platform, une étape de configuration du serveur supplémentaire est requise.

Procédure

1. Vérifiez que l'horodatage de tous les serveurs (date et heure) est le même que celui défini sur le système d'exploitation Linux. Il est possible d'utiliser un service de synchronisation date/heure à cet effet.
2. Assurez-vous qu'aucune version d'IBM Java n'est installée sur les serveurs.
3. Définissez **UMASK** sur 022.

Préparation des serveurs pour Command Center Edition

Avant d'installer IBM Defense Operations Platform Command Center Edition, une étape de configuration du serveur supplémentaire est requise.

Procédure

1. Vérifiez que votre réseau exécute IPV4. Le groupement du serveur à haute disponibilité ne prend pas en charge IPV6.
2. Assurez-vous que les éléments suivants sont configurés correctement pour que la technologie de groupement de Tivoli System Automation puisse être installée avec succès.
 - a. Assurez-vous que les noms d'hôte sont indiqués correctement.
 - b. Assurez-vous que les valeurs contenues dans les propriétés de configuration TSA.* dans le fichier de propriétés de topologie sont configurés correctement. Par exemple, assurez-vous que le contrôleur NIC indiqué dans la propriété TSA.PRIMARY.USERNIC existe et qu'il est en activité pendant l'installation.
 - c. Assurez-vous que les ports HADR de reprise à haut niveau de disponibilité après incident de DB2 sont disponibles. Ces ports sont utilisés pour répliquer les informations des bases de données principales vers les bases de données de secours. Par défaut, ces ports se situent dans la plage 55000.
3. Sur le serveur de messagerie 1 et le serveur de messagerie 2, assurez-vous que les services `rpcidmapd`, `nfs` et `rpcbind` sont définis pour démarrer automatiquement et qu'ils sont démarrés. La commande permettant de modifier les informations de démarrage pour un service spécifié est **`chkconfig nom_service on`**, où *nom_service* est le nom du service. La commande permettant de démarrer un service spécifié est **`etc/init.d/nom_service start`**, où *nom_service* est le nom du service.
4. Une adresse IP virtuelle doit être définie pour équilibrer les requêtes Web entre plusieurs serveurs proxy inverses. L'équilibreur de charge répartit la charge de travail entre différents serveurs proxy inverses sur serveur d'application des règles 1 et serveur d'application des règles 2. L'adresse IP virtuelle doit être mappée à un nom d'hôte virtuel qualifié complet. Le nom d'hôte virtuel est une combinaison des propriétés `PORTAL.VIRTUAL.URL` et `WAS.LTPA.DOMAIN`, définies dans le fichier de propriétés de topologie. Le nom d'hôte par défaut est `virtualportal.platform.ibm.com`.

Si un seul serveur proxy inverse est utilisé (serveur d'application des règles 1 ou serveur d'application des règles 2), le nom d'hôte virtuel défini par la combinaison des propriétés `PORTAL.VIRTUAL.URL` et `WAS.LTPA.DOMAIN` doit être mappé (à l'aide d'un alias DNS ou d'un fichier `hosts`) à l'un des serveurs proxy inverses.

Tâches associées:

«Configuration du réseau TCP/IP», à la page 16

Avant d'installer IBM Defense Operations Platform, le réseau TCP/IP doit être configuré sur les serveurs.

Préparation du serveur d'installation

Le serveur d'installation doit être préparé avant qu'il soit possible d'installer IBM Defense Operations Platform.

Pourquoi et quand exécuter cette tâche

Dans Field Edition, le serveur de messagerie est utilisé comme serveur d'installation. Dans Command Center Edition, le serveur de messagerie 1 est utilisé comme serveur d'installation.

Procédure

1. Obtenez le module d'installation IBM Defense Operations Platform en commandant le package de DVD ou en obtenant les images à partir de Passport Advantage.
2. Sur le serveur d'installation, créez un répertoire nommé `/distributionMedia`, si ce répertoire n'existe pas déjà. Si vous voulez utiliser un répertoire autre que `/distributionMedia`, notez le nom du répertoire. Vous devrez indiquer le nom du répertoire différent pendant l'installation. Dans les étapes suivantes, `/distributionMedia` est utilisé dans les exemples.
3. Si vous utilisez les DVD physiques, copiez les images d'installation sur le serveur d'installation.
 - a. Montez un DVD.
 - b. Copiez le contenu du DVD dans le répertoire `/distributionMedia`, ou dans le répertoire que vous avez créé.
 - c. Démontez le DVD.
 - d. Répétez cette opération jusqu'à ce que le contenu de tous les DVD soit copié dans le répertoire sur le serveur d'installation.
4. Si vous utilisez les images ISO à partir de Passport Advantage, copiez les images d'installation sur le serveur d'installation.
 - a. Créez un répertoire `/distributionMedia/iso` ou un sous-répertoire `/iso` sous le répertoire que vous avez créé à l'étape 2. Les instructions suivantes utiliseront `/distributionMedia/iso` dans les exemples.
 - b. Téléchargez ou copiez chaque image ISO à partir de Passport Advantage dans le sous-répertoire `/iso`.
 - c. Créez un répertoire pour installer l'image ISO. Pour cela, vous pouvez exécuter la commande suivante : `mkdir /mnt/dop16`. Les instructions suivantes utiliseront `/mnt/dop16` dans les exemples.
 - d. Installez l'image ISO en exécutant la commande suivante : `mount -o loop /distributionMedia/iso/nomfichier_iso /mnt/dop16` où `nomfichier_iso` est le nom de l'un des fichiers image ISO.
 - e. Copiez le contenu ISO dans `/distributionMedia` en exécutant la commande suivante : `cp -r /mnt/dop16/* /distributionMedia`.
 - f. Répétez l'installation et la copie des contenus ISO jusqu'à ce que tous les fichiers image ISO aient été traités.
 - g. Supprimez le répertoire `/distributionMedia/iso` à moins que vous ne vouliez archiver les images ISO initiales.
5. Décompressez le module d'installation.
 - a. Accédez au répertoire `/installHome`, ou au répertoire que vous avez créé.

b. Exécutez la commande `tar -zxvf dop.tar.gz`.

Fichiers de propriétés de la topologie

Les fichiers de propriétés de la topologie définissent les propriétés personnalisables par l'utilisateur pour le déploiement d'IBM Defense Operations Platform. Ces fichiers doivent être édités en fonction des besoins de l'environnement du client. Toutes les propriétés du fichier de propriétés de la topologie fourni qui ne sont pas documentées ne doivent pas être modifiées.

Après avoir modifié le fichier de propriétés de la topologie, enregistrez une copie et conservez-la dans un emplacement sécurisé. Ce fichier contient des informations sensibles en termes de sécurité, telles que des noms et des mots de passe pour le système, en texte clair. Si une personne non autorisée a accès à ce fichier, elle disposera d'un accès intégral au système.

Le fichier de propriétés de la topologie peut être utilisé après l'installation de l'une des manières suivantes :

- En tant que référentiel des informations de mot de passe, si un mot de passe est oublié.
- En tant que référentiel des mots de passe, si un mot de passe est modifié dans le système. Le fichier de propriétés de la topologie modifié peut servir à mettre à jour les mots de passe utilisés par l'outil de contrôle de plateforme.
- En tant que sauvegarde des informations d'installation, si le système doit être réinstallé. Le fichier de propriétés de la topologie peut être utilisé sans qu'il soit nécessaire de redéfinir tous les paramètres d'installation.

IBM Defense Operations Platform fournit les fichiers de topologie suivants :

Nom du fichier	Objet	Utilisé pour
<code>install_home/dop16/resource/custom.properties</code>	Définit l'emplacement du support d'installation, des répertoires de travail et d'autres propriétés. Ce fichier peut être édité pour répondre aux besoins de l'environnement du client.	Command Center Edition et Field Edition
<code>install_home/dop16/topology/dop.d2.properties</code>	Définit les propriétés personnalisables par l'utilisateur pour le déploiement, y compris les noms d'hôte et les mots de passe. Ce fichier peut être édité pour répondre aux besoins de l'environnement du client.	Field Edition
<code>install_home/dop16/topology/dop.d1.properties</code>	Définit les propriétés personnalisables par l'utilisateur pour le déploiement, y compris les noms d'hôte et les mots de passe. Ce fichier peut être édité pour répondre aux besoins de l'environnement du client.	Command Center Edition

Personnalisation des propriétés d'installation

Le fichier de propriétés d'installation fournit des définitions requises par les scripts d'installation. Ces propriétés peuvent être modifiées lors de l'utilisation des options d'installation de ligne de commande.

Pourquoi et quand exécuter cette tâche

Sur le serveur d'installation, accédez au répertoire dans lequel le module d'installation d'IBM Defense Operations Platform a été copié. Dans ces étapes, ce répertoire est appelé `racine_install`. Le serveur

d'installation est le serveur de messagerie. Dans Command Center Edition, le serveur de messagerie 1 est le serveur d'installation.

Procédure

Facultatif : Editez le fichier *rép_principal_install/dop16/resource/custom.properties* et modifiez les valeurs de propriétés suivantes si vous le souhaitez. Toutes les valeurs de propriétés qui ne sont pas exposées dans le tableau 10 ne doivent pas être modifiées. Il est recommandé aux utilisateurs installant IBM Defense Operations Platform pour la première fois d'utiliser les valeurs par défaut.

Tableau 10. Propriétés d'installation d'IBM Defense Operations Platform

Propriété	Description	Valeur par défaut
image.basedir.local	Nom du répertoire sur le serveur d'installation contenant les fichiers d'installation d'IBM Defense Operations Platform. Il s'agit du répertoire dans lequel les fichiers de support d'installation ont été copiés avant d'exécuter l'outil d'installation. Le répertoire est appelé <i>support_installation</i> dans d'autres instructions d'installation.	/distributionMedia
image.tempdir.local	Répertoire sur le serveur d'installation utilisé pour stocker des fichiers temporaires lors de l'installation.	/tmp/dop/images
backup.local	Ce répertoire est destiné à usage interne uniquement.	/tmp/dop/backup
Unix.image.basedir.remote	Répertoire sur les serveurs cible dans lequel les modules à installer sur ce serveur seront copiés.	/installMedia/dop/image
Unix.script.basedir.remote	Répertoire sur les serveurs cible dans lequel les scripts à exécuter sur ce serveur seront copiés.	/installMedia/dop/script
connection.timeout	Temps d'attente (en millisecondes) d'une connexion aux serveurs cible avant l'échec.	15000
waiting.time	Temps d'attente (en millisecondes) avant de relancer une connexion ayant échoué.	20000
retry.count	Nombre de tentatives de relance d'une connexion ayant échoué avant l'échec de l'installation.	12

Si ces valeurs ne sont pas modifiées, les valeurs par défaut sont utilisées.

Informations sur le serveur cible pour Field Edition

La section SERVERS du fichier de propriétés de la topologie définit les propriétés des serveurs cible.

Le tableau 11 décrit les valeurs de propriété de serveur qui doivent être spécifiées dans le fichier de propriétés de la topologie pour votre environnement.

Tableau 11. Propriétés de serveur cible

Propriété	Description
DB.1.HOST	Nom de système hôte qualifié complet du serveur de données

Tableau 11. Propriétés de serveur cible (suite)

Propriété	Description
DB.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de données
DB.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de données
APP.1.HOST	Nom de système hôte qualifié complet du serveur d'applications
APP.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur d'applications
APP.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur d'applications
MSG.1.HOST	Nom de système hôte qualifié complet du serveur de messagerie
MSG.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de messagerie
MSG.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de messagerie

Important : Les valeurs du nom d'hôte doivent être des noms de système hôte qualifiés complets entrés dans la casse définie. Par exemple, DOP16App.DOP16.com est différent dedop16app.dop16.com.

Un numéro de port ssh peut être défini pour chaque serveur. Toutefois, les numéros de port configurés ne seront utilisés que par l'outil de contrôle de plateforme. Le port 22 doit être activé pour l'accès ssh sur chaque serveur. Ce port est requis pour l'accès ssh à IBM Defense Operations Platform au cours de l'installation.

Informations sur le serveur cible pour Command Center Edition

La section SERVERS du fichier de propriétés de la topologie définit les propriétés des serveurs cible.

Le tableau 12 décrit les valeurs de propriété de serveur qui doivent être spécifiées dans le fichier de propriétés de la topologie pour votre environnement.

Tableau 12. Propriétés de serveur cible

Propriété	Description
DB.1.HOST	Nom de système hôte qualifié complet du serveur de données 1
DB.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de données 1
DB.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de données 1
DB.2.HOST	Nom de système hôte qualifié complet du serveur de données 2
DB.2.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de données 2
DB.2.SSH_PORT	Numéro de port pour l'accès ssh au serveur de données 2
APP.1.HOST	Nom de système hôte qualifié complet du serveur d'applications 1
APP.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur d'applications 1

Tableau 12. Propriétés de serveur cible (suite)

Propriété	Description
APP.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur d'applications 1
APP.2.HOST	Nom de système hôte qualifié complet du serveur d'applications 2
APP.2.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur d'applications 2
APP.2.SSH_PORT	Numéro de port pour l'accès ssh au serveur d'applications 2
MSG.1.HOST	Nom de système hôte qualifié complet du serveur de messagerie 1
MSG.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de messagerie 1
MSG.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de messagerie 1
MSG.2.HOST	Nom de système hôte qualifié complet du serveur de messagerie 2
MSG.2.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de messagerie 2
MSG.2.SSH_PORT	Numéro de port pour l'accès ssh au serveur de messagerie 2
WEB.1.HOST	Nom de système hôte qualifié complet du serveur d'application des règles 1
WEB.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur d'application des règles 1
WEB.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur d'application des règles 1
WEB.2.HOST	Nom de système hôte qualifié complet du serveur d'application des règles 2
WEB.2.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur d'application des règles 2
WEB.2.SSH_PORT	Numéro de port pour l'accès ssh au serveur d'application des règles 2
MON.1.HOST	Nom de système hôte qualifié complet du serveur de surveillance
MON.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de surveillance
MON.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de surveillance
PRO.1.HOST	Nom de système hôte qualifié complet du serveur de processus
PRO.1.ACCOUNT.PWD	Mot de passe associé à l'utilisateur root sur le serveur de processus
PRO.1.SSH_PORT	Numéro de port pour l'accès ssh au serveur de processus

Important : Les valeurs du nom d'hôte doivent être des noms de système hôte qualifiés complets entrés dans la casse définie. Par exemple, DOP16App.DOP16.com est différent dedop16app.dop16.com.

Un numéro de port ssh peut être défini pour chaque serveur. Toutefois, les numéros de port configurés ne seront utilisés que par l'outil de contrôle de plateforme. Le port 22 doit être activé pour l'accès ssh sur chaque serveur. Ce port est requis pour l'accès ssh à IBM Defense Operations Platform au cours de l'installation.

Informations sur les services d'annuaire

Le fichier de propriétés de la topologie définit les valeurs utilisées pour chiffrer les mots de passe utilisateur et d'autres données sensibles dans le répertoire.

Le chiffrement s'appuie sur deux valeurs : LDAP.SEED et LDAP.SALT.

Les valeurs doivent être des caractères ASCII imprimables qui comportent des valeurs de point de code comprises entre 33 et 126. Les espaces ne sont pas autorisés.

Tableau 13. Propriétés des services d'annuaire

Propriété	Description
LDAP.SEED	Chaîne de 12 à 1016 caractères comprenant des caractères ASCII imprimables entre les points de code 33 et 126. Une chaîne chiffrée renforcée doit être utilisée. Par exemple, une chaîne longue comportant des lettres à casse mixte, des nombres et des caractères spéciaux sans mots ni expressions courants.
LDAP.SALT	Chaîne de 12 caractères comprenant des caractères ASCII imprimables entre les points de code 33 et 126. Important : LDAP.SALT doit comporter exactement 12 caractères, sinon l'installation échoue.

Notez les valeurs des propriétés LDAP.SEED et LDAP.SALT. Elles vous seront utiles pour exporter ou répliquer des entrées d'annuaire.

Suffixe LDAP

Les informations de suffixe LDAP utilisées dans IBM Defense Operations Platform sont définies dans le fichier de propriétés de topologie.

Seuls les paramètres LDAP ou, o et c peuvent être modifiés. Ces paramètres doivent répondre aux exigences affichées dans le tableau 14.

Tableau 14. Règles de syntaxe des paramètres LDAP

Paramètre	Règles
c	Doit contenir exactement deux caractères composés uniquement des caractères suivants : <ul style="list-style-type: none"> • Minuscules (a-z) • Majuscules (A-Z)
o	Doit contenir entre 1 et 30 caractères composés uniquement des caractères suivants : <ul style="list-style-type: none"> • Minuscules (a-z) • Majuscules (A-Z) • Nombres (0-9) • Tiret (-) • Trait de soulignement (_)

Tableau 14. Règles de syntaxe des paramètres LDAP (suite)

Paramètre	Règles
ou	Doit contenir entre 1 et 30 caractères composés uniquement des caractères suivants : <ul style="list-style-type: none"> • Minuscules (a-z) • Majuscules (A-Z) • Nombres (0-9) • Tiret (-) • Trait de soulignement (_)

Les valeurs de ou, o et c doivent correspondre lorsqu'elles sont indiquées dans les propriétés suivantes :

- LDAP.SUFFIX
- LDAP.BASE.ENTRY
- LDAP.USER.ENTRY
- LDAP.GROUP.ENTRY
- LDAP.PROXY.DN

Exemple :

```
LDAP.SUFFIX ou=SWG,o=IBM,c=US
LDAP.BASE.ENTRY ou=SWG,o=IBM,c=US
LDAP.USER.ENTRY ou=USERS,ou=SWG,o=IBM,c=US
LDAP.GROUP.ENTRY ou=GROUPS,ou=SWG,o=IBM,c=US
LDAP.PROXY.DN ou=SWG,o=IBM,c=US
```

Domaine LTPA (Lightweight Third-Party Authentication)

IBM Defense Operations Platform utilise un jeton LTPA (Lightweight Third-Party Authentication) pour activer la connexion unique sur plusieurs services. Le nom de domaine LTPA doit être spécifié dans le fichier de propriétés de la topologie.

Spécifiez le nom de domaine LTPA pour votre environnement dans la propriété WAS.LTPA.DOMAIN. La valeur appropriée peut être obtenue en exécutant la commande **hostname -dsur** serveur d'applications dans Field Edition ou on serveur d'applications 1 dans Command Center Edition.

Dans Field Edition, cette valeur doit être la même sur les serveurs suivants :

- serveur d'applications
- serveur de messagerie

Dans Command Center Edition, cette valeur doit être la même sur les serveurs suivants :

- serveur d'applications 1
- serveur d'applications 2
- serveur de messagerie 1
- serveur de messagerie 2

Le nom de domaine LTPA est la partie parente du nom d'hôte qualifié complet des serveurs. Par exemple, si le nom d'hôte qualifié complet est server.yourco.com, alors le domaine LTPA est yourco.com.

Propriétés de groupement

Les propriétés permettant de configurer les composants de la topologie de groupement doivent être définies avant d'installer IBM Defense Operations Platform dans Command Center Edition.

Tableau 15. Propriétés de groupement

Propriété	Description
TSA.NETWORK.SUBNET	Masque de sous-réseau du réseau hébergeant les serveurs de base de données. Il s'agit du masque de sous-réseau des cartes d'interface réseau figurant sur les deux serveurs de base de données.
TSA.PRIMARY.USENIC	Nom de la carte d'interface réseau sur le serveur de données 1. Le nom de la carte d'interface réseau peut être recherché en exécutant la commande ifconfig sur serveur de données 1.
TSA.STANDBY.USENIC	Nom de la carte d'interface réseau sur le serveur de données 2. Le nom de la carte d'interface réseau peut être recherché en exécutant la commande ifconfig sur serveur de données 2.
TSA.QUORUM.IP	Adresse IP d'un système hautement disponible qui ne fait pas partie de l'environnement IBM Defense Operations Platform. Cette adresse IP doit pouvoir être atteinte à partir du serveur de données 1 et du serveur de données 2 IBM Defense Operations Platform. Aucun logiciel ne sera installé dans cet emplacement. La seule exigence est que le système soit disponible pendant l'installation et pendant la phase d'exécution.

Informations sur les mots de passe pour Field Edition

Les mots de passe des différents ID utilisateur utilisés dans la solution IBM Defense Operations Platform sont définis dans le fichier de propriétés de la topologie. Pour des raisons de sécurité, les mots de passe par défaut fournis avec IBM Defense Operations Platform doivent être modifiés.

Seuls les caractères suivants sont autorisés pour le mot de passe :

- Minuscules (a-z)
- Majuscules (A-Z)
- Nombres (0-9)
- Tiret (-)
- Point (.)
- Trait de soulignement (_)
- Tilde (~)

Les tirets et les points ne peuvent pas être les premiers caractères d'un mot de passe.

Sauf mention contraire, ils ne doivent pas comporter plus de 30 caractères.

Tableau 16. Propriétés des mots de passe

Propriété	Nom d'utilisateur associé	Description
DB.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de données
APP.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur d'applications
MSG.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de messagerie
LDAP.DB.PWD	dsrdbm01	Base de données d'annuaire LDAP

Tableau 16. Propriétés des mots de passe (suite)

Propriété	Nom d'utilisateur associé	Description
LDAP.ADMIN.DN.PWD	cn=root	Liaison d'administrateur LDAP
LDAP.BIND.DN.PWD	cn=bind	Liaison LDAP
LDAP.REPLICA.BIND.DN.PWD	cn=master	Liaison de serveur secondaire LDAP
ISIM.KEYSTORE.PWD	aucune	Mot de passe de fichier de clés
ISIM.POSIX.LINUX.PWD	posixagent	Utilisateur de POSIX Linux
IHS.KEYSTORE.PWD	aucune	Fichier de clés du serveur HTTP
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Administrateur des services d'application. Ce mot de passe doit être identique à PORTAL.ADMIN.ACCOUNT.PWD.
WAS.LTPA.PWD	aucune	Jeton LTPA
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrateur de la console WebSphere Application Server pour le serveur WebSphere Portal. Ce mot de passe doit être identique à WAS.ADMIN.ACCOUNT.PWD.
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrateur pour le serveur WebSphere Portal. Ce mot de passe doit être identique à DOMINO.ST.ADMIN.PWD.
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal Base de données
DOMINO.USER.PWD	remarques	Utilisateur de collaboration
DOMINO.ORG.PWD	IBM	Organisation de collaboration
DOMINO.ADMIN.PWD	notes admin	Administrateur de collaboration
DOMINO.ST.ADMIN.PWD	wpsadmin	Administrateur de portail de collaboration. Ce mot de passe doit être identique à PORTAL.ADMIN.UID.PWD.
DOMINO.ST.BIND.PWD	wpsbind	Liaison LDAP de collaboration
DEFAULT.PWD.DAS	dausr1	Serveur d'administration des services de bases de données
DEFAULT.PWD.DB2	db2inst1, db2inst2	Serveur de données des services de bases de données
DEFAULT.PWD.IHS	ihsadmin	Serveur HTTP
DEFAULT.PWD.MQM	mqm	Utilisateur des services de messagerie
MQM.CONN.USER.PWD	mqmconn	Connexion des services de messagerie

Tableau 16. Propriétés des mots de passe (suite)

Propriété	Nom d'utilisateur associé	Description
IOP.ADMIN.USER.PWD	ibmadmin	Outils d'administration du système Cet utilisateur bénéficie de droits d'accès équivalents à l'utilisateur root sur les serveurs cible. L'outil de contrôle de plateforme s'exécute sous ce nom d'utilisateur. Compte tenu des droits d'accès accordés à cet utilisateur, vérifiez que ce mot de passe a une valeur longue, différente des autres mots de passe, et qu'il est sécurisé.
IOP.USER.USER.PWD	ibmuser	Utilisateur général du système

Informations sur les mots de passe pour Command Center Edition

Les mots de passe des différents ID utilisateur utilisés dans la solution IBM Defense Operations Platform sont définis dans le fichier de propriétés de la topologie. Pour des raisons de sécurité, les mots de passe par défaut fournis avec IBM Defense Operations Platform doivent être modifiés.

Seuls les caractères suivants sont autorisés pour le mot de passe :

- Minuscules (a-z)
- Majuscules (A-Z)
- Nombres (0-9)
- Tiret (-)
- Point (.)
- Trait de soulignement (_)
- Tilde (~)

Les tirets et les points ne peuvent pas être les premiers caractères d'un mot de passe.

Sauf mention contraire, ils ne doivent pas comporter plus de 30 caractères.

Tableau 17. Propriétés des mots de passe

Propriété	Nom d'utilisateur associé	Description
WEB.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur d'application des règles 1
WEB.2.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur d'application des règles 2
DB.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de données 1
DB.2.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de données 2
APP.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur d'applications 1
APP.2.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur d'applications 2
MSG.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de messagerie 1

Tableau 17. Propriétés des mots de passe (suite)

Propriété	Nom d'utilisateur associé	Description
MSG.2.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de messagerie 2
MON.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de surveillance
PRO.1.ACCOUNT.PWD	superutilisateur	Mot de passe root pour le serveur de processus
LDAP.DB.PWD	dsrdbm01	Base de données d'annuaire LDAP
LDAP.ADMIN.DN.PWD	cn=root	Liaison d'administrateur LDAP
LDAP.BIND.DN.PWD	cn=bind	Liaison LDAP
LDAP.PROXY.INSTANCE.PWD	tdsproxy	Instance de proxy LDAP
LDAP.PROXY.ADMIN.DN.PWD	cn=root	Liaison d'administrateur proxy LDAP
LDAP.PROXY.BIND.DN.PWD	cn=bind	Liaison de proxy LDAP
LDAP.REPLICA.BIND.DN.PWD	cn=master	Liaison de serveur secondaire LDAP
ISIM.KEYSTORE.PWD	aucune	Mot de passe de fichier de clés
ISIM.POSIX.LINUX.PWD	posixagent	Utilisateur de POSIX Linux
IHS.KEYSTORE.PWD	aucune	Fichier de clés du serveur HTTP
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Administrateur des services d'applications La valeur WAS.ADMIN.ACCOUNT.PWD doit être identique à PORTAL.ADMIN.ACCOUNT.PWD.
WAS.LTPA.PWD	aucune	Jeton LTPA
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrateur de la console WebSphere Application Server pour le serveur WebSphere Portal La valeur PORTAL.ADMIN.ACCOUNT.PWD doit être identique à WAS.ADMIN.ACCOUNT.PWD.
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrateur du serveur WebSphere Portal La valeur PORTAL.ADMIN.UID.PWD doit être identique à DOMINO.ST.ADMIN.PWD.
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal Base de données
DOMINO.USER.PWD	remarques	Utilisateur de collaboration
DOMINO.ORG.PWD	IBM	Organisation de collaboration
DOMINO.ADMIN.PWD	notes admin	Administrateur de collaboration
DOMINO.ST.ADMIN.PWD	wpsadmin	Administrateur du portail de collaboration La valeur DOMINO.ST.ADMIN.PWD doit être identique à PORTAL.ADMIN.UID.PWD.
DOMINO.ST.BIND.PWD	wpsbind	Liaison LDAP de collaboration
DEFAULT.PWD.DAS	dausr1	Serveur d'administration des services de bases de données

Tableau 17. Propriétés des mots de passe (suite)

Propriété	Nom d'utilisateur associé	Description
DEFAULT.PWD.DB2	db2inst1, db2inst2	Serveur de données des services de bases de données
DEFAULT.PWD.IHS	ihsadmin	Serveur HTTP
DEFAULT.PWD.MQM	mqm	Utilisateur des services de messagerie
MQM.CONN.USER.PWD	mqmconn	Connexion des services de messagerie
IOP.ADMIN.USER.PWD	ibmadmin	Outils d'administration du système Cet utilisateur bénéficie de droits d'accès équivalents à l'utilisateur root sur les serveurs cible. L'outil de contrôle de plateforme s'exécute sous ce nom d'utilisateur. Compte tenu des droits d'accès accordés à cet utilisateur, vérifiez que ce mot de passe a une valeur longue, différente des autres mots de passe, et qu'il est sécurisé.
IOP.USER.USER.PWD	ibmuser	Utilisateur général du système
TAM.SECMASTER.PWD	sec_master	Administrateur IBM Security Access Manager
DEFAULT.PWD.TAI	taiuser	Utilisateur d'association de confiance
ODM.DB.USER.PWD	db2wodm	IBM Operational Decision Manager - base de données
ODM.ADMIN.UID.PWD	resAdmin1	IBM Operational Decision Manager - administrateur
ODM.DEPLOYER.UID.PWD	resDeployer1	IBM Operational Decision Manager - déployeur
ODM.MONITOR.UID.PWD	resMonitor1	IBM Operational Decision Manager - moniteur
ODM.DB.DC.USER.PWD	wodmdc	IBM Operational Decision Manager - base de données
ODM.rtsAdmin.UID.PWD	rtsAdmin	IBM Operational Decision Manager - administrateur
ODM.rtsConfig.UID.PWD	rtsConfig	IBM Operational Decision Manager - administrateur de configuration
ODM.rtsUser.UID.PWD	rtsUser	IBM Operational Decision Manager - utilisateur
OMNIBUS.OWNER.ACCOUNT.PWD	netcool	Tivoli Netcool/OMNIBus - propriétaire
OMNIBUS.ADMIN.ACCOUNT.PWD	tipadmin	Tivoli Netcool/OMNIBus - administrateur
BPM.DB.USER.PWD	db2bpm	IBM Business Process Manager - base de données
WSRR.DB.USER.PWD	db2wsrr	WebSphere Service Registry and Repository - base de données
TEPS.DB.USER.PWD	itmuser	Tivoli Monitoring - base de données

Tableau 17. Propriétés des mots de passe (suite)

Propriété	Nom d'utilisateur associé	Description
ITM.ADMIN.PWD	sysadmin	Tivoli Monitoring - administrateur Le mot de passe doit comporter entre 5 et 15 caractères

Propriétés Cyber Hygiene

Le fichier de propriétés de la topologie définit les propriétés de traitement Cyber Hygiene.

Le tableau 18 décrit les valeurs qui doivent être spécifiées dans le fichier de propriétés de la topologie pour votre environnement en cas d'utilisation de Cyber Hygiene.

Tableau 18. Propriétés Cyber Hygiene

Propriété	Description
IOP.CH.DISABLEROOTLOGIN	Si Cyber Hygiene est exécuté, cette propriété détermine si l'utilisateur root est autorisé à se connecter aux serveurs cible. Y indique que la connexion de l'utilisateur root est désactivée N indique que la connexion de l'utilisateur root est activée
IOP.CH.GRUB.PWD	Cette propriété permet de spécifier le mot de passe GRUB (GRand Unified Bootloader) que Cyber Hygiene appliquera à tous les serveurs.

Exécution du programme d'installation de ligne de commande Field Edition

IBM Defense Operations Platform est installé à l'aide d'un script qui prépare et contrôle les serveurs et installe IBM Defense Operations Platform Field Edition.

Procédure

1. Connectez-vous au serveur d'installation en tant qu'utilisateur root.
Pour Field Edition, le serveur d'installation est serveur de messagerie.
2. Accédez au répertoire `/rép_principale_install/dop16/bin`.
3. Exécutez la commande `./dop-env.sh`.
4. Exécutez la commande `./dop.d2.install.sh -p mot_de_passe_installation`. Le `mot_de_passe_installation` est utilisé pour assurer la sécurité de la topologie définie pour IBM Defense Operations Platform. Ce mot de passe est requis pour apporter des modifications à l'installation d'IBM Defense Operations Platform et constitue le mot de passe initial pour les outils d'IBM Defense Operations Platform.

Seuls les caractères suivants sont autorisés pour le mot de passe :

- Minuscules (a-z)
- Majuscules (A-Z)
- Nombres (0-9)
- Tiret (-)
- Point (.)
- Trait de soulignement (_)
- Tilde (~)

Les tirets et les points ne peuvent pas être les premiers caractères d'un mot de passe.

Si aucun n'est indiqué au cours de l'étape de création du magasin de clés de topologie, le *mot_de_passe_installation* prendra la valeur *ibmdop16*. Un menu contenant des étapes d'installation s'affiche.

5. Un contrat de licence est présenté. L'acceptation de la licence est nécessaire pour que l'installation puisse se poursuivre.
6. Sélectionnez une option dans le menu.

Tableau 19. Options d'installation

Sélection	Phase d'installation	Description de l'étape	Durée moyenne requise
1	Pré-contrôle	Valider les totaux de contrôle du support d'installation	15 minutes
2	Préparation	Copier les modèles vers le répertoire de topologie	2 minutes
3	Préparation	Créer un magasin de clés de topologie	1 minute
4	Préparation	Paramétrer toutes les topologies	2 minutes
5	Préparation	(Facultatif) Chiffrer toutes les topologies	1 minute
6	Préparation	Exécuter "Configurer/Cibler" la topologie	5 minutes
7	Préparation	Exécuter les contrôles prérequis environnementaux	15 minutes
8	Installation	(Facultatif) Télécharger le support sur les serveurs cibles Si le support n'est pas téléchargé au cours de cette étape, il sera téléchargé à l'étape suivante. En téléchargeant le support à l'étape suivante, un point de contrôle peut être défini après avoir téléchargé le support.	30 minutes
9	Installation	Exécuter une topologie d'installation de produits de base	2 heures
10	Installation	Exécuter une topologie de configuration de produits	3 heures 30 minutes
11	Installation	Installer le composant Identity Manager	1 heure 15 minutes
12	Installation	(Facultatif) Installer l'outil Data Studio	15 minutes
13	Installation	Installer l'outil de contrôle de plateforme	15 minutes
14	Installation	Installer l'outil de vérification du système	1 heure 15 minutes
15	Installation	(Facultatif) Installer et exécuter l'outil cyber hygiene une fois terminé. Avant d'exécuter l'outil cyber hygiene, il est recommandé de prendre un point de contrôle du système. Cyber hygiene exige que les paramètres de propriété soient définis dans le fichier de propriétés de la topologie. Vérifiez que ces paramètres ont été définis avant d'exécuter l'outil.	De 15 à 30 minutes

7. Reprenez à partir de l'étape 4, à la page 43 en sélectionnant les étapes d'installation dans l'ordre. Ne sélectionnez pas l'étape suivante tant que l'étape d'installation précédente n'est pas terminée. Ne redémarrez pas de serveurs jusqu'à ce que toutes les étapes se soient terminées avec succès. L'étape d'installation peut également être spécifiée dans la commande. Par exemple : `./dop.d2.install.sh 1 -p mot_de_passe_installation`.

Résultats

La progression de l'installation s'affiche. Elle est également enregistrée dans les journaux situés dans le répertoire *rép_principale_install/dop16/log* du serveur d'installation.

La progression de l'outil Cyber hygiene sur le serveur d'installation s'affiche sur la console et est consignée dans le fichier `/tmp/dop.16.cyber-hygiene.log`. Une fois l'exécution terminée sur le serveur d'installation, cyber hygiene peut continuer à fonctionner sur les autres serveurs IBM Defense Operations Platform. Pour déterminer la progression de l'outil cyber hygiene, exécutez la commande **ps -ef | grep hygiene**. Une fois l'exécution terminée, les fichiers journaux cyber hygiene sont stockés sur les autres serveurs IBM Defense Operations Platform, dans le répertoire `/var/cyber-hygiene/results/`. Chaque répertoire contiendra trois fichiers `.log`. Pour plus d'informations sur l'interprétation des fichiers journaux, consultez le fichier `/opt/IBM/iop/tools/ch/scripts-to-remotely-run-ch_DOP-1.6.doc` que vous trouverez sur le serveur d'installation, qui sera disponible une fois cyber hygiene exécuté.

Que faire ensuite

Si vous devez renouveler l'étape cyber hygiene (option 15), procédez au préalable comme suit :

1. Sur le serveur d'installation, modifiez le fichier `/install_home/dop16/topology/dop.d2.cyberhygiene.xml`.
2. Modifiez l'état de l'instance (Prêt ou Incertain, à mi-hauteur dans le fichier, sur la ligne contenant `type="runTool"` et `id="run_ch_i1"`) en spécifiant Nouveau.
3. Exécutez `./dop.d2.install.sh 15 -p mot_de_passe_installation` où `mot_de_passe_installation` représente le mot de passe de topologie.

Si le fichier xml n'est pas modifié avant la réexécution de l'étape cyber hygiene, on assistera à un report d'environ 10 secondes, mais aucune action ne sera effectuée.

Exécution du programme d'installation de ligne de commande Command Center Edition

IBM Defense Operations Platform est installé à l'aide d'un script qui prépare et contrôle les serveurs et installe IBM Defense Operations Platform Command Center Edition.

Procédure

1. Connectez-vous au serveur d'installation en tant qu'utilisateur root.
Pour Command Center Edition, le serveur d'installation est le serveur de messagerie 1.
2. Accédez au répertoire `/rép_principale_install/dop16/bin`.
3. Exécutez la commande `./dop-env.sh`.
4. Le `mot_de_passe_installation` est utilisé pour assurer la sécurité de la topologie définie pour IBM Defense Operations Platform. Ce mot de passe est requis pour apporter des modifications à l'installation d'IBM Defense Operations Platform et constitue le mot de passe initial pour les outils d'IBM Defense Operations Platform.

Seuls les caractères suivants sont autorisés pour le mot de passe :

- Minuscules (a-z)
- Majuscules (A-Z)
- Nombres (0-9)
- Tiret (-)
- Point (.)
- Trait de soulignement (_)
- Tilde (~)

Les tirets et les points ne peuvent pas être les premiers caractères d'un mot de passe.

Si aucun n'est indiqué au cours de l'étape de création du magasin de clés de topologie, le `mot_de_passe_installation` prendra la valeur `ibmdop16`. Un menu contenant des étapes d'installation s'affiche.

5. Un contrat de licence est présenté. L'acceptation de la licence est nécessaire pour que l'installation puisse se poursuivre.
6. Sélectionnez une option dans le menu.

Tableau 20. Options d'installation

Sélection	Phase d'installation	Description de l'étape	Durée moyenne requise
1	Pré-contrôle	Valider les totaux de contrôle du support d'installation	15 minutes
2	Préparation	Copier les modèles vers le répertoire de topologie	2 minutes
3	Préparation	Créer un magasin de clés de topologie	1 minute
4	Préparation	Paramétrer toutes les topologies	2 minutes
5	Préparation	Chiffrer toutes les topologies	1 minute
6	Préparation	Exécuter "Configurer/Cibler" la topologie	5 minutes
7	Préparation	Exécuter les contrôles prérequis environnementaux	15 minutes
8	Installation	(Facultatif) Télécharger le support sur les serveurs cibles Si le support n'est pas téléchargé au cours de cette étape, il sera téléchargé à l'étape suivante. En téléchargeant le support à l'étape suivante, un point de contrôle peut être défini après avoir téléchargé le support.	1 heure
9	Installation	Exécuter une topologie d'installation de produits de base	3 heures 45 minutes
10	Installation	Exécuter une topologie à haute disponibilité de la configuration de produits	8 heures 15 minutes
11	Installation	Installer le composant Identity Management	1 heure 15 minutes
12	Installation	Préparer et configurer la gestion du cluster d'automatisation système	15 minutes
13	Installation	(Facultatif) Installer l'outil Data Studio	15 minutes
14	Installation	Installer l'outil de contrôle de plateforme	15 minutes
15	Installation	Installer l'outil de vérification du système	1 heure 30 minutes
16	Installation	(Facultatif) Installer et exécuter l'outil cyber hygiène une fois terminé. Avant d'exécuter l'outil cyber hygiène, il est recommandé de prendre un point de contrôle du système. Cyber hygiène exige que les paramètres de propriété soient définis dans le fichier de propriétés de la topologie. Vérifiez que ces paramètres ont été définis avant d'exécuter l'outil.	De 15 à 30 minutes

7. Reprenez à partir de l'étape 4, à la page 45 en sélectionnant les étapes d'installation dans l'ordre. Ne sélectionnez pas l'étape suivante tant que l'étape d'installation précédente n'est pas terminée. Ne redémarrez pas de serveurs jusqu'à ce que toutes les étapes se soient terminées avec succès. L'étape d'installation peut également être spécifiée dans la commande. Par exemple : `./dop.d1.install.sh 1 -p mot_de_passe_installation`.

Résultats

La progression de l'installation s'affiche. Elle est également enregistrée dans les journaux situés dans le répertoire `/rép_principale_install/dop16/log` du serveur d'installation.

La progression de l'outil Cyber hygiène sur le serveur d'installation s'affiche sur la console et est consignée dans le fichier `/tmp/dop.16.cyber-hygiene.log`. Une fois l'exécution terminée sur le serveur

d'installation, cyber hygiene peut continuer à fonctionner sur les autres serveurs IBM Defense Operations Platform. Pour déterminer la progression de l'outil cyber hygiene, exécutez la commande **ps -ef | grep hygiene**. Une fois l'exécution terminée, les fichiers journaux cyber hygiene sont stockés sur les autres serveurs IBM Defense Operations Platform, dans le répertoire `/var/cyber-hygiene/results/`. Chaque répertoire contiendra trois fichiers `.log`. Pour plus d'informations sur l'interprétation des fichiers journaux, consultez le fichier `/opt/IBM/iop/tools/ch/scripts-to-remotely-run-ch_DOP-1.6.doc` que vous trouverez sur le serveur d'installation, qui sera disponible une fois cyber hygiene exécuté.

Que faire ensuite

Si vous devez renouveler l'étape cyber hygiene (option 16), procédez au préalable comme suit :

1. Sur le serveur d'installation, modifiez le fichier `/install_home/dop16/topology/dop.d1.cyberhygiene.xml`.
2. Modifiez l'état de l'instance (Prêt ou Incertain, à mi-hauteur dans le fichier, sur la ligne contenant `type="runTool"` et `id="run_ch_i1"`) en spécifiant Nouveau.
3. Exécutez `./dop.d1.install.sh 15 -p mot_de_passe_installation` où `mot_de_passe_installation` représente le mot de passe de topologie.

Si le fichier `xml` n'est pas modifié avant la réexécution de l'étape cyber hygiene, on assistera à un report d'environ 10 secondes, mais aucune action ne sera effectuée.

Vérification de l'installation avant la configuration de post installation

Après l'exécution du programme d'installation, vérifiez qu'IBM Defense Operations Platform a été correctement installé avant de commencer les étapes de configuration de post-installation.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour arrêter tous les composants.
2. Vérifiez que tous les composants se sont arrêtés correctement en consultant les messages affichés.
3. Arrêtez le système d'exploitation Linux sur tous les serveurs.
4. Mettez hors tension puis sous tension tous les serveurs d'exécution, ou réamorçez tous les serveurs.
5. Utilisez l'outil de contrôle de plateforme pour démarrer tous les composants.
6. Utilisez l'outil de contrôle de plateforme pour interroger le statut de tous les composants.
7. Exécutez tous les tests de l'outil de vérification du système.
8. Assurez-vous que tous les tests ont été exécutés correctement.

Que faire ensuite

Si des erreurs sont signalées, corrigez-les et exécutez cette procédure à nouveau.

Tâches associées:

«Utilisation de l'outil de vérification du système», à la page 69

L'outil de vérification du système permet de déterminer l'état opérationnel des services comprenant le système IBM Defense Operations Platform.

«Interrogation du statut des composants dans Field Edition», à la page 60

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés dans IBM Defense Operations Platform Field Edition.

«Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Démarrage des composants dans Field Edition», à la page 58

l'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Démarrage des composants dans Command Center Edition», à la page 63
outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Field Edition», à la page 59
outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Arrêt des composants dans Command Center Edition», à la page 64
L'L' outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Configuration de post-installation d'IBM Defense Operations Platform

Après avoir installé IBM Defense Operations Platform, vous devez effectuer plusieurs étapes de configuration de post-installation pour terminer l'installation.

Configuration des services de collaboration pour IPv6

Si votre installation utilise le réseau IPv6, des étapes de configuration sont requises pour les services de collaboration.

Pourquoi et quand exécuter cette tâche

L'architecture d'IBM Defense Operations Platform doit être installée avant toute configuration du réseau IPv6 pour les services de collaboration.

Procédure

1. Suivez la procédure décrite dans la documentation Lotus Domino afin de configurer Lotus Domino pour l'adressage IPv6.
2. Suivez la procédure décrite dans la documentation Lotus Sametime Standard afin de configurer Lotus Sametime Standard pour l'adressage IPv6.
3. Suivez la procédure décrite dans la documentation WebSphere Portal pour configurer la sécurisation du portlet Sametime Contact List si vous n'utilisez pas un réseau IPv4 avec une adresse IPv4 affectée au serveur d'applications.

Information associée:

-  Configuration de Lotus Domino pour l'adressage IPv6
-  Configuration de Sametime Community Server pour la prise en charge d'IPv6
-  Configuration de la sécurisation du portlet Liste de contacts Sametime

Configuration de la connexion unique pour les services de collaboration

Importez le jeton LTPA SSO WebSphere Portal sur le serveur d'applications pour permettre aux utilisateurs d'accéder aux services de collaboration sans avoir à saisir à nouveau leurs données d'identification.

Avant de commencer

Un client Lotus Notes 8.5.x est requis pour réaliser cette tâche. Un client Notes peut être utilisé ou installé sur un client Windows à l'aide du fichier notes_designer_admin853_w32en.exe situé dans le dossier /distributionMedia sur le serveur d'installation. Le poste de travail doit être en mesure de se connecter au serveur d'applications via le protocole TCP/IP à l'aide du nom d'hôte complet.

Pourquoi et quand exécuter cette tâche

Vous devez installer l'architecture d'IBM Defense Operations Platform préalablement à l'importation du jeton LTPA (Lightweight Third-Party Authentication).

Ce jeton a été créé lors de l'installation de l'architecture d'IBM Defense Operations Platform.

Procédure

1. Installez un client Lotus Notes 8.5.x sur un poste de travail. Il est possible d'utiliser une installation existante. Le poste de travail doit être en mesure de se connecter au serveur d'applications via le protocole TCP/IP à l'aide du nom d'hôte complet.
2. Copiez le fichier `/opt/IBM/ISP/stproxy.ltpa` du serveur d'applications sur le poste de travail exécutant Lotus Notes. Il s'agit du jeton LTPA qui sera importé dans le répertoire de service de collaboration.
3. Copiez le fichier `/local/notesdata/admin.id` du serveur d'applications sur le poste de travail exécutant Lotus Notes. Il s'agit du fichier d'ID de l'administrateur du service de collaboration. Cet ID vous servira à vous connecter au répertoire des services de collaboration.
4. Sur le poste de travail, démarrez le client Lotus Notes et connectez-vous à l'aide du fichier `admin.id`.
 - a. Dans le panneau de connexion de Lotus Notes, cliquez sur **Nom de l'utilisateur**.
 - b. Accédez au répertoire dans lequel vous avez copié le fichier `admin.id` et sélectionnez-le.
 - c. Entrez le mot de passe défini dans le fichier de propriétés de la topologie pour la propriété `DOMINO.ADMIN.PWD`.
 - d. Cliquez sur **Oui** si un avertissement de sécurité s'affiche.
5. Ouvrez le fichier `names.nsf`.
 - a. Cliquez sur **Fichier > Ouvrir > Application Lotus Notes**.
 - b. Entrez le nom d'hôte complet du serveur d'applications dans **Rechercher**.
 - c. Entrez `names.nsf` dans **Nom de fichier**.
 - d. Cliquez sur **Ouvrir**.
6. Naviguez jusqu'à **Web > Web Configurations**.
7. Sélectionnez **Web SSO Configuration for LTPA Token** et cliquez sur **Edit Document**.
8. Cliquez sur **Clés > Import WebSphere LTPA Keys**. Cliquez sur **OK** si un avertissement s'affiche pour indiquer l'écrasement des clés existantes.
9. Entrez le chemin dans lequel le fichier `stproxy.ltpa` a été copié. Cliquez sur **OK**.
10. Entrez le mot de passe du jeton LTPA. Le mot de passe est défini pour la propriété `WAS.LTPA.PWD` dans le fichier de propriétés de la topologie.
11. Dans **Token Format** sélectionnez `LtpaToken2`.
12. Cliquez sur **OK > Sauvegarder et fermer**.
13. Dans **Field Edition**, redémarrez le service de collaboration à l'aide de l'outil de contrôle de plateforme.
 - a. Connectez-vous au serveur de gestion, puis ouvrez une fenêtre de terminal.
 - b. Exécutez `su -ibmadmin`.
 - c. Exécutez `DOPControl -a stop -c collab -p mot_de_passe`, où `mot_de_passe` correspond au mot de passe de l'outil de contrôle de plateforme, défini lors de l'installation de l'outil de contrôle de plateforme.
 - d. Exécutez `DOPControl -a start -c collab -p mot_de_passe`, où `mot_de_passe` correspond au mot de passe de l'outil de contrôle de plateforme, défini lors de l'installation de l'outil de contrôle de plateforme.
14. Dans **Command Center Edition**, redémarrez le service de collaboration à l'aide de l'outil de contrôle de plateforme.
 - a. Connectez-vous au serveur de gestion, puis ouvrez une fenêtre de terminal.

- b. Exécutez `su -ibmadmin`.
- c. Exécutez `DOPControl -a stop -c collabpri -p mot_de_passe`, où `mot_de_passe` correspond au mot de passe de l'outil de contrôle de plateforme, défini lors de l'installation de l'outil de contrôle de plateforme.
- d. Exécutez `DOPControl -a start -c collabpri -p mot_de_passe`, où `mot_de_passe` correspond au mot de passe de l'outil de contrôle de plateforme, défini lors de l'installation de l'outil de contrôle de plateforme.

Définition du délai d'expiration de session

Le délai d'expiration de session détermine la durée pendant laquelle un utilisateur peut rester inactif avant que la session ne soit fermée et que l'utilisateur n'ait à se reconnecter. Ce délai d'attente s'applique également aux administrateurs qui sont connectés via le service de portail.

Pourquoi et quand exécuter cette tâche

Au moment de l'installation d'IBM Defense Operations Platform, aucun délai d'expiration de session n'est défini. Les utilisateurs restent connectés jusqu'à ce qu'ils décident de se déconnecter, même si la session est inactive.

Si votre organisation a mis en place des règles de sécurité imposant des délais d'expiration de session après une période d'inactivité, utilisez la procédure suivante afin de définir des délais d'expiration de session personnalisés pour votre système IBM Defense Operations Platform.

Procédure

Configurez les délais d'attente des serveurs.

1. Sur le Field Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications.
2. Sur le Command Center Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications 1.
3. Connectez-vous en tant qu'utilisateur admin avec le mot de passe défini pour `PORTAL.ADMIN.ACCOUNT.PWD` dans le fichier de propriétés de la topologie.
4. Cliquez sur **Serveurs > Type de serveur > WebSphere Application Servers > WebSphere Portal**.
5. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
6. Entrez la valeur de délai d'attente en minutes.
7. Cliquez sur **OK**.
8. Cliquez sur **Sauvegarder**.
9. Cliquez sur **Serveurs > Type de serveur > Serveurs d'applications WebSphere > STProxyServer1**.
10. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
11. Entrez la valeur de délai d'attente en minutes.
12. Cliquez sur **OK**.
13. Cliquez sur **Sauvegarder**.

Dans Command Center Edition, configurez les serveurs supplémentaires suivants.

14. Cliquez sur **Serveurs > Type de serveur > WebSphere Application Servers > WebSphere_Portal_PortalNode2**.
15. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
16. Entrez la valeur de délai d'attente en minutes.
17. Cliquez sur **OK**.

18. Cliquez sur **Sauvegarder**.

Redémarrez le serveur.

19. Arrêtez et redémarrez le serveur d'applications dans Field Edition ou serveur d'applications 1 dans Command Center Edition à l'aide de l'outil de contrôle de plateforme.

Configuration d'un serveur LDAP de services de collaboration secondaire dans Command Center Edition

Un serveur LDAP secondaire est requis pour les services de collaboration lors d'une exécution dans Command Center Edition.

Procédure

1. Installez un client Lotus Notes 8.5.x sur un poste de travail. Il est possible d'utiliser une installation existante. Le poste de travail doit être en mesure de se connecter au serveur d'applications 1 via le protocole TCP/IP à l'aide du nom d'hôte complet.
2. Copiez le fichier `/local/notesdata/admin.id` du serveur d'applications 1 sur le poste de travail exécutant Lotus Notes. Il s'agit du fichier d'ID de l'administrateur du service de collaboration. Cet ID vous servira à vous connecter au répertoire des services de collaboration.
3. Sur le poste de travail, démarrez le client Lotus Notes et connectez-vous à l'aide du fichier `admin.id`.
 - a. Dans le panneau de connexion de Lotus Notes, cliquez sur **Nom de l'utilisateur**.
 - b. Accédez au répertoire dans lequel vous avez copié le fichier `admin.id` et sélectionnez-le.
 - c. Entrez le mot de passe défini dans le fichier de propriétés de la topologie pour la propriété `DOMINO.ADMIN.PWD`.
 - d. Cliquez sur **Oui** si un avertissement de sécurité s'affiche.
4. Ouvrez le fichier `names.nsf`.
 - a. Cliquez sur **Fichier > Ouvrir > Application Lotus Notes**.
 - b. Entrez le nom d'hôte complet du serveur d'applications 1 dans **Rechercher**.
 - c. Entrez `names.nsf` dans **Nom de fichier**.
 - d. Cliquez sur **Ouvrir**.
5. Ouvrez le fichier `da.nsf`.
 - a. Cliquez sur **Fichier > Ouvrir > Application Lotus Notes**.
 - b. Entrez le nom de système hôte qualifié complet du serveur d'applications 1 dans **Chercher dans**.
 - c. Entrez `da.nsf` dans **Nom de fichier**.
 - d. Cliquez sur **Ouvrir**.
6. Dupliquez l'entrée d'assistance d'annuaire existante.
7. Mettez à jour l'entrée d'assistance d'annuaire dupliquée.
 - a. Dans l'onglet **Concepts de base**, définissez **Autorisation de groupe** sur Non.
 - b. Pour **Ordre de recherche**, indiquez 2.
 - c. Dans l'onglet **LDAP**, modifiez **Hôte LDAP** en remplaçant votre nom d'hôte LDAP principal par votre nom d'hôte LDAP secondaire.
8. Ouvrez le fichier `stconfig.nsf`.
 - a. Cliquez sur **Fichier > Ouvrir > Application Lotus Notes**.
 - b. Entrez le nom de système hôte qualifié complet du serveur d'applications 1 dans **Chercher dans**.
 - c. Entrez `stconfig.nsf` dans **Nom de fichier**.
 - d. Cliquez sur **Ouvrir**.
9. Cliquez sur **Par formulaire**.
10. Dupliquez le formulaire `LDAPServer`.
11. Mettez à jour le formulaire dupliqué.

- a. Pour **Connexion LDAP**, indiquez le nom d'hôte qualifié complet de votre LDAP secondaire.
 - b. Pour **Ordre de recherche**, indiquez 2.
12. Redémarrez les services de collaboration.
- a. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadmin`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadmin` en exécutant la commande `su - ibmadmin`.
 - a. Exécutez les commandes suivantes :


```
DOPControl -a stop -c colsby -p mot_de_passe
DOPControl -a stop -c colpri -p mot_de_passe
DOPControl -a start -c colpri -p mot_de_passe
DOPControl -a start -c colsby -p mot_de_passe
```

où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé.

Configuration d'autres relations de gestionnaires de grappes dans Command Center Edition

Une fois IBM Defense Operations Platform Command Center Edition installé, les relations des gestionnaires de grappes doivent être configurées.

Pourquoi et quand exécuter cette tâche

Si cette configuration n'est pas effectuée, un arrêt anormal non contrôlé du serveur de données principal se produit ou son interface réseau ne commute pas la base de données sur le serveur de données de secours. Lorsque la reprise en ligne échoue, IBM Defense Operations Platform devient inutilisable.

Procédure

1. Connectez-vous au serveur de messagerie 1.
2. Ouvrez une fenêtre de terminal.
3. Si vous n'êtes pas connecté en tant qu'utilisateur `root`, exécutez la commande `su - root` pour basculer vers le superutilisateur.
4. Exécutez `cd rép_principal_install/dop16/bin` où `rép_principal_install` est le répertoire dans lequel les fichiers d'installation ont été copiés lors de l'installation de IBM Defense Operations Platform.
5. Exécutez `./dop-env.sh`
6. Exécutez `./ba.sh installTopology -t dop.ha.tsapatch -p mot_de_passe_installation` où `mot_de_passe_installation` correspond au mot de passe d'installation défini lors de l'installation de IBM Defense Operations Platform.

Configuration du système NFS externe facultatif dans Command Center Edition

Le système de fichiers NFS (Network File System) externe facultatif est configuré à l'aide d'un script.

Pourquoi et quand exécuter cette tâche

Le système de fichier réseau externe permet de fournir une solution plus robuste de reprise en ligne pour les services de messagerie.

Procédure

1. Connectez-vous au serveur d'installation en tant qu'utilisateur `root`.
2. Accédez au répertoire `rép_principal_install/dop16/bin`.
3. Exécutez la commande `./dop-env.sh`.

4. Exécutez la commande `./dop.ha.wmqextnfs.sh -p mot_de_passe_installation`. Le `mot_de_passe_installation` est celui qui a été indiqué lorsque IBM Defense Operations Platform a été installé ou a été modifié ultérieurement. S'il n'est pas indiqué, `mot_de_passe_installation` prend par défaut la valeur `ibmdop16`. Un menu contenant des étapes d'installation s'affiche.
5. Sélectionnez une option dans le menu.

Tableau 21. Options de configuration du système NFS externe

Sélection	Phase	Description de l'étape	Durée moyenne requise
1	Préparation	Copier le modèle vers le répertoire de topologie	1 minute
2	Préparation	Paramétrer la topologie	1 minute
3	Préparation	Chiffrer la topologie	1 minute
4	Installation	Installer le système NFS externe	7 minutes

6. Reprenez à partir de l'étape 4 en sélectionnant les étapes d'installation dans l'ordre. Ne sélectionnez pas l'étape suivante tant que l'étape d'installation précédente n'est pas terminée. L'étape d'installation peut également être spécifiée dans la commande. Par exemple : `./dop.d1.wmqextnfs.sh 1 -p mot_de_passe_installation`.

Résultats

La progression de l'installation s'affiche. Elle est également enregistrée dans les journaux situés dans le répertoire `/install_home/dop16/log` du serveur d'installation.

Configuration du nom d'hôte de l'outil d'administration Web Tivoli Directory Server

Le nom d'hôte de la serveur de données doit être configuré dans l'outil d'administration Web de Tivoli Directory Server afin de pouvoir utiliser cet outil.

Procédure

1. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante : `http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
2. Connectez-vous en tant qu'utilisateur `superadmin` et cliquez sur **Administration de la console > Gérer le serveur de console**. Entrez le nom de DNS complet de la serveur de données dans **Nom_hôte** et cliquez sur **OK**.

Activation de la journalisation Tivoli Directory Server

Activez la journalisation Tivoli Directory Server pour faciliter le débogage des erreurs Tivoli Directory Server.

Procédure

1. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante : `http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
2. Cliquez sur **Administration du serveur > Journaux > Modifier les paramètres du journal > Sélectionner le journal d'audit du serveur**.
3. Cliquez sur **Modifier les paramètres**.
4. Modifiez les paramètres suivants :
 - Dans **Journal d'audit du serveur**, sélectionnez **Activer la journalisation d'audit du serveur**.
 - Dans **Niveau du journal d'audit**, sélectionnez **Toutes les tentatives**.

- Dans **Performances d'audit**, sélectionnez **Activer l'audit pour les données de performance**.
- Dans **Opérations à consigner**, sélectionnez tous les éléments.

5. Cliquez sur **Terminé**.

Suppression des fichiers d'installation du système de production

Pendant l'installation d'IBM Defense Operations Platform, la configuration du service d'installation, le support d'installation, et les fichiers journaux sont enregistrés sur les serveurs. Une fois l'installation terminée et vérifiée, les fichiers dédiés uniquement à l'installation peuvent être supprimés des serveurs du système de production.

Les éléments suivants peuvent être archivés et supprimés de tous les serveurs :

- Le répertoire défini par la propriété `Unix.image.basedir.remote` dans le fichier de propriétés de la topologie. L'emplacement par défaut est `installMedia/dop/image`.
- Le répertoire défini par la propriété `Unix.script.basedir.remote` dans le fichier de propriétés de la topologie. L'emplacement par défaut est `installMedia/dop/script`.

Les éléments suivants peuvent être archivés et supprimés du serveur d'installation, lequel correspond au serveur de messagerie dans Field Edition et au serveur de messagerie 1 dans Command Center Edition.

- Le répertoire défini par la propriété `image.basedir.local` du fichier `custom.properties`. L'emplacement par défaut est `/distributionMedia`.
- Le répertoire défini par la propriété `image.tempdir.local` du fichier `custom.properties`. L'emplacement par défaut est `/tmp/dop/images`.
- Le répertoire défini par la propriété `backup.basedir.local` du fichier `custom.properties`. L'emplacement par défaut est `/tmp/dop/backup`.

Etant donné que le fichier de propriétés de la topologie sur le serveur d'installation contient des mots de passe en texte clair, il doit être conservé dans un emplacement sécurisé.

Les fichiers de propriétés de la topologie sont les suivants :

- Field Edition: `rep_base_install/dop16/topology/dop.d2.properties`
- Command Center Edition : `rep_base_install/dop16/topology/dop.d1.properties`

Vérification de l'installation

Après avoir installé IBM Defense Operations Platform Command Center Edition ou Field Edition, vérifiez que le produit a été correctement installé. La vérification assure que tous les composants sont démarrés et fonctionnent comme prévu.

Pourquoi et quand exécuter cette tâche

Deux procédures de vérification sont fournies. La procédure de vérification rapide peut être utilisée juste après l'installation d'IBM Defense Operations Platform et chaque fois qu'une vérification rapide du système global est désirée. La procédure de vérification complète prend beaucoup plus de temps, mais doit être effectuée avant qu'IBM Defense Operations Platform ne soit considéré comme pleinement opérationnel.

Procédure

Vérification rapide

1. Exécutez tous les tests de l'outil de vérification du système.
2. Assurez-vous que tous les tests ont été exécutés correctement.

3. Utilisez l'outil de contrôle de plateforme pour démarrer tous les composants qui doivent être démarrés.

Vérification complète

4. Utilisez l'outil de contrôle de plateforme pour arrêter tous les composants.
5. Vérifiez que tous les composants se sont arrêtés correctement en consultant les messages affichés.
6. Arrêtez le système d'exploitation Linux sur tous les serveurs.
7. Mettez hors tension puis sous tension tous les serveurs d'exécution, ou réamorces tous les serveurs.
8. Utilisez l'outil de contrôle de plateforme pour démarrer tous les composants.
9. Utilisez l'outil de contrôle de plateforme pour interroger le statut de tous les composants.
10. Exécutez tous les tests de l'outil de vérification du système.
11. Assurez-vous que tous les tests ont été exécutés correctement.

Que faire ensuite

Si des erreurs sont signalées, corrigez-les et exécutez cette procédure à nouveau.

Tâches associées:

«Utilisation de l'outil de vérification du système», à la page 69

L'outil de vérification du système permet de déterminer l'état opérationnel des services comprenant le système IBM Defense Operations Platform.

«Interrogation du statut des composants dans Field Edition», à la page 60

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés dans IBM Defense Operations Platform Field Edition.

«Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Démarrage des composants dans Field Edition», à la page 58

L'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Démarrage des composants dans Command Center Edition», à la page 63

L'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Field Edition», à la page 59

L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Arrêt des composants dans Command Center Edition», à la page 64

L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Installation d'IBM Defense Operations Platform Workbench Edition

IBM Defense Operations Platform Workbench Edition contient des produits qui offrent des fonctionnalités supplémentaires à IBM Defense Operations Platform.

IBM Defense Operations Platform Workbench Edition inclut les produits suivants :

- Rational Build Forge Enterprise Edition 7.1.3
- Lotus Expeditor 6.2.3
- Rational Requirements Composer 4.0
- Rational License Key Server 8.1.3
- IBM Java SDK/JRE 7.0.5
- IBM Forms Experience Builder 8.5

- IBM Integration Designer 8.5
- InfoSphere Data Architect 9.1
- Rational RequisitePro 7.1.4
- IBM Forms Server 8.0.1
- Rational Asset Manager Enterprise Edition 7.5.2
- Rational Quality Manager 4.0.4
- Rational Team Concert 4.0.4
- Rational Software Architect for WebSphere Software 8.5.5
- Rational Functional Tester 8.5
- Rational Service Tester for SOA Quality 8.5
- Rational Performance Tester 8.5 Security AppScan Standard 8.7

Ces produits sont installés à l'aide des programmes et des instructions d'installation fournis. IBM Defense Operations Platform ne contient pas d'instructions ou de méthodes d'installation spécifiques dans le cadre de l'installation de ces produits au sein de l'environnement IBM Defense Operations Platform.

Ces produits, inclus dans Workbench Edition sont exclusivement destinés à une utilisation avec IBM Defense Operations Platform.

Chapitre 3. Gestion de la solution

Vous pouvez exécuter les types de tâche administrative suivants pour IBM Defense Operations Platform.

Accès aux consoles d'administration IBM Defense Operations Platform

IBM Defense Operations Platform est constitué d'un certain nombre de produits. Chacun de ces produits possède une ou plusieurs consoles d'administration. Pour faciliter la recherche des consoles d'administration installées, IBM Defense Operations Platform fournit des pages à partir desquelles il est possible d'accéder aux consoles.

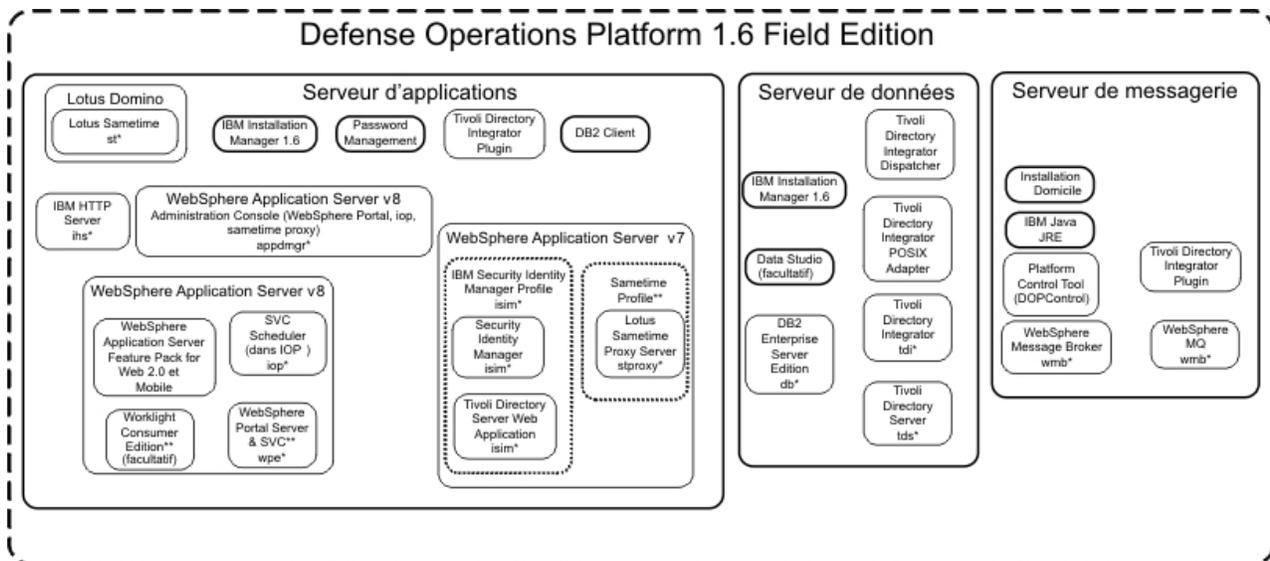
Procédure

- Pour accéder aux consoles d'administration installées avec Field Edition, allez à https://serveur_applications/dop/DOP16_D2_Admin_URLs.htm où *serveur_applications* est le nom d'hôte du serveur d'applications. Vous trouverez le nom d'hôte du serveur d'applications dans le fichier *base_installation/dop16/topology/dop.d2.properties* dans la propriété APP.1.HOST.
- Pour accéder aux consoles d'administration installées avec Command Center Edition, allez à https://serveur_processus/dop/DOP16_D1_Admin_URLs.htm où *serveur_processus* est le nom d'hôte du serveur de processus. Vous trouverez le nom d'hôte du serveur de processus dans le fichier *base_installation/dop16/topology/dop.d1.properties* dans la propriété PRO.1.HOST.

Démarrage, arrêt et interrogation du statut dans Field Edition

l'outil de contrôle de plateforme permet à un utilisateur d'arrêter, de démarrer et d'interroger les composants IBM Defense Operations Platform qui s'exécutent dans Field Edition. Un outil de contrôle de plateforme est également disponible pour IBM Defense Operations Platform s'exécutant dans Command Center Edition.

La figure 1, à la page 58 répertorie les produits et composants de IBM Defense Operations Platform Field Edition et de leurs composants de contrôle de plateforme.



*Nom de composant DOPControl
 ** Managed by WebSphere Application Server v8 administration console

Figure 1. Composants Field Edition

Concepts associés:

«Démarrage, arrêt, gestion et interrogation du statut dans Command Center Edition», à la page 62 outil de contrôle de plateforme permet à un utilisateur d'arrêter, de démarrer et d'interroger les services IBM Defense Operations Platform qui s'exécutent dans Command Center Edition. Un outil de contrôle de plateforme est également disponible pour IBM Defense Operations Platform s'exécutant dans Field Edition.

Démarrage des composants dans Field Edition

outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Field Edition.

Pourquoi et quand exécuter cette tâche

La commande DOPControl doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Avvertissement : Seuls les administrateurs d'IBM Defense Operations Platform expérimentés sont habilités à démarrer des composants individuels. Des résultats imprévisibles peuvent se produire si les composants ne sont pas démarrés dans un ordre précis.

Procédure

Sur le serveur de messagerie, exécutez la commande ci-après pour démarrer tous les composants IBM Defense Operations Platform.

```
DOPControl -a start -c all -p mot_de_passe
```

où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

Les composants sont démarrés dans l'ordre requis. Les composants prérequis sont démarrés avant les composants dépendants. Par exemple, les composants de base de données et de répertoire sont démarrés en premier.

Avertissement : L'arrêt de tous les composants peut prendre 45 minutes, voire davantage. Pour démarrer un seul composant, exécutez la commande suivante.

```
DOPControl -a start -c composant -p mot_de_passe
```

où *composant* est un ID répertorié dans la section **Options de cible** dans l'aide de DOPControl et où *mot_de_passe* est le mot de passe de topologie défini lors de l'installation d'IBM Defense Operations Platform. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

L'option `nostatus` peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

Les composants IBM Defense Operations Platform demandés sont démarrés.

Que faire ensuite

Après l'exécution de la commande DOPControl, consultez les journaux contenus dans le répertoire /opt/IBM/ISP/mgmt/logs. Les journaux contiennent les résultats de la commande DOPControl la plus récente.

Tâches associées:

«Arrêt des composants dans Field Edition»

l'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Interrogation du statut des composants dans Field Edition», à la page 60

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés dans IBM Defense Operations Platform Field Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Field Edition», à la page 61

Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans Field Edition.

Arrêt des composants dans Field Edition

l'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Field Edition.

Pourquoi et quand exécuter cette tâche

La commande DOPControl doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Avertissement : Seuls des administrateurs d'IBM Defense Operations Platform expérimentés sont habilités à arrêter des composants individuels. Des résultats imprévisibles peuvent se produire si des composants ne sont pas arrêtés dans l'ordre requis.

Procédure

Sur le serveur de messagerie, exécutez la commande ci-après pour arrêter tous les composants IBM Defense Operations Platform.

```
DOPControl -a stop -c all -p mot_de_passe
```

où *mot_de_passe* est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

Avertissement : L'arrêt de tous les composants peut prendre 45 minutes, voire davantage. Pour arrêter un composant unique, exécutez la commande suivante.

```
DOPControl -a stop -c composant -p mot_de_passe
```

où *composant* est un ID répertorié dans la section **Options de cible** dans l'aide de DOPControl et où *mot_de_passe* est le mot de passe de topologie défini lors de l'installation d'IBM Defense Operations Platform. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

L'option `nostatus` peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

Les composants IBM Defense Operations Platform demandés sont arrêtés.

Que faire ensuite

Après l'exécution de la commande DOPControl, consultez les journaux contenus dans le répertoire /opt/IBM/ISP/mgmt/logs. Les journaux contiennent les résultats de la commande DOPControl la plus récente.

Tâches associées:

«Démarrage des composants dans Field Edition», à la page 58

L'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Interrogation du statut des composants dans Field Edition»

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés dans IBM Defense Operations Platform Field Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Field Edition», à la page 61

Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans Field Edition.

Interrogation du statut des composants dans Field Edition

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés dans IBM Defense Operations Platform Field Edition.

Pourquoi et quand exécuter cette tâche

La commande DOPControl doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Procédure

Sur le serveur de messagerie, exécutez la commande ci-après pour interroger l'état de tous les composants IBM Defense Operations Platform.

```
DOPControl -a status -c all -p mot_de_passe
```

où *mot_de_passe* est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets

simples. Par exemple : 'pass\$phrase'

Pour vérifier un seul composant, exécutez la commande suivante.

```
DOPControl -a status -c composant -p mot_de_passe
```

où *composant* est un ID répertorié dans la section **Options de cible** dans l'aide de DOPControl et où *mot_de_passe* est le mot de passe de topologie défini lors de l'installation d'IBM Defense Operations Platform. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

Résultats

Les composants qui sont démarrés sont identifiés par **[on]**. Les composants non démarrés sont identifiés par **[off]**.

Que faire ensuite

Après l'exécution de la commande DOPControl, consultez les journaux contenus dans le répertoire /opt/IBM/ISP/mgmt/logs. Les journaux contiennent les résultats de la commande DOPControl la plus récente.

Tâches associées:

«Démarrage des composants dans Field Edition», à la page 58

outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Arrêt des composants dans Field Edition», à la page 59

outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Field Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Field Edition»

Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans Field Edition.

Obtention de l'aide pour l'outil de contrôle de plateforme dans Field Edition

Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans Field Edition.

Pourquoi et quand exécuter cette tâche

La commande DOPControl doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Procédure

Sur le serveur de messagerie, exécutez l'une des commandes suivantes pour afficher les options de la commande DOPControl.

```
DOPControl -a help  
ou DOPControl -h
```

La commande peut également être exécutée sans chemin d'accès. Par exemple, `DOPControl -h`.

Résultats

Les options de la commande DOPControl sont affichées.

Tâches associées:

Démarrage des composants dans Command Center Edition

l'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Pourquoi et quand exécuter cette tâche

La commande `DOPControl` doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Avertissement : Seuls les administrateurs d'IBM Defense Operations Platform expérimentés sont habilités à démarrer des composants individuels. Des résultats imprévisibles peuvent se produire si les composants ne sont pas démarrés dans un ordre précis.

Procédure

1. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadmin`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadmin` en exécutant la commande `su - ibmadmin`. Dans des conditions normales d'exploitation, utilisez l'outil de contrôle de plateforme sur le serveur de messagerie 1. Si le serveur de messagerie 1 n'est pas disponible, vous pouvez exécuter l'outil de contrôle de plateforme sur le serveur de messagerie 2. N'utilisez pas l'outil de contrôle de plateforme à la fois sur le serveur de messagerie 1 et sur le serveur de messagerie 2, des résultats imprévisibles risqueraient de se produire.
2. Exécutez la commande suivante pour démarrer tous les composants d'IBM Defense Operations Platform.

```
DOPControl -a start -c all -p mot_de_passe
```

où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

Les composants sont démarrés dans l'ordre requis. Les composants prérequis sont démarrés avant les composants dépendants. Par exemple, les composants de base de données et de répertoire sont démarrés en premier.

Avertissement : L'arrêt de tous les composants peut prendre 45 minutes, voire davantage.

Pour démarrer un seul composant, exécutez la commande suivante.

```
DOPControl -a start composant -p mot_de_passe
```

où `composant` est un ID répertorié dans l'aide de `DOPControl` et où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

L'option `nostatus` peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

Les composants IBM Defense Operations Platform demandés sont démarrés.

Tâches associées:

«Arrêt des composants dans Command Center Edition», à la page 64

L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Gestion des composants HADR dans Command Center Edition», à la page 66

l'outil de contrôle de plateforme offre des composants d'administration système IBM Defense Operations Platform Command Center Edition. Ces composants Command Center Edition permettent à

l'administrateur de gérer des conditions uniques. Ces commandes doivent être utilisées avec prudence. «Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65 L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition. «Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition», à la page 68 Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Arrêt des composants dans Command Center Edition

L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Pourquoi et quand exécuter cette tâche

La commande `DOPControl` doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Avvertissement : Seuls des administrateurs d'IBM Defense Operations Platform expérimentés sont habilités à arrêter des composants individuels. Des résultats imprévisibles peuvent se produire si des composants ne sont pas arrêtés dans l'ordre requis.

Procédure

1. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadmin`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadmin` en exécutant la commande `su - ibmadmin`. Dans des conditions normales d'exploitation, utilisez l'outil de contrôle de plateforme sur le serveur de messagerie 1. Si le serveur de messagerie 1 n'est pas disponible, vous pouvez exécuter l'outil de contrôle de plateforme sur le serveur de messagerie 2. N'utilisez pas l'outil de contrôle de plateforme à la fois sur le serveur de messagerie 1 et sur le serveur de messagerie 2, des résultats imprévisibles risqueraient de se produire.
2. Exécutez la commande suivante pour arrêter tous les composants d'IBM Defense Operations Platform.
`DOPControl -a stop -c all -p mot_de_passe`

où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

Avvertissement : L'arrêt de tous les composants peut prendre 45 minutes, voire davantage. Pour arrêter un composant unique, exécutez la commande suivante.

```
DOPControl -a stop -c composant -p mot_de_passe
```

où `composant` est un ID répertorié dans l'aide de `DOPControl` et où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

L'option `nostatus` peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

Les composants IBM Defense Operations Platform demandés sont arrêtés.

Tâches associées:

«Démarrage des composants dans Command Center Edition», à la page 63
l'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Gestion des composants HADR dans Command Center Edition», à la page 66
l'outil de contrôle de plateforme offre des composants d'administration système IBM Defense Operations Platform Command Center Edition. Ces composants Command Center Edition permettent à l'administrateur de gérer des conditions uniques. Ces commandes doivent être utilisées avec prudence.

«Interrogation du statut des composants dans un environnement Command Center Edition»
L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition», à la page 68
Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Interrogation du statut des composants dans un environnement Command Center Edition

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Pourquoi et quand exécuter cette tâche

La commande `DOPControl` doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Procédure

1. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadmin`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadmin` en exécutant la commande `su - ibmadmin`. Dans des conditions normales d'exploitation, utilisez l'outil de contrôle de plateforme sur le serveur de messagerie 1. Si le serveur de messagerie 1 n'est pas disponible, vous pouvez exécuter l'outil de contrôle de plateforme sur le serveur de messagerie 2. N'utilisez pas l'outil de contrôle de plateforme à la fois sur le serveur de messagerie 1 et sur le serveur de messagerie 2, des résultats imprévisibles risqueraient de se produire.
2. Exécutez la commande suivante pour interroger le statut de tous les composants d'IBM Defense Operations Platform.

```
DOPControl -a status -c all -p mot_de_passe
```

où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

Pour vérifier un seul composant, exécutez la commande suivante.

```
DOPControl -a status -c composant -p mot_de_passe
```

où `composant` est un ID répertorié dans l'aide de `DOPControl` et où `mot_de_passe` est le mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du `mot_de_passe` contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : `'pass$phrase'`

Résultats

Les composants qui sont démarrés sont identifiés par **[on]**. Les composants non démarrés sont identifiés par **[off]**.

Tâches associées:

«Démarrage des composants dans Command Center Edition», à la page 63
outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Command Center Edition», à la page 64
L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Gestion des composants HADR dans Command Center Edition»
outil de contrôle de plateforme offre des composants d'administration système IBM Defense Operations Platform Command Center Edition. Ces composants Command Center Edition permettent à l'administrateur de gérer des conditions uniques. Ces commandes doivent être utilisées avec prudence.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition», à la page 68
Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Gestion des composants HADR dans Command Center Edition

outil de contrôle de plateforme offre des composants d'administration système IBM Defense Operations Platform Command Center Edition. Ces composants Command Center Edition permettent à l'administrateur de gérer des conditions uniques. Ces commandes doivent être utilisées avec prudence.

Pourquoi et quand exécuter cette tâche

La commande `DOPControl` doit être exécutée avec l'utilisateur `ibmadmin`. Si vous n'êtes pas connecté en tant qu'utilisateur `ibmadmin`, exécutez la commande `su - ibmadmin` pour basculer vers l'utilisateur `ibmadmin`.

Avertissement : La gestion des composants de reprise à haut niveau de disponibilité après incident (HADR) ne doit être effectuée que par des administrateurs expérimentés d'IBM Defense Operations Platform.

Procédure

1. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadmin`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadmin` en exécutant la commande `su - ibmadmin`. Dans des conditions normales d'exploitation, utilisez l'outil de contrôle de plateforme sur le serveur de messagerie 1. Si le serveur de messagerie 1 n'est pas disponible, vous pouvez exécuter l'outil de contrôle de plateforme sur le serveur de messagerie 2. N'utilisez pas l'outil de contrôle de plateforme à la fois sur le serveur de messagerie 1 et sur le serveur de messagerie 2, des résultats imprévisibles risqueraient de se produire.
2. Exécutez la commande suivante avec l'option de commande d'administration système souhaitée.

```
DOPControl -a action -c composant -p mot_de_passe
```

où *action* peut être l'une des valeurs suivantes :

activate

Activation des composants DB2 HADR.

deactivate

Désactivation des composants DB2 HADR.

resume Reprise des composants DB2 HADR.

suspend

Interruption des composants DB2 HADR.

La valeur *composant* dépend de l'action spécifiée. Vous obtiendrez les valeurs de *composant* valides en exécutant la commande `DOPControl -h`.

mot_de_passe correspond au mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

L'option *nostatus* peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

L'action demandée est effectuée.

Tâches associées:

«Démarrage des composants dans Command Center Edition», à la page 63
l'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Command Center Edition», à la page 64
L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65
L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition», à la page 68
Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Montage et démontage manuels du répertoire WebSphere Message Broker

Le répertoire `/opt/ibm/ioc/shared/wmq` est partagé entre les instances WebSphere Message Broker primaire et de secours. Ce répertoire doit être monté automatiquement par le système d'exploitation à des fins de partage réseau. Toutefois, dans certains cas, un montage et un démontage manuels peuvent être nécessaires.

Procédure

1. Connectez-vous au serveur de messagerie 1 ou au serveur de messagerie 2 en tant qu'utilisateur `ibmadm`. Si vous êtes connecté en tant qu'utilisateur différent, basculez vers l'utilisateur `ibmadm` en exécutant la commande `su - ibmadm`. Dans des conditions normales d'exploitation, utilisez l'outil de contrôle de plateforme sur le serveur de messagerie 1. Si le serveur de messagerie 1 n'est pas disponible, vous pouvez exécuter l'outil de contrôle de plateforme sur le serveur de messagerie 2. N'utilisez pas l'outil de contrôle de plateforme à la fois sur le serveur de messagerie 1 et sur le serveur de messagerie 2, des résultats imprévisibles risqueraient de se produire.
2. Exécutez la commande suivante avec l'option de commande d'administration système souhaitée.
`DOPControl -a action -c composant -p mot_de_passe`

où *action* est l'une des valeurs suivantes :

mount Montage du répertoire `/opt/ibm/ioc/shared/wmq`. Cette action doit être exécutée en cas d'échec du montage automatique, ou lorsqu'une action de démontage a été exécutée auparavant.

unmount
Démontage du répertoire de messages partagés. Utilisez cette option pour arrêter le partage réseau du répertoire `/opt/ibm/ioc/shared/wmq`

et le *composant* correspond à l'une des valeurs suivantes :

shmsgpri

Indique que le répertoire /opt/ibm/ioc/shared/wmq doit être monté ou démonté sur serveur de messagerie 1.

shmsgsb

Indique que le répertoire /opt/ibm/ioc/shared/wmq doit être monté ou démonté sur serveur de messagerie 2.

mot_de_passe correspond au mot de passe de topologie défini lorsqu'IBM Defense Operations Platform a été installé. Si la valeur du *mot_de_passe* contient des caractères spéciaux, elle doit être placée entre guillemets simples. Par exemple : 'pass\$phrase'

L'option nostatus peut éventuellement être ajoutée à la commande. Toute sortie renvoyée par la commande sera supprimée.

Résultats

L'action demandée est effectuée.

Tâches associées:

«Démarrage des composants dans Command Center Edition», à la page 63
l'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Command Center Edition», à la page 64
L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65
L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition»
Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Obtention de l'aide pour l'outil de contrôle de plateforme dans Command Center Edition

Des informations sont disponibles sur les options permettant l'exécution de l'outil de contrôle de plateforme dans l'environnement Command Center Edition.

Pourquoi et quand exécuter cette tâche

La commande DOPControl doit être exécutée avec l'utilisateur ibmadmin. Si vous n'êtes pas connecté en tant qu'utilisateur ibmadmin, exécutez la commande su - ibmadmin pour basculer vers l'utilisateur ibmadmin.

Procédure

Sur le serveur de messagerie 1 ou serveur de messagerie 2, exécutez l'une des commandes suivantes pour afficher les options de la commande DOPControl.

```
DOPControl -a help
```

ou

```
DOPControl -h
```

Résultats

Les options de la commande **IOControl** sont affichées.

Tâches associées:

«Démarrage des composants dans Command Center Edition», à la page 63

L'outil de contrôle de plateforme peut être utilisé pour démarrer des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Arrêt des composants dans Command Center Edition», à la page 64

L'outil de contrôle de plateforme peut être utilisé pour arrêter des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

«Gestion des composants HADR dans Command Center Edition», à la page 66

L'outil de contrôle de plateforme offre des composants d'administration système IBM Defense Operations Platform Command Center Edition. Ces composants Command Center Edition permettent à l'administrateur de gérer des conditions uniques. Ces commandes doivent être utilisées avec prudence.

«Interrogation du statut des composants dans un environnement Command Center Edition», à la page 65

L'outil de contrôle de plateforme peut être utilisé pour déterminer le statut des composants exécutés sur IBM Defense Operations Platform Command Center Edition.

Détermination du statut des services et composants IBM Defense Operations Platform

IBM Defense Operations Platform fournit plusieurs tests d'outil de vérification du système qui peuvent être utilisés pour déterminer l'état opérationnel de différents services et composants IBM Defense Operations Platform.

Les tests sont logiquement regroupés par fonction. Par exemple, la collaboration et la surveillance.

Chaque test fournit une documentation d'aide contenant des étapes de traitement des problèmes pour résoudre les problèmes liés au composant, au serveur ou au service.

Utilisation de l'outil de vérification du système

L'outil de vérification du système permet de déterminer l'état opérationnel des services comprenant le système IBM Defense Operations Platform.

Pourquoi et quand exécuter cette tâche

L'outil de vérification du système vérifie les fonctions du système.

Pour plus de détails sur les tests individuels et la résolution des incidents si le test échoue, cliquez sur **Aide** pour le test.

Propriétés fournit des informations supplémentaires sur le test pour une utilisation lors de l'appel du service de support logiciel IBM.

Procédure

1. Connectez-vous à la console d'administration IBM Defense Operations Platform.
2. Cliquez sur n'importe quel lien WebSphere Portal au début de la page.
3. Connectez-vous en tant qu'administrateur WebSphere Portal. L'administrateur est défini dans la propriété `PORTAL.ADMIN.UID` dans le fichier de propriétés de la topologie. L'administrateur par défaut est `wpsadmin`.
4. Cliquez sur **Administration** dans la bannière supérieure.
5. Cliquez sur l'onglet **Vérification du système**.

6. Sélectionnez le ou les tests à exécuter en effectuant l'une des opérations suivantes :
- Cliquez sur un test spécifique à exécuter.
 - Cliquez sur **Exécuter tous les tests** pour tester les fonctions des tests sélectionnés.

Résultats

L'icône en forme de  s'affiche lorsqu'un test aboutit. L'icône en forme de  s'affiche lorsqu'un test échoue. Si un test échoue, suivez les instructions d'identification des problèmes du test afin de résoudre les erreurs. Ces instructions sont également accessibles en cliquant sur l'icône en forme de  ou sur **Aide**.

Si un test spécifique a été exécuté, les résultats d'exécution du test s'affichent dans la partie inférieure du portlet avec le temps d'exécution de test. Si **Exécuter tous les tests** a été sélectionné, ces informations ne sont pas affichées.

Que faire ensuite

L'outil peut être réinitialisé et tous les résultats effacés en cliquant sur **Réinitialiser**.

Tâches associées:

«Accès aux consoles d'administration IBM Defense Operations Platform», à la page 57
IBM Defense Operations Platform est constitué d'un certain nombre de produits. Chacun de ces produits possède une ou plusieurs consoles d'administration. Pour faciliter la recherche des consoles d'administration installées, IBM Defense Operations Platform fournit des pages à partir desquelles il est possible d'accéder aux consoles.

Test Serveur d'applications (REST BPM_DE.AppTarget.BPMNode1.0)

Le test Serveur d'applications (REST BPM_DE.AppTarget.BPMNode1.0) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST BPM_DE.AppTarget.BPMNode1.0) utilise la ressource suivante :

- WebSphere Application Server sur serveur de processus.

Identification des problèmes

Si le test Serveur d'applications (REST BPM_DE.AppTarget.BPMNode1.0) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante avec les options de votre choix.
 - Pour vérifier le statut du serveur IBM Business Process Manager, indiquez *status* pour *action* et *bpm* pour *composant*.
 - Pour démarrer le serveur IBM Business Process Manager, indiquez *start* pour *action* et *bpm* pour *composant*.
 - Pour arrêter le serveur IBM Business Process Manager, indiquez *stop* pour *action* et *bpm* pour *composant*.

Indiquez le mot de passe de votre topologie dans *motdepasse_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
4. Vérifiez que le serveur BPM_DE.AppTarget.BPMNode1.0 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` où `WAS_ADMIN_USER` est l'ID administrateur WebSphere (normalement `admin`) et `WAS_ADMIN_PWD` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "BPM_DE.AppTarget.BPMNode1.0"`. Ce dernier est arrêté. s'affiche, lancez le serveur à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startServer.sh BPM_DE.AppTarget.BPMNode1.0`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "BPM_DE.AppTarget.BPMNode1.0" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `the_DE_AppTarget.WBMNode1.0`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur BPM_DE.AppTarget.BPMNode1.0 prêt pour e-business; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `BPM_DE.AppTarget.BPMNode1.0`

Arrêtez les serveurs dans cet ordre :

- a. `BPM_DE.AppTarget.BPMNode1.0`
- b. `nodeagent`

Le serveur `BPM_DE.AppTarget.BPMNode1.0` est arrêté en exécutant la commande suivante dans une fenêtre de commande, sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/`

bpmProfile1/bin/stopServer.sh -all -username *ADMIN_WAS* -password *WAS_ADMIN_PWD*
où *ADMIN_WAS* est l'ID administrateur WebSphere (normalement admin) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* où *ADMIN_WAS* est l'ID administrateur WebSphere (normalement admin) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur BPM_DE.AppTarget.BPMNode1.0 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *APPLICATION_SERVER_HOST* est le nom d'hôte du serveur d'applications.

- b. Affichez le statut du serveur BPM_DE.AppTarget.BPMNode1.0 en cliquant sur **Serveurs > Types de serveurs > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. BPM_DE.AppTarget.BPMNode1.0

Arrêtez les serveurs dans cet ordre :

- a. BPM_DE.AppTarget.BPMNode1.0
- b. nodeagent

Pour arrêter le serveur BPM_DE.AppTarget.BPMNode1.0, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* où *ADMIN_WAS* est l'ID administrateur WebSphere (normalement admin) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST IopServer1)

Le test Serveur d'applications (REST IopServer1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST IopServer1) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

Identification des problèmes

Si le test Serveur d'applications (REST IopServer1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *iop* et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

- a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

- b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour contrôler le statut du serveur principal, indiquez *status* pour *action* et *ioppri* pour *composant*.
- Pour contrôler le statut du serveur de secours, indiquez *status* pour *action* et *iopsby* pour *composant*.
- Pour démarrer le serveur principal, indiquez *start* pour *action* et *ioppri* pour *composant*.
- Pour démarrer le serveur de secours, indiquez *start* pour *action* et *iopsby* pour *composant*.
- Pour arrêter le serveur principal, indiquez *stop* pour *action* et *ioppri* pour *composant*.
- Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *iopsby* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

- b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

- c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :

- /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/logs/IopServer1/SystemOut.log

- /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/logs/IopServer1/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
 5. Vérifiez que le serveur IopServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'application "IopServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `IopServer1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startServer.sh IopServer1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "IopServer1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `IopServer1`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur IopServer1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `IopServer1`

Arrêtez les serveurs dans cet ordre :

- a. `IopServer1`
- b. `nodeagent`

Le serveur `IopServer1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur `IopServer1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.

- b. Affichez le statut du serveur IopServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. IopServer1

Arrêtez les serveurs dans cet ordre :

- a. IopServer1
- b. nodeagent

Pour arrêter le serveur IopServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST IopServer2)

Le test Serveur d'applications (REST IopServer2) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST IopServer2) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications 2.

Identification des problèmes

Si le test Serveur d'applications (REST IopServer2) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.

- Pour contrôler le statut du serveur principal, indiquez *status* pour *action* et *ioppri* pour *composant*.
- Pour contrôler le statut du serveur de secours, indiquez *status* pour *action* et *iopsby* pour *composant*.
- Pour démarrer le serveur principal, indiquez *start* pour *action* et *ioppri* pour *composant*.
- Pour démarrer le serveur de secours, indiquez *start* pour *action* et *iopsby* pour *composant*.
- Pour arrêter le serveur principal, indiquez *stop* pour *action* et *ioppri* pour *composant*.
- Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *iopsby* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/AppServer/profiles/IopProfile2/logs/IopServer2/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/IopProfile2/logs/IopServer2/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur IopServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN_WAS* est l'ID administrateur WebSphere (normalement *admin*) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE.` s'affiche. Si vous avez dû démarrer le *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654.`
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "IopServer2"`. Ce dernier est arrêté. s'affiche, démarrez le serveur *IopServer2* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startServer.sh IopServer2`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "IopServer2" est DEMARRE.` s'affiche. Si vous avez dû démarrer *IopServer2*, un message similaire au suivant s'affiche : `ADMU3000I : Serveur IopServer2 prêt pour e-business ; l'ID de processus est 26654.`

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. IopServer2

Arrêtez les serveurs dans cet ordre :

- a. IopServer2
- b. nodeagent

Le serveur IopServer2 est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur IopServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
- b. Affichez le statut du serveur IopServer2 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. IopServer2

Arrêtez les serveurs dans cet ordre :

- a. IopServer2
- b. nodeagent

Pour arrêter le serveur IopServer2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST isim1)

Le test Serveur d'applications (REST isim1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST isim1) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

Identification des problèmes

Si le test Serveur d'applications (REST isim1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *isim* et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour vérifier le statut d'IBM Security Identity Manager, indiquez *status* pour *action* et *isim* pour *composant*.
- Pour arrêter IBM Security Identity Manager, indiquez *stop* pour *action* et *isim* pour *composant*.
- Pour démarrer IBM Security Identity Manager, indiquez *start* pour *action* et *isim* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
- c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
- /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log
 - /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur isim1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
- a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "isim1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `isim1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "isim1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `isim1`, un message similaire au suivant s'affiche : `ADMU3000I : serveur isim1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `isim1`

Arrêtez les serveurs dans cet ordre :

- a. `isim1`
- b. `nodeagent`

Le serveur `isim1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur isim1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9061/ibm/console` en utilisant l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.

- b. Afficher le statut du serveur isim1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. isim1

Arrêtez les serveurs dans cet ordre :

- a. isim1
- b. nodeagent

Pour arrêter le serveur isim1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST odmServer1)

Le test Serveur d'applications (REST odmServer1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST odmServer1) utilise la ressource suivante :

- WebSphere Application Server sur serveur de processus.

Identification des problèmes

Si le test Serveur d'applications (REST odmServer1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour vérifier le statut d'IBM Operational Decision Manager, indiquez status pour *action* et odm pour *composant*.
 - Pour vérifier le statut d'IBM Operational Decision Manager Decision Center, indiquez status pour *action* et odmdc pour *composant*.
 - Pour démarrer IBM Operational Decision Manager, indiquez start pour *action* et odm pour *composant*.
 - Pour démarrer IBM Operational Decision Manager Decision Center, indiquez start pour *action* et odmdc pour *composant*.
 - Pour arrêter IBM Operational Decision Manager, indiquez stop pour *action* et odm pour *composant*.
 - Pour arrêter IBM Operational Decision Manager Decision Center, indiquez stop pour *action* et odmdc pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
4. Vérifiez que le serveur odmServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur de processus, connectez-vous en tant que ibmadmin.
 - b. Dans une fenêtre de commande, exécutez : /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/serverStatus.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD où WAS_ADMIN_USER est l'ID administrateur WebSphere (normalement admin) et WAS_ADMIN_PWD est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté. s'affiche, démarrez le nodeagent à l'aide de la commande suivante : /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startNode.sh. Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE. s'affiche. Si vous avez dû démarrer le serveur nodeagent, un message similaire au suivant s'affiche : ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654.
 - a. Si le message ADMU0509I : Impossible d'atteindre le serveur d'applications "odmServer1". Ce dernier est arrêté. s'affiche, démarrez le serveur à l'aide de la commande suivante :

/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startServer.sh odmServer1. Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "odmServer1" est DEMARRE. s'affiche. Si vous avez dû démarrer le serveur, un message similaire au suivant s'affiche :
ADMU3000I : Serveur odmServer1 prêt pour e-business ; l'ID de processus est 26654.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. odmServer1

Arrêtez les serveurs dans cet ordre :

- a. odmServer1
- b. nodeagent

Le serveur odmServer1 est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur odmServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
 - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://PROCESS_SERVER_HOST:9060/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *PROCESS_SERVER_HOST* est le nom d'hôte du serveur de processus.
 - b. Affichez le statut du serveur odmServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startNode.sh dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. odmServer1

Arrêtez les serveurs dans cet ordre :

- a. odmServer1
- b. nodeagent

Pour arrêter le serveur odmServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST odmdc1)

Le test Serveur d'applications (REST odmdc1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST odmdc1) utilise la ressource suivante :

- WebSphere Application Server sur serveur de processus.

Identification des problèmes

Si le test Serveur d'applications (REST odmdc1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour vérifier le statut d'IBM Operational Decision Manager, indiquez status pour *action* et odm pour *composant*.
 - Pour vérifier le statut d'IBM Operational Decision Manager Decision Center, indiquez status pour *action* et odmdc pour *composant*.
 - Pour démarrer IBM Operational Decision Manager, indiquez start pour *action* et odm pour *composant*.
 - Pour démarrer IBM Operational Decision Manager Decision Center, indiquez start pour *action* et odmdc pour *composant*.
 - Pour arrêter IBM Operational Decision Manager, indiquez stop pour *action* et odm pour *composant*.
 - Pour arrêter IBM Operational Decision Manager Decision Center, indiquez stop pour *action* et odmdc pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

- c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/logs/odmcd1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/logs/odmcd1/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
4. Vérifiez que le serveur odmcd1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté. s'affiche`, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE. s'affiche`. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "odmcd1". Ce dernier est arrêté. s'affiche`, démarrez le serveur à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/bin/startServer.sh odmcd1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "odmcd1" est DEMARRE. s'affiche`. Si vous avez dû démarrer le serveur, un message similaire au suivant s'affiche : `ADMU3000I : Serveur odmcd1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `odmcd1`

Arrêtez les serveurs dans cet ordre :

- a. `odmcd1`
- b. `nodeagent`

Le serveur `odmcd1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur `odmcd1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://PROCESS_SERVER_HOST:9060/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `PROCESS_SERVER_HOST` est le nom d'hôte du serveur de processus.
- b. Affichez le statut du serveur `odmdc1` en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `odmdc1`

Arrêtez les serveurs dans cet ordre :

- a. `odmdc1`
- b. `nodeagent`

Pour arrêter le serveur `odmdc1`, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST STProxyServer1)

Le test Serveur d'applications (REST STProxyServer1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST STProxyServer1) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

Identification des problèmes

Si le test Serveur d'applications (REST STProxyServer1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *stproxy* et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour contrôler le statut du serveur Sametime, indiquez *status* pour *action* et *stproxy* pour *composant*.
- Pour démarrer le serveur Sametime, indiquez *start* pour *action* et *stproxy* pour *composant*.
- Pour arrêter le serveur Sametime, indiquez *stop* pour *action* et *stproxy* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :

- /opt/IBM/WebSphere/AppSrv7/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log
- /opt/IBM/WebSphere/AppSrv7/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log

4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

5. Vérifiez que le serveur STProxyServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :

a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.

- b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
- c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
- a. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "STProxyServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `STProxyServer1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "STProxyServer1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `STProxyServer1`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur STProxyServer1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `STProxyServer1`

Arrêtez les serveurs dans cet ordre :

- a. `STProxyServer1`
- b. `nodeagent`

Le serveur `STProxyServer1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

- 6. Vérifiez que le serveur `STProxyServer1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
 - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
 - b. Affichez le statut du serveur `STProxyServer1` en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de ⓘ indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. STProxyServer1

Arrêtez les serveurs dans cet ordre :

- a. STProxyServer1
- b. nodeagent

Pour arrêter le serveur STProxyServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST WebSphere_Portal)

Le test Serveur d'applications (REST WebSphere_Portal) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST WebSphere_Portal) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

Identification des problèmes

Si le test Serveur d'applications (REST WebSphere_Portal) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `wpe` et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.
 - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour vérifier le statut du serveur WebSphere Portal principal, indiquez status pour *action* et wpepri pour *composant*.
 - Pour vérifier le statut du serveur WebSphere Portal de secours, indiquez status pour *action* et wpesby pour *composant*.
 - Pour démarrer le serveur WebSphere Portal principal, indiquez start pour *action* et wpepri pour *composant*.
 - Pour démarrer le serveur WebSphere Portal de secours, indiquez start pour *action* et wpesby pour *composant*.
 - Pour arrêter le serveur WebSphere Portal principal, indiquez stop pour *action* et wpepri pour *composant*.
 - Pour arrêter le serveur WebSphere Portal de secours, indiquez stop pour *action* et wpesby pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur WebSphere_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
 - b. Dans une fenêtre de commande, exécutez : /opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username *ADMIN_WAS* -password *MDP_ADMIN_WAS* où *ADMIN_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté. s'affiche, démarrez le nodeagent à l'aide de la commande suivante : /opt/IBM/WebSphere/wp_profile/bin/startNode.sh. Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE. s'affiche. Si vous avez dû démarrer le

nodeagent, un message similaire au suivant s'affiche : ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654.

- a. Si le message ADMU0509I : Impossible d'atteindre le serveur d'application "WebSphere_Portal". Ce dernier est arrêté. s'affiche, démarrez WebSphere_Portal à l'aide de la commande suivante : /opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal. Ignorez cette étape si le message ADMU0508I : le serveur d'applications "WebSphere_Portal" est DEMARRE. s'affiche. Si vous avez dû démarrer WebSphere_Portal, un message similaire au suivant s'affiche : ADMU3000I: Serveur WebSphere_Portal prêt pour e-business ; l'ID de processus est 26654.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere_Portal
- b. nodeagent

Le serveur WebSphere_Portal est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username *ADMIN_WAS* -password *MDP_ADMIN_WAS* où *ADMIN_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username *ADMIN_WAS* -password *MDP_ADMIN_WAS* où *ADMIN_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur WebSphere_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
 - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse http://APPLICATION_SERVER_HOST:9062/ibm/console avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *APPLICATION_SERVER_HOST* est le nom d'hôte du serveur d'applications.
 - b. Affichez le statut du serveur WebSphere_Portal en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/wp_profile/bin/startNode.sh dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere_Portal
- b. nodeagent

Pour arrêter le serveur WebSphere_Portal, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST WebSphere_Portal_PortalNode2)

Le test Serveur d'applications (REST WebSphere_Portal_PortalNode2) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST WebSphere_Portal_PortalNode2) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications 2.

Identification des problèmes

Si le test Serveur d'applications (REST WebSphere_Portal_PortalNode2) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
 - Pour vérifier le statut du serveur WebSphere Portal principal, indiquez `status` pour *action* et `wpepri` pour *composant*.
 - Pour vérifier le statut du serveur WebSphere Portal de secours, indiquez `status` pour *action* et `wpesby` pour *composant*.
 - Pour démarrer le serveur WebSphere Portal principal, indiquez `start` pour *action* et `wpepri` pour *composant*.
 - Pour démarrer le serveur WebSphere Portal de secours, indiquez `start` pour *action* et `wpesby` pour *composant*.
 - Pour arrêter le serveur WebSphere Portal principal, indiquez `stop` pour *action* et `wpepri` pour *composant*.
 - Pour arrêter le serveur WebSphere Portal de secours, indiquez `stop` pour *action* et `wpesby` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
- c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere_Portal_PortalNode2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
- a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WebSphere_Portal_PortalNode2"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WebSphere_Portal_PortalNode2` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Ignorez cette étape si le message `ADMU0508I : le serveur d'applications "WebSphere_Portal_PortalNode2" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WebSphere_Portal_PortalNode2`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WebSphere_Portal_PortalNode2 prêt pour e-business; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WebSphere_Portal_PortalNode2`

Arrêtez les serveurs dans cet ordre :

- a. `WebSphere_Portal_PortalNode2`
- b. `nodeagent`

Le serveur `WebSphere_Portal_PortalNode2` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere_Portal_PortalNode2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
 - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
 - b. Affichez le statut du serveur WebSphere_Portal_PortalNode2 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.
 - L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.
 - L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.
 - L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere_Portal_PortalNode2

Arrêtez les serveurs dans cet ordre :

- a. WebSphere_Portal_PortalNode2
- b. nodeagent

Pour arrêter le serveur WebSphere_Portal_PortalNode2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST WSRRServer1)

Le test Serveur d'applications (REST WSRRServer1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Ressources

Le test Serveur d'applications (REST WSRRServer1) utilise la ressource suivante :

- WebSphere Application Server sur serveur de processus.

Identification des problèmes

Si le test Serveur d'applications (REST WSRRServer1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour vérifier le statut du serveur WebSphere Service Registry and Repository, indiquez `status` pour *action* et `wrrr` pour *composant*.
 - Pour démarrer le serveur WebSphere Service Registry and Repository, indiquez `start` pour *action* et `wrrr` pour *composant*.
 - Pour arrêter le serveur WebSphere Service Registry and Repository, indiquez `stop` pour *action* et `wrrr` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
 - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
 - `/opt/IBM/WebSphere/AppServer/profiles/wrrrProfile1/logs/WSRRServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/wrrrProfile1/logs/WSRRServer1/SystemErr.log`
3. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande `df -h`. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande `df -h` renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
4. Vérifiez que le serveur WSRRServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/wrrrProfile1/bin/serverStatus.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` où `WAS_ADMIN_USER` est l'ID administrateur WebSphere (normalement `admin`) et `WAS_ADMIN_PWD` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/wrrrProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WSRRServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/wrrrProfile1/bin/startServer.sh WSRRServer1`. Ignorez cette étape si le message `ADMU0508I: The Application Server "WSRRServer1" is STARTED`. s'affiche. Si vous avez dû démarrer le serveur, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WSRRServer1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WSRRServer1

Arrêtez les serveurs dans cet ordre :

- a. WSRRServer1
- b. nodeagent

Le serveur WSRRServer1 est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WSRRServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.

- b. Affichez le statut du serveur WSRRServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WSRRServer1

Arrêtez les serveurs dans cet ordre :

- a. WSRRServer1
- b. nodeagent

Pour arrêter le serveur WSRRServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST WorklightServer1)

Le test Serveur d'applications (REST WorklightServer1) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Remarque : IBM Worklight est disponible uniquement pour installation via un mandat IBM Services.

Ressources

Le test Serveur d'applications (REST WorklightServer1) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

Identification des problèmes

Si le test Serveur d'applications (REST WorklightServer1) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter, en fonction des besoins. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `wrkl` et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

- a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

- b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour vérifier le statut d'IBM Worklight, indiquez `status` pour *action* et `wrkl` pour *composant*.
- Pour démarrer IBM Worklight, indiquez `start` pour *action* et `wrkl` pour *composant*.
- Pour arrêter IBM Worklight, indiquez `stop` pour *action* et `wrkl` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
- `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

- b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
- c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
- /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Testez que le serveur WorklightServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici la procédure manuelle à suivre :
- a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "WorklightServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WorklightServer1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "WorklightServer1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WorklightServer1`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WorklightServer1 prêt pour e-business ; l'ID de processus est 26654`.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WorklightServer1`

Arrêtez les serveurs dans cet ordre :

- a. `WorklightServer1`
- b. `nodeagent`

Le serveur `WorklightServer1` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/`

WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere.

6. Testez que le serveur WorklightServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. APPLICATION_SERVER_HOST est le nom d'hôte du serveur d'applications.
- b. Affichez le statut du serveur WorklightServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer1

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer1
- b. nodeagent

Pour arrêter le serveur WorklightServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (REST WorklightServer2)

Le test Serveur d'applications (REST WorklightServer2) vérifie l'accès au service REST de WebSphere Application Server sur le serveur cible.

Remarque : IBM Worklight est disponible uniquement pour installation via un mandat IBM Services.

Ressources

Le test Serveur d'applications (REST WorklightServer2) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications 2.

Identification des problèmes

Si le test Serveur d'applications (REST WorklightServer2) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
 - Pour vérifier le statut d'IBM Worklight, indiquez *status* pour *action* et *wrkl* pour *composant*.
 - Pour démarrer IBM Worklight, indiquez *start* pour *action* et *wrkl* pour *composant*.
 - Pour arrêter IBM Worklight, indiquez *stop* pour *action* et *wrkl* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
 - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WorklightServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
 - a. Sur le système du serveur d'applications 2, connectez-vous en tant que *ibmadmin*.
 - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP_ADMIN_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
 - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté.` s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE.` s'affiche. Si vous avez dû démarrer le serveur *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654.`
 - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WorklightServer2". Ce dernier est arrêté.` s'affiche, démarrez le serveur *WorklightServer2* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startServer.sh WorklightServer2`. Ignorez cette étape si le message `ADMU0508I : Le serveur`

d'applications "WorklightServer2" est DEMARRE. s'affiche. Si vous avez dû démarrer WorklightServer2, un message similaire au suivant s'affiche : ADMU3000I : Serveur WorklightServer2 prêt pour e-business ; l'ID de processus est 26654.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer2

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer2
- b. nodeagent

Le serveur WorklightServer2 est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS où ADMIN_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP_ADMIN_WAS est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WorklightServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
 - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. APPLICATION_SERVER_HOST est le nom d'hôte du serveur d'applications.
 - b. Affichez le statut du serveur WorklightServer2 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh dans une fenêtre de commande.

Important : Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer2

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer2
- b. nodeagent

Pour arrêter le serveur WorklightServer2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (Console d'administration de WebSphere Application Server version 7)

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 7) accède à WebSphere Application Server sur le serveur d'applications.

Ressources

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 7) utilise la ressource suivante :

- IBM Operational Decision Manager sur le serveur serveur d'applications WebSphere Application Server server1

Identification des problèmes

Si le test Serveur d'applications (Console d'administration de WebSphere Application Server version 7) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter, en fonction des besoins. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *isim* et indiquez le mot de passe de votre topologie dans *mot_de_passe_topologie*.
 - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *isim* pour *composant*.
 - Pour démarrer le serveur, indiquez *start* pour *action* et *isim* pour *composant*.
 - Pour arrêter le serveur, indiquez *stop* pour *action* et *isim* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur d'applications consultez les journaux de WebSphere Application Server suivants :
 - Journal des erreurs : /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/server1/SystemErr.log
 - Journal de sortie : /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/server1/SystemOut.log
 - Journal de début : opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/se/startServer.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que WebSphere Application Server est en cours d'exécution.
 - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant qu'utilisateur `ibmadmin`.
 - b. Exécutez la commande **./opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.shserver1**.
 - c. Si WebSphere Application Server n'est pas en cours de fonctionnement, exécutez la commande suivante en tant qu'utilisateur `ibmadmin` sur le serveur d'applications (Field Edition) ou serveur d'applications 1 (Command Center Edition).


```
/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh server1
```

 Vous pouvez également utiliser la commande `DOPControl` pour démarrer le composant `isim`.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (Console d'administration de WebSphere Application Server version 8)

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8) accède à WebSphere Application Server sur le serveur d'applications.

Ressources

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8) utilise la ressource suivante :

- IBM Operational Decision Manager sur le serveur serveur d'applications WebSphere Application Server dmgr

Identification des problèmes

Si le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter, en fonction des besoins. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *appdmgr* et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.
 - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *appdmgr* pour *composant*.
 - Pour démarrer le serveur, indiquez *start* pour *action* et *appdmgr* pour *composant*.
 - Pour arrêter le serveur, indiquez *stop* pour *action* et *appdmgr* pour *composant*.Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin

DOPControl -a action -c composant -p mot_de_passe_de_topologie
```
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
 - c. Sur le serveur d'applications consultez les journaux de WebSphere Application Server suivants :
 - Journal des erreurs : /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
 - Journal de sortie : /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
 - Journal de début : /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/startServer.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que WebSphere Application Server est en cours d'exécution.
 - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant qu'utilisateur *ibmadmin*.
 - b. Exécutez la commande **./opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.shserver1**.

- c. Si WebSphere Application Server n'est pas en cours de fonctionnement, exécutez la commande suivante en tant qu'utilisateur `ibmadmin` sur le serveur d'applications (Field Edition) ou serveur d'applications 1 (Command Center Edition).

```
/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startServer.sh dmgr
```

Vous pouvez également utiliser la commande `DOPControl` pour démarrer le composant `appdmgr`.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Serveur d'applications (Console d'administration de WebSphere Application Server version 8.5)

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8.5) accède à WebSphere Application Server sur le serveur de processus.

Ressources

Le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8.5) utilise la ressource suivante :

- IBM Operational Decision Manager sur le serveur serveur de processus WebSphere Application Server `dmgr`

Identification des problèmes

Si le test Serveur d'applications (Console d'administration de WebSphere Application Server version 8.5) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et pour les démarrer ou les arrêter, en cas de besoin. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `prodmgr` pour *composant*.
 - Pour démarrer le serveur, indiquez `start` pour *action* et `prodmgr` pour *composant*.
 - Pour arrêter le serveur, indiquez `stop` pour *action* et `prodmgr` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de processus. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de processus à partir du serveur d'applications et vice-versa. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
 - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
 - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
 - c. Sur le serveur d'applications consultez les journaux de WebSphere Application Server suivants :

- Journal des erreurs : /opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/SystemErr.log
 - Journal de sortie : /opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/SystemOut.log
 - Journal de début : opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/startServer.log
4. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
 5. Vérifiez que WebSphere Application Server est en cours d'exécution.
 - a. Connectez-vous à une session de terminal sur le serveur de processus en tant qu'utilisateur `ibmadmin`.
 - b. Exécutez la commande **./opt/IBM/WebSphere/AppServer85/profiles/dmgr/bin/serverStatus.shserver1**.
 - c. Si WebSphere Application Server n'est pas en cours d'exécution, exécutez la commande suivante en tant qu'utilisateur `ibmadmin` sur le serveur de processus.
`/opt/IBM/WebSphere/AppServer85/profiles/dmgr/bin/startServer.sh dmgr`
 Vous pouvez également utiliser la commande `DOPControl` pour démarrer le composant `prodmgr`.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Collaboration (Console Lotus Domino)

Le test Collaboration (Console Lotus Domino) détermine si l'annuaire Domino est accessible via son adresse URL.

Ressources

Le test Collaboration (Console Lotus Domino) utilise la ressource suivante :

- Le serveur Domino (sur le serveur d'applications).

Identification des problèmes

Si le test Collaboration (Console Lotus Domino) échoue, procédez comme suit pour rechercher et résoudre le problème.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `st` et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.
 - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour contrôler le statut du serveur, indiquez `status` pour *action* et `st` pour *composant*.
- Pour démarrer le serveur, indiquez `start` pour *action* et `st` pour *composant*.
- Pour arrêter le serveur, indiquez `stop` pour *action* et `st` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
- Sur serveur d'applications consultez les journaux de Lotus Domino suivants :
 - `/local/notesdata/console.out`
 - `/local/notesdata/log.nsf`
 - Tous les journaux situés dans le répertoire `/local/notesdata/IBM_TECHNICAL_SUPPORT/`.
4. Vérifiez que les systèmes de fichiers sur le système du serveur d'applications n'ont pas atteint leur capacité maximale. Pour ce faire, utilisez la commande `df -h`.
5. Vérifiez que les composants du processus Lotus Domino sont en cours d'exécution.
- Connectez-vous à la console du répertoire Lotus Domino à l'adresse `http://APP_SERVER_HOST:84/names.nsf` où `APP_SERVER_HOST` est le nom d'hôte du serveur d'applications. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de l'administrateur de Domino.
 - Si la console n'est pas accessible, sur le serveur d'applications, exécutez la commande `ps -ef | grep note` pour déterminer si les processus Lotus Domino sont en cours d'exécution. Les processus Lotus Domino sont les suivants :
 - `server`
 - `event`
 - `update`
 - `replica`
 - `router`
 - `adminp`
 - `calconn`
 - `sched`
 - `http`
 - `rnrmgr`
 - `staddin`
6. Si certains, mais pas tous les processus sont en cours d'exécution, arrêtez les processus en cours d'exécution avant de redémarrer tous les processus.
- Sur le serveur d'applications, connectez-vous en tant qu'utilisateur `notes`.
 - Accédez au répertoire `/local/notesdata`.
 - Exécutez la commande `"nohup /opt/IBM/lotus/bin/server -q console.out > 2>&1 &"` pour arrêter tous les processus Lotus Domino en cours d'exécution.
 - Vérifiez que tous les processus sont arrêtés en exécutant la commande `ps -ef | grep notes`.
 - Si des processus Lotus Domino sont toujours en cours d'exécution, arrêtez-les à l'aide de la commande `kill -9 pid`, où `pid` est l'identificateur du processus Lotus Domino.
7. Si les processus Lotus Domino ne sont pas en cours d'exécution, démarrez les composants du serveur Lotus Domino.
- Sur le serveur d'applications, connectez-vous en tant qu'utilisateur `notes`.
 - Accédez au répertoire `/local/notesdata`.

- c. Exécutez la commande "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" pour démarrer tous les composants du serveur de Lotus Domino.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Collaboration (Console Lotus Sametime)

Le test Collaboration (Console Lotus Sametime) détermine si la console Sametime est accessible via son adresse URL.

Ressources

Le test Collaboration (Console Lotus Sametime) utilise la ressource suivante :

- Serveur Sametime (sur le serveur d'applications).

Identification des problèmes

Si le test Collaboration (Console Lotus Sametime) échoue, procédez comme suit pour rechercher et résoudre le problème.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *st* et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.
 - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
 - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *st* pour *composant*.
 - Pour démarrer le serveur, indiquez *start* pour *action* et *st* pour *composant*.
 - Pour arrêter le serveur, indiquez *stop* pour *action* et *st* pour *composant*.Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

```
su - ibmadmin

DOPControl -a action -c composant -p mot_de_passe_de_topologie
```
3. Collecter et examiner la configuration du serveur de communauté et les fichiers journaux de Sametime.
 - a. Connectez-vous au serveur d'applications en tant qu'utilisateur *notes*.
 - b. Accédez au répertoire `/local/notesdata`.

- c. Exécutez la commande `sh stdiagzip.sh`. Cette commande permet de collecter tous les fichiers journaux pertinents et de les écrire dans le répertoire `/local/notesdata/`.
 - d. Consultez les journaux dans le répertoire `/local/notesdata/`.
4. Vérifiez que les systèmes de fichiers sur le système du serveur d'applications n'ont pas atteint leur capacité maximale. Pour ce faire, utilisez la commande `df -h`.
5. Vérifiez que les composants du processus Sametime sont en cours d'exécution.
 - a. Connectez-vous sur la page d'accueil Sametime à l'adresse `http://APP_SERVER_HOST:84/stcenter.nsf` où `APP_SERVER_HOST` est le nom d'hôte du serveur d'applications. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de l'administrateur de Domino.
 - b. Sur la page d'accueil de Sametime, cliquez sur **Administrer le serveur**.
 - c. Sur la page Présentation du serveur, vérifiez que tous les services de Sametime sont en cours d'exécution.
6. Si certains, mais pas tous les processus sont en cours d'exécution, arrêtez les processus en cours d'exécution avant de redémarrer tous les processus.
 - a. Sur le serveur d'applications, connectez-vous en tant qu'utilisateur notes.
 - b. Accédez au répertoire `/local/notesdata`.
 - c. Exécutez la commande `"nohup /opt/IBM/lotus/bin/server -q console.out > 2>&1 &"` pour arrêter tous les processus Sametime en cours d'exécution.
 - d. Vérifiez que tous les processus sont arrêtés en exécutant la commande `ps -ef | grep notes`.
 - e. Si des processus sont toujours en cours d'exécution, arrêtez-les à l'aide de la commande `kill -9 pid`, où `pid` est l'identificateur du processus Lotus Domino.
7. Si les processus Sametime ne sont pas en cours d'exécution, démarrez les composants du serveur Lotus Sametime.
 - a. Sur le serveur d'applications, connectez-vous en tant qu'utilisateur notes.
 - b. Accédez au répertoire `/local/notesdata`.
 - c. Exécutez la commande `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` pour démarrer tous les composants du serveur Lotus Sametime.

Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

Test Collaboration (Console de proxy Lotus Sametime)

Le test Collaboration (Console de proxy Lotus Sametime) détermine si Lotus Sametime Proxy Web Application peut être accessible via l'URL de Lotus Sametime Proxy Web Application.

Ressources

Le test Collaboration (Console de proxy Lotus Sametime) utilise la ressource suivante :

- Sametime Proxy (sur le serveur d'applications).

Identification des problèmes

Si le test Collaboration (Console de proxy Lotus Sametime) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `stproxy` et indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.

- a. Pour contrôler le statut du composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
 - b. Pour démarrer le composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
 - c. Pour arrêter le composant, exécutez les commandes suivantes :


```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
- Pour contrôler le statut du serveur, indiquez *status* pour *action* et *stproxy* pour *composant*.
 - Pour démarrer le serveur, indiquez *start* pour *action* et *stproxy* pour *composant*.
 - Pour arrêter le serveur, indiquez *stop* pour *action* et *stproxy* pour *composant*.
- Indiquez votre mot de passe de topologie pour *mot_de_passe_de_topologie*.
- ```
su - ibmadmin

DOPControl -a action -c composant -p mot_de_passe_de_topologie
```
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Sur le serveur d'applications, consultez les journaux de Sametime Proxy Server suivants :
    - /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemErr.log
4. Vérifiez que les systèmes de fichiers sur le système du serveur d'applications n'ont pas atteint leur capacité maximale. Pour ce faire, utilisez la commande **df -h**.
5. Vérifiez que le serveur Sametime Proxy est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
- a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password *WAS\_ADMIN\_PWD*, où *WAS\_ADMIN\_PWD* est le mot de passe de l'administrateur de WebSphere Application Server.
  - c. Si le message ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté. s'affiche, démarrez le serveur nodeagent à l'aide de la commande suivante : /opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh . Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE. s'affiche. Si vous avez dû démarrer le nodeagent, un message similaire au suivant s'affiche : ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654.
  - d. Si le message ADMU0509I: Impossible d'atteindre le serveur d'applications "STProxyServer1". Ce dernier est arrêté. s'affiche, démarrez STProxyServer1 à l'aide de la commande suivante : /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/startServer.sh STProxyServer1. Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "STProxyServer1" est DEMARRE. s'affiche. Si vous avez dû démarrer STProxyServer1, un message similaire au suivant s'affiche : ADMU3000I: Serveur STProxyServer1 prêt pour e-business ; l'ID de processus est 26654.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. STProxyServer1

Arrêtez les serveurs dans cet ordre :

- a. STProxyServer1
- b. nodeagent

Pour arrêter le serveur STProxyServer1, exécutez la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh waswebadmin -username STProxyServer1-password WAS_ADMIN_PWD`, où `WAS_ADMIN_PWD` est le mot de passe de l'administrateur de WebSphere.

Pour arrêter le serveur nodeagent, exécutez la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, où `WAS_ADMIN_PWD` est le mot de passe de l'administrateur de WebSphere.

6. Vérifiez que le serveur Sametime Proxy est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur STProxyServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. STProxyServer1

Arrêtez les serveurs dans cet ordre :

- a. STProxyServer1
- b. nodeagent

Pour arrêter le serveur STProxyServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Pour arrêter le serveur nodeagent, exécutez la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, où `WAS_ADMIN_PWD` est le mot de passe de l'administrateur de WebSphere.

7. Vérifiez que Sametime Proxy Console est accessible à partir du système WebSphere Portal, sur le serveur d'applications, à l'aide de l'URL suivante : `http://APPLICATION_SERVER_HOST:9083/stwebclient/popup.jsp`. Où `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Applications)

Le test Base de données (DB2 Instance - Applications) vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le the serveur de données.

## Ressources

Le test Base de données (DB2 Instance - Applications) utilise la ressource suivante :

- L'instance de DB2 Applications (sur le système du serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Applications) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez `db2app` et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance d'Applications :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance d'Applications, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.

6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst2** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire /datahome/db2inst2/sqllib/db2dump. Consultez le fichier db2diag.log du /datahome/db2inst2/sqllib/db2dump pour voir les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Applications) [1]

Le test Base de données (DB2 Instance - Applications) [1] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 1.

## Ressources

Le test Base de données (DB2 Instance - Applications) [1] utilise la ressource suivante :

- L'instance de DB2 Applications (sur le système du serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Applications) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez *status* pour *action* et *db24apppri* pour *composant*.
  - Pour contrôler le statut du serveur de secours, indiquez *status* pour *action* et *db24appsby* pour *composant*.
  - Pour démarrer le serveur principal, indiquez *start* pour *action* et *db24apppri* pour *composant*.
  - Pour démarrer le serveur de secours, indiquez *start* pour *action* et *db24appsby* pour *composant*.
  - Pour arrêter le serveur principal, indiquez *stop* pour *action* et *db24apppri* pour *composant*.
  - Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *db24appsby* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du

serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance d'Applications :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance d'Applications, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst2** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst2/sqllib/db2dump`. Consultez le fichier `db2diag.log` du `/datahome/db2inst2/sqllib/db2dump` pour voir les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Applications) [2]

Le test Base de données (DB2 Instance - Applications) [2] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 2.

## Ressources

Le test Base de données (DB2 Instance - Applications) [2] utilise la ressource suivante :

- L'instance de DB2 Applications (sur le système du serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Applications) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.

- Pour vérifier le statut du serveur principal, indiquez `status` pour *action* et `db24apppri` pour *composant*.
- Pour contrôler le statut du serveur de secours, indiquez `status` pour *action* et `db24appsby` pour *composant*.
- Pour démarrer le serveur principal, indiquez `start` pour *action* et `db24apppri` pour *composant*.
- Pour démarrer le serveur de secours, indiquez `start` pour *action* et `db24appsby` pour *composant*.
- Pour arrêter le serveur principal, indiquez `stop` pour *action* et `db24apppri` pour *composant*.
- Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `db24appsby` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

- Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
- Recherchez les exceptions d'exécution dans les fichiers journaux.
  - Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
- Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
- Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance d'Applications :
 

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance d'Applications, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
- Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst2** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
- Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst2/sqllib/db2dump`. Consultez le fichier `db2diag.log` du `/datahome/db2inst2/sqllib/db2dump` pour voir les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Directory Server)

Le test Base de données (DB2 Instance - Directory Server) vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données.

### Ressources

Le test Base de données (DB2 Instance - Directory Server) utilise la ressource suivante :

- L'instance de DB2 Directory Server (sur le serveur de données)

### Identification des problèmes

Si le test Base de données (DB2 Instance - Directory Server) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez *db* et indiquez le mot de passe de votre topologie dans *motdepasse\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Directory Server :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Directory Server, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.

6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - dsrdbm01** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux sont stockés sur le serveur de données dans le répertoire `/datahome/dsrdbm01/sql1lib/db2dump`.
8. Consultez le `db2diag.log` pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Directory Server) [1]

Le test Base de données (DB2 Instance - Directory Server) [1] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 1.

## Ressources

Le test Base de données (DB2 Instance - Directory Server) [1] utilise la ressource suivante :

- L'instance de DB2 Directory Server (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Directory Server) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez `status` pour *action* et `tdspri` pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez `status` pour *action* et `tdssby` pour *composant*.
  - Pour démarrer le serveur principal, indiquez `start` pour *action* et `tdspri` pour *composant*.
  - Pour démarrer le serveur de secours, indiquez `start` pour *action* et `tdssby` pour *composant*.
  - Pour arrêter le serveur principal, indiquez `stop` pour *action* et `tdspri` pour *composant*.
  - Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `tdssby` pour *composant*.

Indiquez le mot de passe de votre topologie dans `motdepasse_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
  5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
    - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Directory Server :
 

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Directory Server, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
  6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - dsrdbm01** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
  7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux sont stockés sur le serveur de données dans le répertoire /datahome/dsrdbm01/sql/lib/db2dump.
  8. Consultez le db2diag.log pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Directory Server) [2]

Le test Base de données (DB2 Instance - Directory Server) [2] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 2.

## Ressources

Le test Base de données (DB2 Instance - Directory Server) [2] utilise la ressource suivante :

- L'instance de DB2 Directory Server (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Directory Server) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez dbpri pour *action* et tdsprî pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez dbsby pour *action* et tdsprî pour *composant*.
  - Pour démarrer le serveur principal, indiquez dbpri pour *action* et tdsprî pour *composant*.
  - Pour démarrer le serveur de secours, indiquez dbsby pour *action* et tdsprî pour *composant*.
  - Pour arrêter le serveur principal, indiquez dbpri pour *action* et tdsprî pour *composant*.
  - Pour arrêter le serveur de secours, indiquez dbsby pour *action* et tdsprî pour *composant*.

Indiquez le mot de passe de votre topologie dans *motdepasse\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Directory Server :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Directory Server, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - dsrdbm01** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux sont stockés sur le serveur de données dans le répertoire `/datahome/dsrdbm01/sql1lib/db2dump`.
8. Consultez le `db2diag.log` pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Logiciel intermédiaire)

Le test Base de données (DB2 Instance - Logiciel intermédiaire) vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données.

## Ressources

Le test Base de données (DB2 Instance - Logiciel intermédiaire) utilise la ressource suivante :

- L'instance de DB2 Middleware (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Logiciel intermédiaire) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez `db24mid` et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Middleware :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Middleware, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst1** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst1/sqllib/db2dump`.
8. Consultez le `db2diag.log` pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Logiciel intermédiaire) [1]

Le test Base de données (DB2 Instance - Logiciel intermédiaire) [1] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 1.

## Ressources

Le test Base de données (DB2 Instance - Logiciel intermédiaire) [1] utilise la ressource suivante :

- L'instance de DB2 Middleware (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Logiciel intermédiaire) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez *status* pour *action* et *db24midpri* pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez *status* pour *action* et *db24midsby* pour *composant*.
  - Pour démarrer le serveur principal, indiquez *start* pour *action* et *db24midpri* pour *composant*.
  - Pour démarrer le serveur de secours, indiquez *start* pour *action* et *db24midsby* pour *composant*.
  - Pour arrêter le serveur principal, indiquez *stop* pour *action* et *db24midpri* pour *composant*.
  - Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *db24midsby* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier */etc/hosts*.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log*
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log*
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log*
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log*
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé

même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Middleware :

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Middleware, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.

6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst1** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst1/sqllib/db2dump`.
8. Consultez le `db2diag.log` pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (DB2 Instance - Logiciel intermédiaire) [2]

Le test Base de données (DB2 Instance - Logiciel intermédiaire) [2] vérifie le statut du gestionnaire DB2 de l'instance DB2 sur le serveur de données 2.

## Ressources

Le test Base de données (DB2 Instance - Logiciel intermédiaire) [2] utilise la ressource suivante :

- L'instance de DB2 Middleware (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (DB2 Instance - Logiciel intermédiaire) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez `status` pour *action* et `db24midpri` pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez `status` pour *action* et `db24midsby` pour *composant*.
  - Pour démarrer le serveur principal, indiquez `start` pour *action* et `db24midpri` pour *composant*.
  - Pour démarrer le serveur de secours, indiquez `start` pour *action* et `db24midsby` pour *composant*.
  - Pour arrêter le serveur principal, indiquez `stop` pour *action* et `db24midpri` pour *composant*.
  - Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `db24midsby` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance de Middleware :
 

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de bases de données est démarré pour l'instance de Middleware, le message suivant s'affiche : Statut du gestionnaire de la base de données = Actif.
6. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst1** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.
7. Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst1/sqllib/db2dump`.
8. Consultez le `db2diag.log` pour les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Base de données (System Verification Check Scheduler)

Le test Base de données (System Verification Check Scheduler) vérifie le statut du gestionnaire DB2 de l'instance DB2 de *nom de la base de données* sur le serveur de données.

## Ressources

Le test Base de données (System Verification Check Scheduler) utilise la ressource suivante :

- L'instance DB2 d'Application (sur le serveur de données)

## Identification des problèmes

Si le test Base de données (System Verification Check Scheduler) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *db24mid* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *db24apppri* pour *composant*.
  - Pour démarrer le serveur, indiquez *start* pour *action* et *db24apppri* pour *composant*.
  - Pour arrêter le serveur, indiquez *stop* pour *action* et *db24apppri* pour *composant*.Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin

DOPControl -a action -c composant -p mot_de_passe_de_topologie
```
3. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications sur lequel le test a été initié et le serveur de données sur lequel réside la base de données. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de données à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier */etc/hosts*.
4. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log*
    - */opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log*
5. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
6. Vérifiez que le gestionnaire de bases de données utilisé par le serveur de données soit lancé.
  - a. Sur le serveur de données, exécutez la commande suivante à partir d'une fenêtre de commande en tant qu'utilisateur de l'instance d'application DB2 (*db2inst2*).

```
db2 get snapshot for dbm | grep "Database manager status"
```

Si le gestionnaire de base de données est démarré pour l'instance *nom de base de données*, le message suivant s'affiche : Statut du gestionnaire de bases de données = Actif.
7. Si les processus DB2 ne sont pas en cours d'exécution, démarrez-les en exécutant **su - db2inst2** à partir de la fenêtre de commande si vous agissez en tant que superutilisateur. Sinon, exécutez **db2start** pour lancer le gestionnaire de base de données.

- Consultez les journaux DB2 pour les erreurs liées à l'instance de base de données utilisée pour ce test. Les journaux se trouvent sur le serveur de données dans le répertoire `/datahome/db2inst2/sqllib/db2dump`. Consultez le fichier `db2diag.log` du `/datahome/db2inst2/sqllib/db2dump` pour voir les erreurs survenues lors du démarrage de la base de données utilisée pour ce test.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Decision Management (Console Decision Center de WebSphere Operational Decision Management)

Le test Decision Management (Console Decision Center de WebSphere Operational Decision Management) détermine le statut du serveur WebSphere Operational Decision Management Decision Center.

## Ressources

Le test Decision Management (Console Decision Center de WebSphere Operational Decision Management) utilise les ressources suivantes :

- WebSphere Operational Decision Management sur le serveur de processus.
- Serveur `odmdc1` WebSphere Application Server

## Identification des problèmes

Si le test Decision Management (Console Decision Center de WebSphere Operational Decision Management) échoue, procédez comme suit pour rechercher et résoudre le problème.

## Procédure

- Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur WebSphere Operational Decision Management, indiquez `status` pour *action* et `odm` pour *composant*.
  - Pour démarrer le serveur WebSphere Operational Decision Management, indiquez `start` pour *action* et `odm` pour *composant*.
  - Pour arrêter le serveur WebSphere Operational Decision Management, indiquez `stop` pour *action* et `odm` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

- Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de processus. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de processus à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
- Recherchez les exceptions d'exécution dans les fichiers journaux.
  - Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
- c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
    - Journal des erreurs : /opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemErr.log
    - Journal de sortie : /opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemOut.log
    - Journal de début : /opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/startServer.log
  4. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
  5. Vérifiez que le serveur odmdc1 WebSphere Application Server est en cours d'exécution.
    - a. Connectez-vous à une session de terminal sur le serveur de processus en tant qu'utilisateur `ibmadmin`.
    - b. Exécutez la commande `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/serverStatus.sh odmdc1`.

## Test Decision Management (console Rule Execution Server de WebSphere Operational Decision Management)

Le test Decision Management (console Rule Execution Server de WebSphere Operational Decision Management) détermine le statut du serveur WebSphere Operational Decision Management Rule Execution.

### Ressources

Le test Decision Management (console Rule Execution Server de WebSphere Operational Decision Management) utilise les ressources suivantes :

- WebSphere Operational Decision Management sur le serveur de processus.
- Serveur odmServer1 WebSphere Application Server

### Identification des problèmes

Si le test Decision Management (console Rule Execution Server de WebSphere Operational Decision Management) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur WebSphere Operational Decision Management, indiquez `status` pour *action* et `odm` pour *composant*.
  - Pour démarrer le serveur WebSphere Operational Decision Management, indiquez `start` pour *action* et `odm` pour *composant*.
  - Pour arrêter le serveur WebSphere Operational Decision Management, indiquez `stop` pour *action* et `odm` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de processus. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte

qualifié complet et le nom d'hôte abrégé du serveur de processus à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
  - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
    - Journal des erreurs : `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemErr.log`
    - Journal de sortie : `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemOut.log`
    - Journal de début : `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/startServer.log`
4. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
5. Vérifiez que le serveur `odmServer1` WebSphere Application Server est en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur de processus en tant qu'utilisateur `ibmadmin`.
  - b. Exécutez la commande `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/serverStatus.sh odmServer1`.

## Test Répertoire (Tivoli Directory Server)

Le test Répertoire (Tivoli Directory Server) détermine si Tivoli Directory Server est disponible par l'envoi d'une requête HTTP au serveur.

### Ressources

Le test Répertoire (Tivoli Directory Server) utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de données)

## Identification des problèmes

Si le test Répertoire (Tivoli Directory Server) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez `tds` et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

- b. Pour démarrer le composant, exécutez les commandes suivantes :
 

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
- c. Pour arrêter le composant, exécutez les commandes suivantes :
 

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  3. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
  4. Vérifiez que le serveur LDAP de Tivoli Directory Server est en cours d'exécution.
    - a. Connectez-vous à une session de terminal sur le serveur de données 1 serveur de données en tant qu'utilisateur root.
    - b. Exécutez la commande **ps -ef | grep ibmslapd**. Les résultats seront semblables à ce qui suit :
 

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmslapd**, est en cours d'exécution.
    - c. Exécutez la commande **ps -ef | grep ibmdiradm**. Les résultats seront semblables à ce qui suit :
 

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmdiradm**, est en cours d'exécution.
  5. Si Tivoli Directory Server, **ibmslapd**, n'est pas en cours d'exécution, procédez comme suit.
    - a. En tant qu'utilisateur *superutilisateur* Linux, exécutez **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** pour démarrer Directory Server
  6. Si Tivoli Directory Administration Serveur, **ibmdiradm**, n'est pas en cours d'exécution, procédez comme suit :
    - a. Dans une session de terminal sur le serveur de données, exécutez **su-dsrdbm01**.
    - b. Exécutez **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** pour démarrer le serveur d'applications.
  7. Si Tivoli Directory Server, **ibmslapd**, est en cours d'exécution, procédez comme suit :

**Remarque :** Effectuez cette étape même si Tivoli Directory Server a été lancé à l'étape précédente.

- a. Connectez-vous à une session de terminal sur le serveur de données en tant que **dsrdbm01**.
- b. Exécutez **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\*** où **ADMIN\_PASSWORD** est le mot de passe du compte administrateur du superutilisateur LDAP. Les objets utilisateur LDAP existants s'afficheront.
8. Vérifiez que Tivoli Directory Server Web Administration Tool est en cours d'exécution. Tivoli Directory Server Web Administration Tool est utilisé pour arrêter et démarrer l'instance LDAP, pour ajouter des utilisateurs ou des comptes et pour visualiser des fichiers journaux.
  - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant que **ibmadmin**.
  - b. Exécutez la commande **/opt/IBM/WebSphere/AppServer/v7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PASSWORD** sur le serveur d'applications,

où `WAS_ADMIN_PASSWORD` est le mot de passe de l'administrateur de WebSphere Application Server. Si l'outil est en cours d'exécution, un message similaire au suivant sera renvoyé.

```
ADMU0508I: Le serveur d'applications "tdsServer" est DEMARRE
```

Si le message suivant est renvoyé, le `tdsServer` doit être démarré.

```
ADMU0509I: Impossible d'atteindre le serveur d'applications "tdsServer". Ce dernier est arrêté.
```

- c. Pour démarrer `tdsServer`, exécutez la commande `/opt/IBM/WebSphere/AppSrv7/profiles/ism1/bin/startServer.sh tdsServer`. Le serveur `tdsServer` démarrera et un message similaire au suivant s'affichera.

```
ADMU3000I: Serveur tdsServer prêt pour e-business ; l'ID de processus est 26654
```

9. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante : `http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
10. Connectez-vous avec le compte administrateur du superutilisateur LDAP, `cn=root`, et le mot de passe approprié. Le nom du serveur LDAP doit être `DATABASE_DIRECTORY_SERVER_HOST:389`, où `DATABASE_DIRECTORY_SERVER_HOST` est le nom d'hôte du serveur de données.
11. Cliquez sur **Administration du serveur > Démarrer/arrêter/réinitialiser le serveur**. Le statut du serveur LDAP s'affichera. Cette page peut également être utilisée pour démarrer, arrêter ou réinitialiser le serveur LDAP.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Répertoire (Tivoli Directory Server) [1]

Le test Répertoire (Tivoli Directory Server) [1] détermine si Tivoli Directory Server est disponible par l'envoi d'une requête HTTP au serveur.

## Ressources

Le test Répertoire (Tivoli Directory Server) [1] utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de données)

## Identification des problèmes

Si le test Répertoire (Tivoli Directory Server) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez `status` pour *action* et `tdspri` pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez `status` pour *action* et `tdssby` pour *composant*.
  - Pour démarrer le serveur principal, indiquez `start` pour *action* et `tdspri` pour *composant*.
  - Pour démarrer le serveur de secours, indiquez `start` pour *action* et `tdssby` pour *composant*.
  - Pour arrêter le serveur principal, indiquez `stop` pour *action* et `tdspri` pour *composant*.
  - Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `tdssby` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.

- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
- b. Sur le serveur de données consultez le journal de Tivoli Directory Server suivant :  
/datahome/dsrdbm01/idsslapd-dsrdbm01/logs/audit.log
3. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur LDAP de Tivoli Directory Server est en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur de données 1 serveur de données en tant qu'utilisateur root.
  - b. Exécutez la commande **ps -ef | grep ibmslapd**. Les résultats seront semblables à ce qui suit :
 

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmslapd**, est en cours d'exécution.
  - c. Exécutez la commande **ps -ef | grep ibmdiradm**. Les résultats seront semblables à ce qui suit :
 

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmdiradm**, est en cours d'exécution.
5. Si Tivoli Directory Server, **ibmslapd**, n'est pas en cours d'exécution, procédez comme suit.
  - a. En tant qu'utilisateur *superutilisateur* Linux, exécutez **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** pour démarrer Directory Server
6. Si Tivoli Directory Administration Serveur, **ibmdiradm**, n'est pas en cours d'exécution, procédez comme suit :
  - a. Dans une session de terminal sur le serveur de données, exécutez **su-dsrdbm01**.
  - b. Exécutez **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** pour démarrer le serveur d'applications.
7. Si Tivoli Directory Server, **ibmslapd**, est en cours d'exécution, procédez comme suit :

**Remarque :** Effectuez cette étape même si Tivoli Directory Server a été lancé à l'étape précédente.

- a. Connectez-vous à une session de terminal sur le serveur de données en tant que dsrdbm01.
- b. Exécutez **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\*** où **ADMIN\_PASSWORD** est le mot de passe du compte administrateur du superutilisateur LDAP. Les objets utilisateur LDAP existants s'afficheront.
8. Vérifiez que Tivoli Directory Server Web Administration Tool est en cours d'exécution. Tivoli Directory Server Web Administration Tool est utilisé pour arrêter et démarrer l'instance LDAP, pour ajouter des utilisateurs ou des comptes et pour visualiser des fichiers journaux.
  - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant que **ibmadmin**.
  - b. Exécutez la commande **/opt/IBM/WebSphere/AppServer/v7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PASSWORD** sur le serveur d'applications, où **WAS\_ADMIN\_PASSWORD** est le mot de passe de l'administrateur de WebSphere Application Server. Si l'outil est en cours d'exécution, un message similaire au suivant sera renvoyé.
 

```
ADMU0508I: Le serveur d'applications "tdsServer" est DEMARRE
```

 Si le message suivant est renvoyé, le **tdsServer** doit être démarré.
 

```
ADMU0509I: Impossible d'atteindre le serveur d'applications "tdsServer". Ce dernier est arrêté.
```
  - c. Pour démarrer **tdsServer**, exécutez la commande **/opt/IBM/WebSphere/AppServer/v7/profiles/isim1/bin/startServer.sh tdsServer** . Le serveur **tdsServer** démarrera et un message similaire au suivant s'affichera.

ADMU3000I: Serveur tdsServer prêt pour e-business ; l'ID de processus est 26654

9. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante :  
`http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
10. Connectez-vous avec le compte administrateur du superutilisateur LDAP, `cn=root`, et le mot de passe approprié. Le nom du serveur LDAP doit être `DATABASE_DIRECTORY_SERVER_HOST:389`, où `DATABASE_DIRECTORY_SERVER_HOST` est le nom d'hôte du serveur de données.
11. Cliquez sur **Administration du serveur > Démarrer/arrêter/réinitialiser le serveur**. Le statut du serveur LDAP s'affichera. Cette page peut également être utilisée pour démarrer, arrêter ou réinitialiser le serveur LDAP.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Répertoire (Tivoli Directory Server) [2]

Le test Répertoire (Tivoli Directory Server) [2] détermine si Tivoli Directory Server est disponible par l'envoi d'une requête HTTP au serveur.

## Ressources

Le test Répertoire (Tivoli Directory Server) [2] utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de données de sauvegarde)

## Identification des problèmes

Si le test Répertoire (Tivoli Directory Server) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez `status` pour *action* et `tdspri` pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez `status` pour *action* et `tdssby` pour *composant*.
  - Pour démarrer le serveur principal, indiquez `start` pour *action* et `tdspri` pour *composant*.
  - Pour démarrer le serveur de secours, indiquez `start` pour *action* et `tdssby` pour *composant*.
  - Pour arrêter le serveur principal, indiquez `stop` pour *action* et `tdspri` pour *composant*.
  - Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `tdssby` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

- c. Sur le serveur de données consultez le journal de Tivoli Directory Server suivant :  
/datahome/dsrdbm01/idsldap-dsrdbm01/logs/audit.log
3. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
  4. Vérifiez que le serveur LDAP de Tivoli Directory Server est en cours d'exécution.
    - a. Ouvrez une session de terminal sur serveur de données 2, en tant qu'utilisateur racine.
    - b. Exécutez la commande **ps -ef | grep ibmslapd**. Les résultats seront semblables à ce qui suit :
 

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmslapd**, est en cours d'exécution.
    - c. Exécutez la commande **ps -ef | grep ibmdiradm**. Les résultats seront semblables à ce qui suit :
 

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

 Cet exemple montre que le démon de Tivoli Directory Server, **ibmdiradm**, est en cours d'exécution.
  5. Si Tivoli Directory Server, **ibmslapd**, n'est pas en cours d'exécution, procédez comme suit.
    - a. En tant qu'utilisateur *superutilisateur* Linux, exécutez **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** pour démarrer Directory Server
  6. Si Tivoli Directory Administration Serveur, **ibmdiradm**, n'est pas en cours d'exécution, procédez comme suit :
    - a. Dans une session de terminal sur le serveur de données 2, exécutez **su-dsrdbm01**.
    - b. Exécutez **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** pour démarrer le serveur d'applications.
  7. Si Tivoli Directory Server, **ibmslapd**, est en cours d'exécution, procédez comme suit :

**Remarque :** Effectuez cette étape même si Tivoli Directory Server a été lancé à l'étape précédente.

- a. Connectez-vous à une session de terminal sur le serveur de données en tant que **dsrdbm01**.
  - b. Exécutez **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\*** où **ADMIN\_PASSWORD** est le mot de passe du compte administrateur du superutilisateur LDAP. Les objets utilisateur LDAP existants s'afficheront.
8. Vérifiez que Tivoli Directory Server Web Administration Tool est en cours d'exécution. Tivoli Directory Server Web Administration Tool est utilisé pour arrêter et démarrer l'instance LDAP, pour ajouter des utilisateurs ou des comptes et pour visualiser des fichiers journaux.
    - a. Connectez-vous à une session de terminal sur le serveur d'applications 2 en tant qu'utilisateur **ibmadmin**.
    - b. Exécutez la commande **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PASSWORD** sur le serveur d'applications 2, où **WAS\_ADMIN\_PASSWORD** est le mot de passe de l'administrateur de WebSphere Application Server. Si l'outil est en cours d'exécution, un message similaire au suivant sera renvoyé.
 

```
ADMU0508I: Le serveur d'applications "tdsServer" est DEMARRE
```

 Si le message suivant est renvoyé, le **tdsServer** doit être démarré.
 

```
ADMU0509I: Impossible d'atteindre le serveur d'applications "tdsServer". Ce dernier est arrêté.
```
    - c. Pour démarrer **tdsServer**, exécutez la commande **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer** . Le serveur **tdsServer** démarrera et un message similaire au suivant s'affichera.
 

```
ADMU3000I: Serveur tdsServer prêt pour e-business ; l'ID de processus est 26654
```

9. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante :  
`http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
10. Connectez-vous avec le compte administrateur du superutilisateur LDAP, `cn=root`, et le mot de passe approprié. Le nom du serveur LDAP doit être `HOTE_SERVEUR_ANNUAIRE_BD:389`, où `HOTE_SERVEUR_ANNUAIRE_BD` est le nom d'hôte du serveur de données de sauvegarde.
11. Cliquez sur **Administration du serveur > Démarrer/arrêter/réinitialiser le serveur**. Le statut du serveur LDAP s'affichera. Cette page peut également être utilisée pour démarrer, arrêter ou réinitialiser le serveur LDAP.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Répertoire (Console Tivoli Directory Server)

Le test Répertoire (Console Tivoli Directory Server) détermine si Tivoli Directory Server est disponible par l'envoi d'une requête HTTP au serveur.

## Ressources

Le test Répertoire (Console Tivoli Directory Server) utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de données)

## Identification des problèmes

Si le test Répertoire (Console Tivoli Directory Server) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *tds* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Si vous travaillez dans un environnement à haute disponibilité, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *tds* pour *composant*.
  - Pour démarrer le serveur, indiquez *start* pour *action* et *tds* pour *composant*.
  - Pour arrêter le serveur, indiquez *stop* pour *action* et *tds* pour *composant*.Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur LDAP de Tivoli Directory Server est en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur de données 1 serveur de données en tant qu'utilisateur root.
  - b. Exécutez la commande **ps -ef | grep ibmslapd**. Les résultats seront semblables à ce qui suit :

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

Cet exemple montre que le démon de Tivoli Directory Server, **ibmslapd**, est en cours d'exécution.
  - c. Exécutez la commande **ps -ef | grep ibmdiradm**. Les résultats seront semblables à ce qui suit :

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Cet exemple montre que le démon de Tivoli Directory Server, **ibmdiradm**, est en cours d'exécution.
6. Si Tivoli Directory Server, **ibmslapd**, n'est pas en cours d'exécution, procédez comme suit.
  - a. En tant qu'utilisateur *superutilisateur* Linux, exécutez **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** pour démarrer Directory Server
7. Si Tivoli Directory Administration Serveur, **ibmdiradm**, n'est pas en cours d'exécution, procédez comme suit :
  - a. Dans une session de terminal sur le serveur de données, exécutez **su-dsrdbm01**.
  - b. Exécutez **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** pour démarrer le serveur d'applications.
8. Si Tivoli Directory Server, **ibmslapd**, est en cours d'exécution, procédez comme suit :

**Remarque :** Effectuez cette étape même si Tivoli Directory Server a été lancé à l'étape précédente.

- a. Connectez-vous à une session de terminal sur le serveur de données en tant que **dsrdbm01**.
  - b. Exécutez **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\*** où **ADMIN\_PASSWORD** est le mot de passe du compte administrateur du superutilisateur LDAP. Les objets utilisateur LDAP existants s'afficheront.
9. Vérifiez que Tivoli Directory Server Web Administration Tool est en cours d'exécution. Tivoli Directory Server Web Administration Tool est utilisé pour arrêter et démarrer l'instance LDAP, pour ajouter des utilisateurs ou des comptes et pour visualiser des fichiers journaux.
    - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant que **ibmadmin**.
    - b. Exécutez la commande **/opt/IBM/WebSphere/AppServer/v7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PASSWORD** sur le serveur d'applications, où **WAS\_ADMIN\_PASSWORD** est le mot de passe de l'administrateur de WebSphere Application Server. Si l'outil est en cours d'exécution, un message similaire au suivant sera renvoyé.

```
ADMU0508I: Le serveur d'applications "tdsServer" est DEMARRE
```

Si le message suivant est renvoyé, le **tdsServer** doit être démarré.

```
ADMU0509I: Impossible d'atteindre le serveur d'applications "tdsServer". Ce dernier est arrêté.
```

- c. Pour démarrer tdsServer, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer` . Le serveur tdsServer démarrera et un message similaire au suivant s'affichera.

ADMU3000I: Serveur tdsServer prêt pour e-business ; l'ID de processus est 26654

10. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante : `http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications.
11. Connectez-vous avec le compte administrateur du superutilisateur LDAP, `cn=root`, et le mot de passe approprié. Le nom du serveur LDAP doit être `DATABASE_DIRECTORY_SERVER_HOST:389`, où `DATABASE_DIRECTORY_SERVER_HOST` est le nom d'hôte du serveur de données.
12. Cliquez sur **Administration du serveur > Démarrer/arrêter/réinitialiser le serveur**. Le statut du serveur LDAP s'affichera. Cette page peut également être utilisée pour démarrer, arrêter ou réinitialiser le serveur LDAP.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Répertoire (Tivoli Directory Server Proxy)

Le test Répertoire (Tivoli Directory Server Proxy) détermine si Tivoli Directory Server est disponible par l'envoi d'une requête HTTP au serveur.

## Ressources

Le test Répertoire (Tivoli Directory Server Proxy) utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de messagerie)

## Identification des problèmes

Si le test Répertoire (Tivoli Directory Server Proxy) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `tdsproxy4app` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `tdsproxy4app` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `tdsproxy4app` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Vérifiez que le système de fichiers sur le serveur de messagerie n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande `df -h`. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande `df -h` renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

4. Vérifiez que le système de fichiers sur le serveur de données n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur proxy Tivoli Directory Server est en cours d'exécution à l'aide de l'outil de contrôle de plateforme (DOPControl) ou en exécutant les tâches suivantes. Seul serveur d'applications 1 a un serveur proxy Tivoli Directory Server en cours d'exécution.

- a. Sur serveur d'applications 1, démarrez une session de terminal et connectez-vous en tant qu'utilisateur racine.
- b. Exécutez la commande **ps -ef | grep tdsproxy**. Si le serveur proxy Tivoli Directory Server est en cours d'exécution, un message similaire au suivant sera renvoyé.

```
tdsproxy 10046 1 0 Oct24 ? 00:00:18 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy
tdsproxy 13920 1 0 22:55 ? 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I tdsproxy -f /datahome/proxy/idsslapd-tdsproxy/etc/ibmslapd.conf
```

- c. Exécutez la commande suivante pour déterminer si Tivoli Directory Server est en cours d'exécution.

```
/opt/ibm/ldap/V6.3/bin/64/ibmdirctl -D cn=root -w mot de passe status
```

où *mot de passe* est le mot de passe défini dans la propriété LDAP.ADMIN.DN du fichier de propriétés de topologie.

6. Si le serveur proxy Tivoli Directory Server ne s'exécute pas sur serveur d'applications 1, démarrez le serveur proxy Tivoli Directory Server à l'aide de l'outil de contrôle de plateforme (DOPControl) ou en exécutant les tâches suivantes.

- a. Sur serveur d'applications 1, démarrez une session de terminal et connectez-vous en tant qu'utilisateur tdsproxy. Si vous êtes connecté en tant qu'utilisateur root, basculez vers l'utilisateur tdsproxy en exécutant la commande **su - tdsproxy**.
- b. Exécutez la commande **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy**. Des messages semblables à ceux qui suivent devraient être renvoyés.

Serveur en cours de démarrage

```
...
Port non SSL initialisé sur 3358.
GLPADM056I Serveur d'administration en cours de démarrage.
GLPCOM003I Port non SSL initialisé sur 3358.
```

- c. Sur serveur d'applications 1, démarrez une session de terminal et connectez-vous en tant qu'utilisateur racine.
- d. Exécutez la commande **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I tdsproxy**. Des messages semblables à ceux qui suivent devraient être renvoyés.

Serveur en cours de démarrage

```
...
Port non SSL initialisé sur 389.
GLPSRV041I Serveur en cours de démarrage.
GLPCOM003I Port non SSL initialisé sur 389.
```

7. Vérifiez que le serveur LDAP de Tivoli Directory Server est en cours d'exécution.

- a. Connectez-vous à une session de terminal sur le serveur de données 1 serveur de données en tant qu'utilisateur root.
- b. Exécutez la commande **ps -ef | grep ibmslapd**. Les résultats seront semblables à ce qui suit :

```
dsrdbm01 13797 1 0 Apr26 pts/1 00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root 32080 19149 0 23:17 pts/1 00:00:00 grep ibmslapd
```

Cet exemple montre que le démon de Tivoli Directory Server, **ibmslapd**, est en cours d'exécution.

- c. Exécutez la commande **ps -ef | grep ibmdiradm**. Les résultats seront semblables à ce qui suit :

```
root 4394 14038 0 14:17 pts/2 00:00:00 grep ibmdiradm
dsrdbm01 11055 1 0 Apr26 pts/1 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Cet exemple montre que le démon de Tivoli Directory Server, **ibmdiradm**, est en cours d'exécution.

8. Si Tivoli Directory Server, ibmslapd, n'est pas en cours d'exécution, procédez comme suit.
  - a. En tant qu'utilisateur *superutilisateur* Linux, exécutez `/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01` pour démarrer Directory Server
9. Si Tivoli Directory Administration Serveur, ibmdiradm, n'est pas en cours d'exécution, procédez comme suit :
  - a. Dans une session de terminal sur le serveur de messagerie, exécutez `su-dsrdbm01`.
  - b. Exécutez `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t` pour démarrer le serveur d'applications.
10. Si Tivoli Directory Server, ibmslapd, est en cours d'exécution, procédez comme suit :

**Remarque :** Effectuez cette étape même si Tivoli Directory Server a été lancé à l'étape précédente.

- a. Connectez-vous à une session de terminal sur le serveur de données en tant que dsrdbm01.
  - b. Exécutez `idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*` où `ADMIN_PASSWORD` est le mot de passe du compte administrateur du superutilisateur LDAP. Les objets utilisateur LDAP existants s'afficheront.
11. Vérifiez que Tivoli Directory Server Web Administration Tool est en cours d'exécution. Tivoli Directory Server Web Administration Tool est utilisé pour arrêter et démarrer l'instance LDAP, pour ajouter des utilisateurs ou des comptes et pour visualiser des fichiers journaux.
  - a. Connectez-vous à une session de terminal sur le serveur d'applications en tant que ibmadmin.
  - b. Exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password MDP_ADMIN_WAS` sur le serveur d'applications, où `MDP_ADMIN_WAS` est le mot de passe de l'administrateur de WebSphere Application Server (généralement admin). Si l'outil est en cours d'exécution, un message similaire au suivant sera renvoyé.
 

```
ADMU0508I : Le serveur d'applications "server1" est DEMARRE
Si le message suivant est renvoyé, le server1 doit être démarré.
ADMU0509I : Le serveur d'applications "server1" est inaccessible. Ce dernier est arrêté.
```
  - c. Pour démarrer server1, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh server1`. Le serveur server1 démarrera et un message similaire au suivant s'affichera.
 

```
ADMU3000I : Serveur server1 prêt pour e-business ; l'ID de processus est 26654
```
12. Accédez à Tivoli Directory Server Web Administration Tool à l'adresse suivante : `http://HOTE_SERVEUR_APPLICATIONS:9081/IDSWebApp`, `HOTE_SERVEUR_APPLICATIONS` correspondant au nom d'hôte du serveur d'applications 1.
13. Connectez-vous avec le compte administrateur du superutilisateur LDAP, `cn=root`, et le mot de passe approprié. Le nom du serveur LDAP doit être `DATABASE_DIRECTORY_SERVER_HOST:389`, où `DATABASE_DIRECTORY_SERVER_HOST` est le nom d'hôte du serveur de messagerie.
14. Cliquez sur **Administration du serveur > Démarrer/arrêter/réinitialiser le serveur**. Le statut du serveur LDAP s'affichera. Cette page peut également être utilisée pour démarrer, arrêter ou réinitialiser le serveur LDAP.
15. Le serveur proxy Tivoli Directory Server peut être arrêté à l'aide de l'outil de contrôle de plateforme (DOPControl) ou en exécutant les tâches suivantes.
  - a. Sur serveur d'applications 1, démarrez une session de terminal et connectez-vous en tant qu'utilisateur `tdsproxy`. Si vous êtes connecté en tant qu'utilisateur `root`, basculez vers l'utilisateur `tdsproxy` en exécutant la commande `su - tdsproxy`.
  - b. Exécutez la commande `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy -k`. Des messages semblables à ceux qui suivent devraient être renvoyés.
 

```
GLPADM034I Instance de serveur Admin arrêtée : 'tdsproxy'.
```
  - c. Sur serveur d'applications 1, démarrez une session de terminal et connectez-vous en tant qu'utilisateur `racine`.

- d. Exécutez la commande `/opt/ibm/1dap/V6.3/sbin/ibmslapd -I tdsproxy -k`. Des messages semblables à ceux qui suivent devraient être renvoyés.

GLPSRV176I Instance de serveur d'annuaire arrêtée 'tdsproxy' normalement.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Répertoire (WebSphere Service Registry and Repository)

Le test Répertoire (WebSphere Service Registry and Repository) détermine le statut du serveur WebSphere Service Registry and Repository.

## Ressources

Le test Répertoire (WebSphere Service Registry and Repository) utilise les ressources suivantes :

- WebSphere Service Registry and Repository sur le serveur de processus.
- Serveur WebSphere Application Server WSRRServer1 (cluster WSRRCluster)

## Identification des problèmes

Si le test Répertoire (WebSphere Service Registry and Repository) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `wrr` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `wrr` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `wrr` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de processus. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de processus à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
  - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
    - Journal des erreurs : `/opt/IBM/WebSphere/AppServer/profiles/wrrProfile1/logs/WSRRServer1/SystemErr.log`
    - Journal de sortie : `/opt/IBM/WebSphere/AppServer/profiles/wrrProfile1/logs/WSRRServer1/SystemOut.log`

- Journal de début : /opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/startServer.log
4. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
  5. Vérifiez que le serveur WSRRServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
    - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.
    - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/serverStatus.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` où `WAS_ADMIN_USER` est l'ID administrateur WebSphere (normalement `admin`) et `WAS_ADMIN_PWD` est le mot de passe de l'administrateur WebSphere Application Server.
    - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
    - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WSRRServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startServer.sh WSRRServer1`. Ignorez cette étape si le message `ADMU0508I: The Application Server "WSRRServer1" is STARTED`. s'affiche. Si vous avez dû démarrer le serveur, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WSRRServer1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WSRRServer1`

Arrêtez les serveurs dans cet ordre :

- a. `WSRRServer1`
- b. `nodeagent`

Le serveur `WSRRServer1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur `WSRRServer1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server V8 à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications 1.
- b. Affichez le statut du serveur WSRRServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.
  - L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.
  - L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.
  - L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WSRRServer1

Arrêtez les serveurs dans cet ordre :

- a. WSRRServer1
- b. nodeagent

Pour arrêter le serveur WSRRServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur de processus : `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Messagerie (vérification de l'installation de Message Broker)

Le test Messagerie (vérification de l'installation de Message Broker) détermine si le courtier de messages et le gestionnaire de files d'attente sont accessibles.

## Ressources

Le test Messagerie (vérification de l'installation de Message Broker) utilise la ressource suivante :

- WebSphere Portal Server (sur le serveur d'applications).

## Identification des problèmes

Si le test Messagerie (vérification de l'installation de Message Broker) échoue, procédez comme suit pour rechercher et résoudre le problème.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez msg et indiquez le mot de passe de votre topologie dans *motdepasse\_topologie*.

- a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

- b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

Vous pouvez également exécuter les commandes suivantes à partir du serveur de messagerie pour vérifier le statut de WebSphere Message Broker :

```
su - mqm
```

```
dspm
```

Si WebSphere Message Broker est en cours d'exécution, QMNAME(DFT.MB.QM) STATUT(En cours d'exécution) est renvoyé. Si WebSphere Message Broker n'est pas en cours d'exécution, QMNAME(DFT.MB.QM) STATUT(Arrêt normal) est renvoyé.

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de messagerie. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de messagerie à partir du serveur d'applications et vice-versa. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier /etc/hosts.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Recherchez les erreurs dans les journaux. Les journaux sont stockés sur le serveur de messagerie dans le répertoire /var/log/messages. Recherche des messages avec le préfixe 'BIP'. Recherchez également des noms de file d'attente et des horodatages lorsque le test a été exécuté.
6. Si WebSphere Message Broker n'est pas en cours d'exécution, démarrez-le à l'aide de l'outil de contrôle de plateforme ou en exécutant les étapes suivantes.

- a. Exécutez les commandes suivantes :

```
su - mqmconn
```

```
source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
MQSI 8.0.0.1
```

```
/opt/IBM/mqsi/8.0.0.1
```

- b. Exécutez la commande suivante.

```
strmqm -x DFT.MB.QM
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

Le gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' est en cours de démarrage. Le gestionnaire de files d'attente est associé à l'installation 'Installation1'. 5 enregistrements de journal consultés sur le gestionnaire de files d'attente 'DFT.MB.QM' pendant la phase de relecture des journaux. Relecture des journaux pour le gestionnaire de files d'attente 'DFT.MB.QM' terminée. Etat du gestionnaire de transactions restauré pour le gestionnaire de files d'attente 'DFT.MB.QM'. Gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' démarré à l'aide de V7.5.0.0.

c. Exécuter la commande suivante :

```
mqsistart DFT_BROKER
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
BIP8096I : Lancement de la commande réussi, consultez le journal système pour vérifier que le composant a démarré sans problème et qu'il continue à s'exécuter sans problème.
```

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Messagerie (vérification de l'installation de Message Broker) [1]

Le test Messagerie (vérification de l'installation de Message Broker) [1] détermine si le courtier de messages et le gestionnaire de files d'attente sont accessibles sur le serveur principal dans un environnement à haute disponibilité.

## Ressources

Le test Messagerie (vérification de l'installation de Message Broker) [1] utilise la ressource suivante :

- WebSphere Portal Server (sur le serveur d'applications).

## Identification des problèmes

Si le test Messagerie (vérification de l'installation de Message Broker) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez *status* pour *action* et *msgpri* pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez *status* pour *action* et *msgsb* pour *composant*.
  - Pour démarrer le serveur principal, indiquez *start* pour *action* et *msgpri* pour *composant*.
  - Pour démarrer le serveur de secours, indiquez *start* pour *action* et *msgsb* pour *composant*.
  - Pour arrêter le serveur principal, indiquez *stop* pour *action* et *msgpri* pour *composant*.
  - Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *msgsb* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*. Le *composant* *msg* peut également être utilisé pour démarrer, arrêter ou obtenir le statut de serveur de messagerie 1 et serveur de messagerie 2.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

Vous pouvez également exécuter les commandes suivantes à partir du serveur de messagerie pour vérifier le statut de WebSphere Message Broker :

```
su - mqm
```

```
dspmqs
```

Si WebSphere Message Broker est en cours d'exécution sur serveur de messagerie 1, QMNAME(DFT.MB.QM) STATUT(En cours d'exécution) est renvoyé. Si WebSphere Message Broker est en cours d'exécution sur serveur de messagerie 2, QMNAME(DFT.MB.QM) STATUT(En cours d'exécution en secours) est renvoyé. Si WebSphere Message Broker n'est pas en cours d'exécution, QMNAME(DFT.MB.QM) STATUT(Arrêt normal) est renvoyé.

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de messagerie. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de messagerie à partir du serveur d'applications et vice-versa. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Recherchez les erreurs dans les journaux. Les journaux sont stockés sur le serveur de messagerie dans le répertoire `/var/log/messages`. Recherche des messages avec le préfixe 'BIP'. Recherchez également des noms de file d'attente et des horodatages lorsque le test a été exécuté.
6. Si WebSphere Message Broker n'est pas en cours d'exécution, démarrez-le à l'aide de l'outil de contrôle de plateforme ou en exécutant les étapes suivantes.

- a. Exécutez les commandes suivantes :

```
su - mqmconn
source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
MQSI 8.0.0.1
/opt/IBM/mqsi/8.0.0.1
```

- b. Exécutez la commande suivante.

```
strmqm -x DFT.MB.QM
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
Le gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' est en cours de démarrage.
Le gestionnaire de files d'attente est associé à l'installation 'Installation1'.
5 enregistrements de journal consultés sur le gestionnaire de files d'attente 'DFT.MB.QM'
pendant la phase de relecture des journaux. Relecture des journaux pour le gestionnaire
de files d'attente 'DFT.MB.QM' terminée. Etat du gestionnaire de transactions
restauré pour le gestionnaire de files d'attente 'DFT.MB.QM'.
Gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' démarré à l'aide de V7.5.0.0.
```

- c. Exécutez la commande suivante :

```
mqsistart DFT_BROKER
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

BIP8096I : Lancement de la commande réussi, consultez le journal système pour vérifier que le composant a démarré sans problème et qu'il continue à s'exécuter sans problème.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Messagerie (vérification de l'installation de Message Broker) [2]

Le test Messagerie (vérification de l'installation de Message Broker) [2] détermine si le courtier de messages et le gestionnaire de files d'attente sont accessibles sur le serveur de sauvegarde dans un environnement à haute disponibilité.

## Ressources

Le test Messagerie (vérification de l'installation de Message Broker) [2] utilise les ressources suivantes :

- WebSphere Portal Server (sur le serveur d'applications).

## Identification des problèmes

Si le test Messagerie (vérification de l'installation de Message Broker) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut du serveur principal, indiquez *status* pour *action* et *msgpri* pour *composant*.
  - Pour vérifier le statut du serveur de secours, indiquez *status* pour *action* et *msgsb* pour *composant*.
  - Pour démarrer le serveur principal, indiquez *start* pour *action* et *msgpri* pour *composant*.
  - Pour démarrer le serveur de secours, indiquez *start* pour *action* et *msgsb* pour *composant*.
  - Pour arrêter le serveur principal, indiquez *stop* pour *action* et *msgpri* pour *composant*.
  - Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *msgsb* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*. Le *composant* *msg* peut également être utilisé pour démarrer, arrêter ou obtenir le statut de serveur de messagerie 1 et serveur de messagerie 2.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

Vous pouvez également exécuter les commandes suivantes à partir du serveur de messagerie pour vérifier le statut de WebSphere Message Broker :

```
su - mqm
```

```
dspm
```

Si WebSphere Message Broker est en cours d'exécution sur serveur de messagerie 1, QMNAME(DFT.MB.QM) STATUT(En cours d'exécution) est renvoyé. Si WebSphere Message Broker est en cours d'exécution sur serveur de messagerie 2, QMNAME(DFT.MB.QM) STATUT(En cours d'exécution en secours) est renvoyé. Si WebSphere Message Broker n'est pas en cours d'exécution, QMNAME(DFT.MB.QM) STATUT(Arrêt normal) est renvoyé.

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de messagerie. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de messagerie à partir du serveur d'applications

et vice-versa. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Recherchez les erreurs dans les journaux. Les journaux sont stockés sur le serveur de messagerie dans le répertoire `/var/log/messages`. Recherche des messages avec le préfixe 'BIP'. Recherchez également des noms de file d'attente et des horodatages lorsque le test a été exécuté.
6. Si WebSphere Message Broker n'est pas en cours d'exécution, démarrez-le à l'aide de l'outil de contrôle de plateforme ou en exécutant les étapes suivantes.

- a. Exécutez les commandes suivantes :

```
su - mqmconn
source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
MQSI 8.0.0.1
/opt/IBM/mqsi/8.0.0.1
```

- b. Exécutez la commande suivante.

```
strmqm -x DFT.MB.QM
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
Le gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' est en cours de démarrage.
Le gestionnaire de files d'attente est associé à l'installation 'Installation1'.
5 enregistrements de journal consultés sur le gestionnaire de files d'attente 'DFT.MB.QM'
pendant la phase de relecture des journaux. Relecture des journaux pour le gestionnaire
de files d'attente 'DFT.MB.QM' terminée. Etat du gestionnaire de transactions
restauré pour le gestionnaire de files d'attente 'DFT.MB.QM'.
Gestionnaire de files d'attente WebSphere MQ 'DFT.MB.QM' démarré à
l'aide de V7.5.0.0.
```

- c. Exécuter la commande suivante :

```
mqsistart DFT_BROKER
```

Des messages semblables à ceux qui suivent devraient être renvoyés.

```
BIP8096I : Lancement de la commande réussi, consultez le journal système pour
vérifier que le composant a démarré sans problème et qu'il
continue à s'exécuter sans problème.
```

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Mobile (console IBM Worklight)

Le test Mobile (console IBM Worklight) détermine si le serveur IBM Worklight est en cours d'exécution et si la console d'administration est disponible.

**Remarque :** IBM Worklight est disponible uniquement pour installation via un mandat IBM Services.

### Ressources

Le test Mobile (console IBM Worklight) utilise la ressource suivante :

- WebSphere Application Server appelé WorklightServer1

### Identification des problèmes

Si le test Mobile (console IBM Worklight) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez wrklt et indiquez le mot de passe de votre topologie dans *motdepasse\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
  - c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

4. Testez que le serveur WorklightServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici la procédure manuelle à suivre :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "WorklightServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WorklightServer1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "WorklightServer1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WorklightServer1`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WorklightServer1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WorklightServer1`

Arrêtez les serveurs dans cet ordre :

- a. `WorklightServer1`
- b. `nodeagent`

Le serveur `WorklightServer1` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Testez que le serveur `WorklightServer1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur `WorklightServer1` en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.  
L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de ❌ indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de ? indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer1

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer1
- b. nodeagent

Pour arrêter le serveur WorklightServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Test Mobile (console IBM Worklight)[1]

Le test Mobile (console IBM Worklight)[1] détermine si le serveur IBM Worklight principal dans un environnement à haute disponibilité est en cours d'exécution et si la console d'administration est disponible.

**Remarque :** IBM Worklight est disponible uniquement pour installation via un mandat IBM Services.

## Ressources

Le test Mobile (console IBM Worklight)[1] utilise la ressource suivante :

- WebSphere Application Server appelé WorklightServer1

## Identification des problèmes

Si le test Mobile (console IBM Worklight)[1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut d'IBM Worklight, indiquez `status` pour *action* et `wrkl` pour *composant*.
  - Pour démarrer IBM Worklight, indiquez `start` pour *action* et `wrkl` pour *composant*.
  - Pour arrêter IBM Worklight, indiquez `stop` pour *action* et `wrkl` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
- b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
- c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
- /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log
  - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Testez que le serveur WorklightServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici la procédure manuelle à suivre :
- a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "WorklightServer1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WorklightServer1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "WorklightServer1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WorklightServer1`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WorklightServer1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WorklightServer1`

Arrêtez les serveurs dans cet ordre :

- a. `WorklightServer1`
- b. `nodeagent`

Le serveur `WorklightServer1` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où

*ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere.

5. Testez que le serveur WorklightServer1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *APPLICATION\_SERVER\_HOST* est le nom d'hôte du serveur d'applications.
- b. Affichez le statut du serveur WorklightServer1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer1

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer1
- b. nodeagent

Pour arrêter le serveur WorklightServer1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere.

## Test Mobile (console IBM Worklight)[2]

Le test Mobile (console IBM Worklight)[2] détermine si le serveur IBM Worklight de sauvegarde d'un environnement à haute disponibilité est en cours d'exécution et si la console d'administration est disponible.

**Remarque :** IBM Worklight est disponible uniquement pour installation via un mandat IBM Services.

## Ressources

Le test Mobile (console IBM Worklight)[2] utilise la ressource suivante :

- WebSphere Application Server appelé WorklightServer2

## Identification des problèmes

Si le test Mobile (console IBM Worklight)[2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour vérifier le statut d'IBM Worklight, indiquez *status* pour *action* et *wrkl* pour *composant*.
  - Pour démarrer IBM Worklight, indiquez *start* pour *action* et *wrkl* pour *composant*.
  - Pour arrêter IBM Worklight, indiquez *stop* pour *action* et *wrkl* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
  - c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WorklightServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications 2, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté.` s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE.` s'affiche. Si vous avez dû démarrer le serveur *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654.`
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WorklightServer2". Ce dernier est arrêté.` s'affiche, démarrez le serveur *WorklightServer2* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startServer.sh WorklightServer2`. Ignorez cette étape si le message `ADMU0508I : Le serveur`

d'applications "WorklightServer2" est DEMARRE. s'affiche. Si vous avez dû démarrer WorklightServer2, un message similaire au suivant s'affiche : ADMU3000I : Serveur WorklightServer2 prêt pour e-business ; l'ID de processus est 26654.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer2

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer2
- b. nodeagent

Le serveur WorklightServer2 est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopServer.sh -all -username ADMIN\_WAS -password MDP\_ADMIN\_WAS où ADMIN\_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP\_ADMIN\_WAS est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username ADMIN\_WAS -password MDP\_ADMIN\_WAS où ADMIN\_WAS est l'ID administrateur WebSphere (admin en règle générale) et MDP\_ADMIN\_WAS est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WorklightServer2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. APPLICATION\_SERVER\_HOST est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur WorklightServer2 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WorklightServer2

Arrêtez les serveurs dans cet ordre :

- a. WorklightServer2
- b. nodeagent

Pour arrêter le serveur WorklightServer2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Surveillance (Netcool Omnibus)

Le test Surveillance (Netcool Omnibus) détermine si le serveur Tivoli Netcool/OMNIBus est accessible.

## Ressources

Le test Surveillance (Netcool Omnibus) utilise la ressource suivante :

- serveur Tivoli Netcool/OMNIBus sur le serveur de surveillance.

## Identification des problèmes

Si le test Surveillance (Netcool Omnibus) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `ncobus` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `ncobus` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `ncobus` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez que les services serveur de contrôle de processus et de l'agent sont en cours d'exécution.
  - a. Sur le serveur de surveillance, exécutez la commande `/opt/IBM/netcool/omnibus/bin/nco_pa_status -server NCO_PA -user netcool -password mot_de_passe_netcool` où `mot_de_passe_netcool` est le mot de passe défini dans la propriété `OMNIBUS.OWNER.ACCOUNT.PWD` du fichier de propriétés de topologie. Une sortie semblable à ce qui suit devrait être renvoyée. La colonne Status doit contenir la valeur `RUNNING`.

```

Service Name Process Name Hostname User Status PID

Core MasterObjectServer dopmon netcool RUNNING 3595

```

- b. Si les services ne sont pas lancés ni en cours d'exécution, démarrez le serveur en exécutant la commande `/etc/init.d/nco start` sur le serveur de surveillance en tant qu'utilisateur `netcool`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
    - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
    - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
- c. Sur le serveur de surveillance, consultez tous les journaux commençant par NCO dans les répertoires suivants.
    - /opt/IBM/netcool/log
    - /opt/IBM/netcool/omnibus/log
  4. Vérifiez que le système de fichiers sur le serveur de surveillance n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
  5. Vérifiez que le portlet Tivoli Netcool/OMNIBus est accessible à partir du serveur d'applications à l'adresse `http://hôte_serveur_surveillance:16310/ibm/console` où `hôte_serveur_surveillance` est le nom d'hôte du serveur d'applications.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Surveillance (Tivoli Enterprise Monitoring Server)

Le test Surveillance (Tivoli Enterprise Monitoring Server) détermine le statut du serveur Tivoli Enterprise Monitoring.

### Ressources

Le test Surveillance (Tivoli Enterprise Monitoring Server) utilise les ressources suivantes :

- services Web Tivoli Enterprise Monitoring serveur SOAP sur le serveur de surveillance.
- serveur Tivoli Enterprise Portal sur le serveur de surveillance.
- base de données Tivoli Enterprise Portal DB2 sur le serveur de surveillance.

## Identification des problèmes

Si le test Surveillance (Tivoli Enterprise Monitoring Server) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `tems` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `tems` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `tems` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de surveillance. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de surveillance à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur de surveillance, consultez les journaux de surveillance suivants :

- Serveur Tivoli Enterprise Monitoring : /opt/IBM/ITM/logs/  
hôte\_serveur\_surveillance\_ms\_\*.log
- Serveur Tivoli Enterprise Portal : /opt/IBM/ITM/logs/hôte\_serveur\_surveillance\_cq\_\*.log
- WebSphere Application Server intégré :
  - Journal des erreurs : /opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/  
SystemErr.log
  - Journal de sortie : /opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/  
SystemOut.log
  - Journal de début : /opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/  
startServer.log

Où *hôte\_serveur\_surveillance* est le nom d'hôte du serveur de surveillance.

4. Vérifiez que le système de fichiers sur le serveur de surveillance n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
5. Vérifiez que les composants Tivoli Enterprise Monitoring sont en cours d'exécution sur le serveur serveur de surveillance.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - b. Exécutez la commande **/opt/IBM/ITM/bin/cinfo -r**.
6. Vérifiez que les bases de données de Tivoli Components sont opérationnelles.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant qu'utilisateur db2inst1.
  - b. Exécutez la commande **ps -ef | grep db2inst1**.
  - c. Vérifiez que les processus DB2 suivants sont en cours d'exécution : db2sync, db2vend et db2acd.
  - d. Si les processus DB2 ne sont pas en cours d'exécution, exécutez la commande **db2start**.
  - e. Consultez les journaux DB2 sur le serveur de données pour afficher toutes les erreurs de base de données associées au démarrage des bases de données utilisées par Tivoli Components. Ces fichiers journaux se trouvent dans le répertoire/datahome/db2inst1/sql1lib/db2dump de serveur de données.
7. Vérifiez que le serveur Tivoli Enterprise Monitoring est en cours d'exécution en recherchant une entrée pour ms. Si cette entrée n'est pas répertoriée, le serveur Tivoli Enterprise Monitoring n'est pas en cours d'exécution.
8. Si le serveur Tivoli Enterprise Monitoring n'est pas en cours d'exécution, démarrez-le.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - b. Exécutez la commande **/opt/IBM/ITM/bin/itmcmd server start HUB\_MWOS**.
9. Vérifiez que le serveur Tivoli Enterprise Portal est en cours d'exécution en recherchant une entrée pour cq dans les résultats de la commande **/opt/IBM/ITM/bin/cinfo -r**. Si l'entrée n'est pas répertoriée, le serveur Tivoli Enterprise Portal n'est pas en cours d'exécution.
10. Si le serveur Tivoli Enterprise Portal n'est pas en cours d'exécution, démarrez-le.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - b. Exécutez la commande **/opt/IBM/ITM/bin/itmcmd agent start cq**.
11. Vérifiez que les autres sous-composants suivants sont exécutés dans les résultats de la commande **/opt/IBM/ITM/bin/cinfo -r**.
  - kf** serveur d'aide Eclipse

**1z** Agent de surveillance pour Linux OS

12. Si les sous-composants ne sont pas en cours d'exécution, démarrez les agents IBM Defense Operations Platform en exécutant la commande **DOPControl -a start -c agents -p mot\_de\_passe\_topologie** où *mot\_de\_passe\_topologie* est le mot de passe de topologie.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Surveillance (Tivoli Enterprise Portal Server)

Le test Surveillance (Tivoli Enterprise Portal Server) détermine le statut du serveur Tivoli Enterprise Portal.

## Ressources

Le test Surveillance (Tivoli Enterprise Portal Server) utilise les ressources suivantes :

- services Web Tivoli Enterprise Monitoring serveur SOAP sur le serveur de surveillance.
- serveur Tivoli Enterprise Portal sur le serveur de surveillance.
- base de données Tivoli Enterprise Portal DB2 sur le serveur de surveillance.

## Identification des problèmes

Si le test Surveillance (Tivoli Enterprise Portal Server) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *teps* pour *composant*.
  - Pour démarrer le serveur, indiquez *start* pour *action* et *teps* pour *composant*.
  - Pour arrêter le serveur, indiquez *stop* pour *action* et *teps* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de surveillance. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de surveillance à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur de surveillance, consultez les journaux de surveillance suivants :
    - Serveur Tivoli Enterprise Monitoring : `/opt/IBM/ITM/logs/hôte_serveur_surveillance_ms_*.log`
    - Serveur Tivoli Enterprise Portal : `/opt/IBM/ITM/logs/hôte_serveur_surveillance_cq_*.log`
    - WebSphere Application Server intégré :
      - Journal des erreurs : `/opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
      - Journal de sortie : `/opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`

- Journal de début : /opt/IBM/ITM/1x8266/iw/profiles/ITMProfile/logs/ITMServer/startServer.log

Où *hôte\_serveur\_surveillance* est le nom d'hôte du serveur de surveillance.

- Vérifiez que le système de fichiers sur le serveur de surveillance n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
- Vérifiez que les composants Tivoli Enterprise Monitoring sont en cours d'exécution sur le serveur de surveillance.
  - Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - Exécutez la commande **/opt/IBM/ITM/bin/cinfo -r**.
- Vérifiez que les bases de données de Tivoli Components sont opérationnelles.
  - Connectez-vous à une session de terminal sur le serveur de surveillance en tant qu'utilisateur db2inst1.
  - Exécutez la commande **ps -ef | grep db2inst1**.
  - Vérifiez que les processus DB2 suivants sont en cours d'exécution : db2sync, db2vend et db2acd.
  - Si les processus DB2 ne sont pas en cours d'exécution, exécutez la commande **db2start**.
  - Consultez les journaux DB2 sur le serveur de données pour afficher toutes les erreurs de base de données associées au démarrage des bases de données utilisées par Tivoli Components. Ces fichiers journaux se trouvent dans le répertoire/datahome/db2inst1/sqllib/db2dump de serveur de données.
- Vérifiez que le serveur Tivoli Enterprise Monitoring est en cours d'exécution en recherchant une entrée pour ms. Si cette entrée n'est pas répertoriée, le serveur Tivoli Enterprise Monitoring n'est pas en cours d'exécution.
- Si le serveur Tivoli Enterprise Monitoring n'est pas en cours d'exécution, démarrez-le.
  - Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - Exécutez la commande **/opt/IBM/ITM/bin/itmcmd server start HUB\_MWOS**.
- Vérifiez que le serveur Tivoli Enterprise Portal est en cours d'exécution en recherchant une entrée pour cq dans les résultats de la commande **/opt/IBM/ITM/bin/cinfo -r**. Si l'entrée n'est pas répertoriée, le serveur Tivoli Enterprise Portal n'est pas en cours d'exécution.
- Si le serveur Tivoli Enterprise Portal n'est pas en cours d'exécution, démarrez-le.
  - Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - Exécutez la commande **/opt/IBM/ITM/bin/itmcmd agent start cq**.
- Vérifiez que les autres sous-composants suivants sont exécutés dans les résultats de la commande **/opt/IBM/ITM/bin/cinfo -r**.
  - kf** serveur d'aide Eclipse
  - lz** Agent de surveillance pour Linux OS
- Si les sous-composants ne sont pas en cours d'exécution, démarrez les agents IBM Defense Operations Platform en exécutant la commande **DOPControl -a start -c agents -p mot\_de\_passe\_topologie** où *mot\_de\_passe\_topologie* est le mot de passe de topologie.

## Test Surveillance (Tivoli Integrated Portal/Netcool)

Le test Surveillance (Tivoli Integrated Portal/Netcool) détermine le statut du serveur Tivoli Integrated Portal.

## Ressources

Le test Surveillance (Tivoli Integrated Portal/Netcool) utilise la ressource suivante :

- Serveur Tivoli Integrated Portal sur le serveur de surveillance

## Identification des problèmes

Si le test Surveillance (Tivoli Integrated Portal/Netcool) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `ncobus` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `ncobus` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `ncobus` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez que les services serveur de contrôle de processus et de l'agent sont en cours d'exécution.
  - a. Sur le serveur de surveillance, exécutez la commande `/opt/IBM/netcool/omnibus/bin/nco_pa_status -server NCO_PA -user netcool -password mot_de_passe_netcool` où `mot_de_passe_netcool` est le mot de passe défini dans la propriété `OMNIBUS.OWNER.ACCOUNT.PWD` du fichier de propriétés de topologie. Une sortie semblable à ce qui suit devrait être renvoyée. La colonne `Status` doit contenir la valeur `RUNNING`.

| Service Name | Process Name       | Hostname | User    | Status  | PID  |
|--------------|--------------------|----------|---------|---------|------|
| Core         | MasterObjectServer | dopmon   | netcool | RUNNING | 3595 |

- b. Si les services ne sont pas lancés ni en cours d'exécution, démarrez le serveur en exécutant la commande `/etc/init.d/nco start` sur le serveur de surveillance en tant qu'utilisateur `netcool`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
    - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
    - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
    - c. Sur le serveur de surveillance, consultez tous les journaux commençant par `NCO` dans les répertoires suivants.
      - `/opt/IBM/netcool/log`
      - `/opt/IBM/netcool/omnibus/log`
      - `/opt/IBM/netcool/typ2/profiles/TIPProfile/logs/server1/SystemOut.log`
      - `/opt/IBM/netcool/typ2/profiles/TIPProfile/logs/server1/SystemErr.log`
  4. Vérifiez que le système de fichiers sur le serveur de surveillance n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande `df -h`. Le système de fichiers peut être considéré complet même

si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.

5. Vérifiez que le portlet Tivoli Netcool/OMNIBus est accessible à partir du serveur d'applications à l'adresse `http://hôte_serveur_surveillance:16310/ibm/console` où `hôte_serveur_surveillance` est le nom d'hôte du serveur d'applications.
6. Gérez le serveur Tivoli Integrated Portal à l'aide des commandes suivantes sur le serveur de surveillance.

- Vérifiez le statut du serveur Tivoli Integrated Portal en exécutant la commande suivante.

```
/opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/serverStatus.sh server1 -user utilisateur -password mot de passe
```

où *utilisateur* est la valeur de la propriété `OMNIBUS.ADMIN.ACCOUNT` dans le fichier de propriétés de la topologie et *mot de passe* est la valeur de la propriété `OMNIBUS.ADMIN.ACCOUNT.PWD` dans le fichier de propriétés de la topologie.

- Arrêtez le serveur Tivoli Integrated Portal en exécutant la commande suivante.

```
/opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/stopServer.sh server1 -user utilisateur -password mot de passe
```

où *utilisateur* est la valeur de la propriété `OMNIBUS.ADMIN.ACCOUNT` dans le fichier de propriétés de la topologie et *mot de passe* est la valeur de la propriété `OMNIBUS.ADMIN.ACCOUNT.PWD` dans le fichier de propriétés de la topologie.

- Démarrez le serveur Tivoli Integrated Portal en exécutant la commande suivante.

```
/opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/startServer.sh server1
```

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Gestion des mots de passe (Tivoli Directory Integrator)

Le test Gestion des mots de passe (Tivoli Directory Integrator) vérifie l'accès à Tivoli Directory Integrator.

## Ressources

Le test Gestion des mots de passe (Tivoli Directory Integrator) utilise la ressource suivante :

- Tivoli Directory Server (sur le serveur de données)
- Tivoli Directory Integrator (sur le serveur de données)

## Identification des problèmes

Si le test Gestion des mots de passe (Tivoli Directory Integrator) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `tdi` et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans un environnement à haute disponibilité, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour démarrer le serveur, indiquez *start* pour *action* et *tdi* pour *composant*.
- Pour arrêter le serveur, indiquez *stop* pour *action* et *tdi* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
  - c. Sur le serveur de données, examinez tous les journaux Tivoli Directory Server situés dans le répertoire suivant :
    - /opt/IBM/TDI/V7.1/timsol/logs
  - d. Sur le serveur de données, examinez tous les journaux Tivoli Directory Server :
    - /opt/IBM/TDI/V7.1/pwd\_plugins/tds/plugin.log
    - /opt/IBM/TDI/V7.1/pwd\_plugins/tds/proxy.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur Tivoli Directory Integrator est démarré.
- a. Connectez-vous au serveur de données en tant qu'utilisateur *ibmadmin*.
  - b. Démarrez ou redémarrez le serveur.
    - Pour démarrer le serveur, exécutez la commande **/opt/IBM/TDI/V7.1/timsol/ITIMAd start**.
    - Pour redémarrer le serveur, exécutez la commande **/opt/IBM/TDI/V7.1/timsol/ITIMAd restart**.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal via le serveur Web)

Le test Portail (console WebSphere Portal via le serveur Web) vérifie l'accès du serveur Web à la console WebSphere Portal.

## Ressources

Le test Portail (console WebSphere Portal via le serveur Web) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

## Identification des problèmes

Si le test Portail (console WebSphere Portal via le serveur Web) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez *wpe* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent". Ce dernier est arrêté. s'affiche, démarrez le nodeagent à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE. s'affiche. Si vous avez dû démarrer le nodeagent, un message similaire au suivant s'affiche : ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654.

- a. Si le message ADMU0509I : Impossible d'atteindre le serveur d'application "WebSphere\_Portal". Ce dernier est arrêté. s'affiche, démarrez WebSphere\_Portal à l'aide de la commande suivante : /opt/IBM/WebSphere/wp\_profile/bin/startServer.sh WebSphere\_Portal. Ignorez cette étape si le message ADMU0508I : le serveur d'applications "WebSphere\_Portal" est DEMARRE. s'affiche. Si vous avez dû démarrer WebSphere\_Portal, un message similaire au suivant s'affiche : ADMU3000I: Serveur WebSphere\_Portal prêt pour e-business ; l'ID de processus est 26654.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Le serveur WebSphere\_Portal est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp\_profile/bin/stopServer.sh -all -username *ADMIN\_WAS* -password *MDP\_ADMIN\_WAS* où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp\_profile/bin/stopNode.sh -username *ADMIN\_WAS* -password *MDP\_ADMIN\_WAS* où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse [http://APPLICATION\\_SERVER\\_HOST:9062/ibm/console](http://APPLICATION_SERVER_HOST:9062/ibm/console) avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *APPLICATION\_SERVER\_HOST* est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur WebSphere\_Portal en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/wp\_profile/bin/startNode.sh dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal via le serveur Web) [1]

Le test Portail (console WebSphere Portal via le serveur Web) [1] vérifie l'accès du serveur Web à la console WebSphere Portal sur le serveur principal dans un environnement à haute disponibilité.

## Ressources

Le test Portail (console WebSphere Portal via le serveur Web) [1] utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

## Identification des problèmes

Si le test Portail (console WebSphere Portal via le serveur Web) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `wpe` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `wpe` pour *composant*.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `wpe` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande `df -h`. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande `df -h` renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.

- b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
- c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le nodeagent à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le nodeagent, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
- a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "WebSphere_Portal"`. Ce dernier est arrêté. s'affiche, démarrez WebSphere\_Portal à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Ignorez cette étape si le message `ADMU0508I : le serveur d'applications "WebSphere_Portal" est DEMARRE`. s'affiche. Si vous avez dû démarrer WebSphere\_Portal, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WebSphere_Portal prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Le serveur WebSphere\_Portal est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur WebSphere\_Portal en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal via le serveur Web) [2]

Le test Portail (console WebSphere Portal via le serveur Web) [2] vérifie l'accès du serveur Web à la console WebSphere Portal sur le serveur de sauvegarde dans un environnement à haute disponibilité.

## Ressources

Le test Portail (console WebSphere Portal via le serveur Web) [2] utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications 2.

## Identification des problèmes

Si le test Portail (console WebSphere Portal via le serveur Web) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `wpe` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `wpe` pour *composant*.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `wpe` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

- c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere\_Portal\_PortalNode2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WebSphere_Portal_PortalNode2"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WebSphere_Portal_PortalNode2` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Ignorez cette étape si le message `ADMU0508I : le serveur d'applications "WebSphere_Portal_PortalNode2" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WebSphere_Portal_PortalNode2`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WebSphere_Portal_PortalNode2 prêt pour e-business; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WebSphere_Portal_PortalNode2`

Arrêtez les serveurs dans cet ordre :

- a. `WebSphere_Portal_PortalNode2`
- b. `nodeagent`

Le serveur `WebSphere_Portal_PortalNode2` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere\_Portal\_PortalNode2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
- b. Affichez le statut du serveur WebSphere\_Portal\_PortalNode2 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal\_PortalNode2

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal\_PortalNode2
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal\_PortalNode2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal)

Le test Portail (console WebSphere Portal) vérifie l'accès à la console WebSphere Portal.

## Ressources

Le test Portail (console WebSphere Portal) utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

## Identification des problèmes

Si le test Portail (console WebSphere Portal) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez *wpe* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```
2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "WebSphere_Portal"`. Ce dernier est arrêté. s'affiche, démarrez *WebSphere\_Portal* à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Ignorez cette étape si le message `ADMU0508I : le serveur d'applications "WebSphere_Portal" est DEMARRE`. s'affiche. Si vous avez dû démarrer *WebSphere\_Portal*, un message similaire au suivant s'affiche : `ADMU3000I: Serveur WebSphere_Portal prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Le serveur WebSphere\_Portal est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur WebSphere\_Portal en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal) [1]

Le test Portail (console WebSphere Portal) [1] vérifie l'accès à la console WebSphere Portal sur le serveur principal dans un environnement à haute disponibilité.

### Ressources

Le test Portail (console WebSphere Portal) [1] utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications.

### Identification des problèmes

Si le test Portail (console WebSphere Portal) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez *status* pour *action* et *wpe* pour *composant*.
  - Pour démarrer le serveur, indiquez *start* pour *action* et *wpe* pour *composant*.
  - Pour arrêter le serveur, indiquez *stop* pour *action* et *wpe* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.

- a. Si le message ADMU0509I : Impossible d'atteindre le serveur d'application "WebSphere\_Portal". Ce dernier est arrêté. s'affiche, démarrez WebSphere\_Portal à l'aide de la commande suivante : /opt/IBM/WebSphere/wp\_profile/bin/startServer.sh WebSphere\_Portal. Ignorez cette étape si le message ADMU0508I : le serveur d'applications "WebSphere\_Portal" est DEMARRE. s'affiche. Si vous avez dû démarrer WebSphere\_Portal, un message similaire au suivant s'affiche : ADMU3000I: Serveur WebSphere\_Portal prêt pour e-business ; l'ID de processus est 26654.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Le serveur WebSphere\_Portal est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp\_profile/bin/stopServer.sh -all -username *ADMIN\_WAS* -password *MDP\_ADMIN\_WAS* où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : /opt/IBM/WebSphere/wp\_profile/bin/stopNode.sh -username *ADMIN\_WAS* -password *MDP\_ADMIN\_WAS* où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur WebSphere\_Portal est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse [http://APPLICATION\\_SERVER\\_HOST:9062/ibm/console](http://APPLICATION_SERVER_HOST:9062/ibm/console) avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. *APPLICATION\_SERVER\_HOST* est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur WebSphere\_Portal en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande /opt/IBM/WebSphere/wp\_profile/bin/startNode.sh dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Portail (console WebSphere Portal) [2]

Le test Portail (console WebSphere Portal) [2] vérifie l'accès à la console WebSphere Portal sur le serveur de sauvegarde dans un environnement à haute disponibilité.

## Ressources

Le test Portail (console WebSphere Portal) [2] utilise la ressource suivante :

- WebSphere Application Server surserveur d'applications 2.

## Identification des problèmes

Si le test Portail (console WebSphere Portal) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des serveurs et les démarrer et les arrêter si nécessaire. Exécutez les commandes suivantes en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `wpe` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `wpe` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `wpe` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
  - c. Sur le serveur d'applications 2, consultez les journaux WebSphere Application Server suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande `df -h`. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande `df -h` renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

4. Vérifiez que le serveur WebSphere\_Portal\_PortalNode2 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "WebSphere_Portal_PortalNode2"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `WebSphere_Portal_PortalNode2` à l'aide de la commande suivante : `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Ignorez cette étape si le message `ADMU0508I : le serveur d'applications "WebSphere_Portal_PortalNode2" est DEMARRE`. s'affiche. Si vous avez dû démarrer `WebSphere_Portal_PortalNode2`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur WebSphere_Portal_PortalNode2 prêt pour e-business; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `WebSphere_Portal_PortalNode2`

Arrêtez les serveurs dans cet ordre :

- a. `WebSphere_Portal_PortalNode2`
- b. `nodeagent`

Le serveur `WebSphere_Portal_PortalNode2` est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur `WebSphere_Portal_PortalNode2` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Affichez le statut du serveur `WebSphere_Portal_PortalNode2` en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de ➡ indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de ✖ indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de ⓘ indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. WebSphere\_Portal\_PortalNode2

Arrêtez les serveurs dans cet ordre :

- a. WebSphere\_Portal\_PortalNode2
- b. nodeagent

Pour arrêter le serveur WebSphere\_Portal\_PortalNode2, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Process Management (Console Business Process Manager - Business Space)

Le test Process Management (Console Business Process Manager - Business Space) détermine si le serveur IBM Business Process Manager est en cours d'exécution.

## Ressources

Le test Process Management (Console Business Process Manager - Business Space) utilise la ressource suivante :

- WebSphere Application Server named WBM\_DE.AppTarget.WBMNode1.0

## Identification des problèmes

Si le test Process Management (Console Business Process Manager - Business Space) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut du composant et le démarrer et l'arrêter si nécessaire. Pour *composant*, utilisez bpm et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
  - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM\_DE.AppTarget.BPMNode1.0/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM\_DE.AppTarget.BPMNode1.0/SystemErr.log
3. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
4. Vérifiez que le serveur BPM\_DE.AppTarget.BPMNode1.0 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` où `WAS_ADMIN_USER` est l'ID administrateur WebSphere (normalement `admin`) et `WAS_ADMIN_PWD` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I: Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I: Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le serveur `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I: Serveur nodeagent prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "BPM_DE.AppTarget.BPMNode1.0"`. Ce dernier est arrêté. s'affiche, lancez le serveur à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startServer.sh BPM_DE.AppTarget.BPMNode1.0`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "BPM_DE.AppTarget.BPMNode1.0" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `the_DE_AppTarget.WBMNode1.0`, un message similaire au suivant s'affiche : `ADMU3000I : Serveur BPM_DE.AppTarget.BPMNode1.0 prêt pour e-business; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `BPM_DE.AppTarget.BPMNode1.0`

Arrêtez les serveurs dans cet ordre :

- a. BPM\_DE.AppTarget.BPMNode1.0
- b. nodeagent

Le serveur BPM\_DE.AppTarget.BPMNode1.0 est arrêté en exécutant la commande suivante dans une fenêtre de commande, sur le serveur de processus : /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopServer.sh -all -username ADMIN\_WAS -password WAS\_ADMIN\_PWD où ADMIN\_WAS est l'ID administrateur WebSphere (normalement admin) et MDP\_ADMIN\_WAS est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username WAS\_ADMIN\_USER -password WAS\_ADMIN\_PWD où ADMIN\_WAS est l'ID administrateur WebSphere (normalement admin) et MDP\_ADMIN\_WAS est le mot de passe de l'administrateur WebSphere.

5. Vérifiez que le serveur BPM\_DE.AppTarget.BPMNode1.0 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

- a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9062/ibm/console` avec l'ID et le mot de passe de l'administrateur de WebSphere Application Server. APPLICATION\_SERVER\_HOST est le nom d'hôte du serveur d'applications.
- b. Affichez le statut du serveur BPM\_DE.AppTarget.BPMNode1.0 en cliquant sur **Serveurs > Types de serveurs > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer l'agent de noeud, exécutez la commande /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. BPM\_DE.AppTarget.BPMNode1.0

Arrêtez les serveurs dans cet ordre :

- a. BPM\_DE.AppTarget.BPMNode1.0
- b. nodeagent

Pour arrêter le serveur BPM\_DE.AppTarget.BPMNode1.0, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté en exécutant la commande suivante dans une fenêtre de commande sur le serveur de processus : /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username WAS\_ADMIN\_USER -password WAS\_ADMIN\_PWD où ADMIN\_WAS est l'ID administrateur WebSphere (normalement admin) et MDP\_ADMIN\_WAS est le mot de passe de l'administrateur WebSphere.

## Test Gestion de processus (Console Business Process Manager)

Le test Gestion de processus (Console Business Process Manager) détermine si l'accès à WebSphere Business Process Management est possible.

### Ressources

Le test Gestion de processus (Console Business Process Manager) utilise la ressource suivante :

- WebSphere Business Process Management sur le serveur de processus.
- Serveur WebSphere Application Server BPM\_DE.AppTarget.BPMNode1.0.

### Identification des problèmes

Si le test Gestion de processus (Console Business Process Manager) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

### Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et pour les démarrer ou les arrêter, en cas de besoin. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur, indiquez `status` pour *action* et `bpm` pour *composant*.
  - Pour démarrer le serveur, indiquez `start` pour *action* et `bpm` pour *composant*.
  - Pour arrêter le serveur, indiquez `stop` pour *action* et `bpm` pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Vérifiez qu'il existe une connectivité du réseau entre le serveur d'applications et le serveur de processus. Cette opération peut être effectuée par l'envoi de commandes **ping** avec le nom d'hôte qualifié complet et le nom d'hôte abrégé du serveur de processus à partir du serveur d'applications. Les résultats des commandes **ping** indiqueront si le nom d'hôte est correctement résolu par le DNS (système de noms de domaine) ou par le fichier `/etc/hosts`.
3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
  - c. Sur le serveur de processus, consultez les journaux de WebSphere Application Server suivants :
    - Journal des erreurs : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM.log`
    - Journal des erreurs : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM.log`
    - Journal de début : `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM.log`
4. Vérifiez que le système de fichiers sur le serveur de processus n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers peut être considéré complet même si son taux d'utilisation est inférieur à 100%. Pour cette raison, si la commande **df -h** renvoie que le système de fichiers est complet à 90% ou plus, vous devez considérer que le système de fichiers a atteint sa capacité.
5. Vérifiez que le serveur WebSphere Application Server fonctionne.
  - a. Sur le système du serveur de processus, connectez-vous en tant que `ibmadmin`.

- b. Exécutez la commande `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh BPM_DE.AppTarget.BPMNode1.0`.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Sécurité (console d'administration IBM Security Identity Manager)

Le test Sécurité (console d'administration IBM Security Identity Manager) détermine si le serveur IBM Security Identity Manager est en cours d'exécution et si la console d'administration est disponible.

## Ressources

Le test Sécurité (console d'administration IBM Security Identity Manager) utilise la ressource suivante :

- WebSphere Application Server nommé isim1.

## Identification des problèmes

Si le test Sécurité (console d'administration IBM Security Identity Manager) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *isim* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

- a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

- b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

- c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour vérifier le statut d'IBM Security Identity Manager, indiquez *status* pour *action* et *isim* pour *composant*.
- Pour arrêter IBM Security Identity Manager, indiquez *stop* pour *action* et *isim* pour *composant*.
- Pour démarrer IBM Security Identity Manager, indiquez *start* pour *action* et *isim* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

- a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
- `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

- b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
- c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
  - /opt/IBM/WebSphere/AppServerv7/profiles/isis1/logs/isis1/SystemOut.log
  - /opt/IBM/WebSphere/AppServerv7/profiles/isis1/logs/isis1/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur isim1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que `ibmadmin`.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "isis1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `isis1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/startServer.sh isim1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "isis1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `isis1`, un message similaire au suivant s'affiche : `ADMU3000I : serveur isim1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `isis1`

Arrêtez les serveurs dans cet ordre :

- a. `isis1`
- b. `nodeagent`

Le serveur `isis1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur isim1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :

a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9061/ibm/console` en utilisant l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.

b. Afficher le statut du serveur isim1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. isim1

Arrêtez les serveurs dans cet ordre :

- a. isim1
- b. nodeagent

Pour arrêter le serveur isim1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Sécurité (console IBM Security Identity Manager)

Le test Sécurité (console IBM Security Identity Manager) détermine si le serveur IBM Security Identity Manager est en cours d'exécution et si la console est disponible.

## Ressources

Le test Sécurité (console IBM Security Identity Manager) utilise la ressource suivante :

- WebSphere Application Server nommé isim1.

## Identification des problèmes

Si le test Sécurité (console IBM Security Identity Manager) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez *isim* et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a status -c composant -p mot_de_passe_de_topologie
```

b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a start -c composant -p mot_de_passe_de_topologie
```

c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour vérifier le statut d'IBM Security Identity Manager, indiquez *status* pour *action* et *isim* pour *composant*.
- Pour arrêter IBM Security Identity Manager, indiquez *stop* pour *action* et *isim* pour *composant*.
- Pour démarrer IBM Security Identity Manager, indiquez *start* pour *action* et *isim* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.

a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log

b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :

- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
- /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log

c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :

- /opt/IBM/WebSphere/AppSrv7/profiles/isim1/logs/isim1/SystemOut.log
- /opt/IBM/WebSphere/AppSrv7/profiles/isim1/logs/isim1/SystemErr.log

4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.

5. Vérifiez que le serveur *isim1* est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :

a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.

- b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (normalement `admin`) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.
- c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le `nodeagent` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le `nodeagent`, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
- a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "isis1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur `isis1` à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/startServer.sh isis1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "isis1" est DEMARRE`. s'affiche. Si vous avez dû démarrer `isis1`, un message similaire au suivant s'affiche : `ADMU3000I : serveur isis1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. `nodeagent`
- b. `isis1`

Arrêtez les serveurs dans cet ordre :

- a. `isis1`
- b. `nodeagent`

Le serveur `isis1` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur `nodeagent` est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isis1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (`admin` en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

- 6. Vérifiez que le serveur `isis1` est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9061/ibm/console` en utilisant l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Afficher le statut du serveur `isis1` en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.

L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.

L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.

L'icône en forme de ⓘ indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. isim1

Arrêtez les serveurs dans cet ordre :

- a. isim1
- b. nodeagent

Pour arrêter le serveur isim1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Sécurité (console en libre service IBM Security Identity Manager)

Le test Sécurité (console en libre service IBM Security Identity Manager) détermine si le serveur IBM Security Identity Manager est en cours d'exécution et si la console self-service est disponible.

## Ressources

Le test Sécurité (console en libre service IBM Security Identity Manager) utilise la ressource suivante :

- WebSphere Application Server nommé isim1.

## Identification des problèmes

Si le test Sécurité (console en libre service IBM Security Identity Manager) échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Si vous travaillez dans Field Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées. Pour *composant*, utilisez `isim` et indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.
  - a. Pour contrôler le statut du composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a status -c composant -p mot_de_passe_de_topologie
```
  - b. Pour démarrer le composant, exécutez les commandes suivantes :

```
su - ibmadmin

DOPControl -a start -c composant -p mot_de_passe_de_topologie
```
  - c. Pour arrêter le composant, exécutez les commandes suivantes :

```
su - ibmadmin
```

```
DOPControl -a stop -c composant -p mot_de_passe_de_topologie
```

2. Si vous travaillez dans Command Center Edition, utilisez l'outil de contrôle de la plateforme pour vérifier le statut des composants, les démarrer et les arrêter tel que nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.

- Pour vérifier le statut d'IBM Security Identity Manager, indiquez *status* pour *action* et *isim* pour *composant*.
- Pour arrêter IBM Security Identity Manager, indiquez *stop* pour *action* et *isim* pour *composant*.
- Pour démarrer IBM Security Identity Manager, indiquez *start* pour *action* et *isim* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

3. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'applications, consultez les journaux suivants de WebSphere Portal :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal/SystemErr.log
  - b. Dans Command Center Edition, sur le serveur d'applications 2, examinez les journaux WebSphere Portal suivants :
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal\_PortalNode2/SystemErr.log
  - c. Sur le serveur d'applications, examinez les journaux WebSphere Application Server suivants :
    - /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log
    - /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log
4. Vérifiez que le système de fichiers sur le serveur d'applications n'a pas atteint sa capacité maximale. Pour ce faire, exécutez la commande **df -h**. Le système de fichiers est considéré comme étant saturé même si moins de 100 % de sa capacité est utilisée. Ainsi, si la commande **df -h** renvoie un message indiquant que le système de fichiers est saturé à 90 % ou plus, vous devriez considérer que le système de fichiers a atteint sa capacité totale.
5. Vérifiez que le serveur *isim1* est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Voici les étapes manuelles :
  - a. Sur le système du serveur d'applications, connectez-vous en tant que *ibmadmin*.
  - b. Dans une fenêtre de commande, exécutez : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où *ADMIN\_WAS* est l'ID administrateur WebSphere (normalement *admin*) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere Application Server.
  - c. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'applications "nodeagent"`. Ce dernier est arrêté. s'affiche, démarrez le *nodeagent* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "nodeagent" est DEMARRE`. s'affiche. Si vous avez dû démarrer le *nodeagent*, un message similaire au suivant s'affiche : `ADMU3000I : nodeagent du serveur prêt pour e-business ; l'ID de processus est 26654`.
  - a. Si le message `ADMU0509I : Impossible d'atteindre le serveur d'application "isim1"`. Ce dernier est arrêté. s'affiche, démarrez le serveur *isim1* à l'aide de la commande suivante : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1`. Ignorez cette étape si le message `ADMU0508I : Le serveur d'applications "isim1" est DEMARRE`. s'affiche. Si vous avez dû démarrer *isim1*, un message similaire au suivant s'affiche : `ADMU3000I : serveur isim1 prêt pour e-business ; l'ID de processus est 26654`.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. isim1

Arrêtez les serveurs dans cet ordre :

- a. isim1
- b. nodeagent

Le serveur isim1 est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere Application Server.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username ADMIN_WAS -password MDP_ADMIN_WAS` où `ADMIN_WAS` est l'ID administrateur WebSphere (admin en règle générale) et `MDP_ADMIN_WAS` est le mot de passe de l'administrateur WebSphere.

6. Vérifiez que le serveur isim1 est démarré. La vérification peut être effectuée à l'aide de la console d'administration WebSphere Application Server ou en suivant des étapes manuelles. Les étapes suivantes utilisent la console d'administration de WebSphere Application Server :
  - a. Connectez-vous à la console d'administration de WebSphere Application Server à l'adresse `http://APPLICATION_SERVER_HOST:9061/ibm/console` en utilisant l'ID et le mot de passe de l'administrateur de WebSphere Application Server. `APPLICATION_SERVER_HOST` est le nom d'hôte du serveur d'applications.
  - b. Afficher le statut du serveur isim1 en cliquant sur **Serveurs > Types de serveur > Serveurs d'applications WebSphere**.
    - L'icône en forme de  indique que le serveur est démarré. Si nécessaire, sélectionnez le serveur et cliquez sur **Redémarrer** pour redémarrer le serveur.
    - L'icône en forme de  indique que le serveur est arrêté. Sélectionnez le serveur et cliquez sur **Démarrer** pour démarrer le serveur.
    - L'icône en forme de  indique que le statut du serveur est indisponible. Il se peut que l'agent de noeud ne soit pas en cours d'exécution. Pour démarrer le nodeagent, exécutez la commande `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` dans une fenêtre de commande.

**Important :** Les serveurs doivent être démarrés et arrêtés dans un ordre spécifique.

Démarrez les serveurs dans cet ordre :

- a. nodeagent
- b. isim1

Arrêtez les serveurs dans cet ordre :

- a. isim1
- b. nodeagent

Pour arrêter le serveur isim1, sélectionnez le serveur et cliquez sur **Arrêter**.

Le serveur nodeagent est arrêté par exécution de la commande suivante dans une fenêtre de commande sur le serveur d'applications : `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/`

stopNode.sh -username *ADMIN\_WAS* -password *MDP\_ADMIN\_WAS* où *ADMIN\_WAS* est l'ID administrateur WebSphere (admin en règle générale) et *MDP\_ADMIN\_WAS* est le mot de passe de l'administrateur WebSphere.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Sécurité (WebSEAL) [1]

Le test Sécurité (WebSEAL) [1] détermine le statut du serveur IBM Security Access Manager WebSEAL.

## Ressources

Le test Sécurité (WebSEAL) [1] utilise les ressources suivantes :

- IBM Security Access Manager sur le serveur d'application des règles.
- IBM Security Access Manager WebSEAL sur le serveur d'application des règles.

## Identification des problèmes

Si le test Sécurité (WebSEAL) [1] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur principal, indiquez *status* pour *action* et *websealpri* pour *composant*.
  - Pour contrôler le statut du serveur de secours, indiquez *status* pour *action* et *websealsby* pour *composant*.
  - Pour démarrer le serveur principal, indiquez *start* pour *action* et *websealpri* pour *composant*.
  - Pour démarrer le serveur de secours, indiquez *start* pour *action* et *websealsby* pour *composant*.
  - Pour arrêter le serveur principal, indiquez *stop* pour *action* et *websealpri* pour *composant*.
  - Pour arrêter le serveur de secours, indiquez *stop* pour *action* et *websealsby* pour *composant*.

Indiquez votre mot de passe de topologie pour *mot\_de\_passe\_de\_topologie*.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'application des règles, consultez les journaux de IBM Security Access Manager suivants :
    - /var/PolicyDirector/log/msg\_\_pdmgrd\_utf8.log
    - /var/PolicyDirector/log/msg\_\_pdacld\_utf8.log
  - b. Sur le serveur d'application des règles, consultez les journaux du IBM Security Access Manager suivants :
    - /var/ibm/tivoli/common/DPW/logs/msg\_\_webseald-default.log
    - /var/ibm/tivoli/common/DPW/logs/www-default/log/\*.log
3. Vérifiez que les composants IBM Security Access Manager WebSEAL requis sont en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - b. Exécutez la commande **pd\_start status**. Les résultats seront semblables à ce qui suit :

Security Access Manager servers

| Server      | Enabled | Running |
|-------------|---------|---------|
| pdmgrd      | yes     | yes     |
| pdacld      | yes     | yes     |
| pdmgrproxyd | no      | no      |

- c. Si les serveurs pdmgrd ou pdacld ne sont pas en cours d'exécution, démarrez-les en exécutant la commande **pd\_start start**.

**Remarque :** Seuls les serveurs pdmgrd et pdacld sont activés sur le serveur de surveillance. Les deux sont démarrés à l'aide de la commande **pd\_start start** et peuvent être arrêtés à l'aide de la commande **pd\_start stop**.

4. Vérifiez que les composants IBM Security Access Manager WebSEAL requis sont en cours d'exécution.
- a. Connectez-vous à une session de terminal sur le serveur d'application des règles 1 en tant que superutilisateur.
- b. Exécutez la commande **pd\_start status**. Les résultats seront semblables à ce qui suit :

Security Access Manager servers

| Server           | Enabled | Running |
|------------------|---------|---------|
| pdmgrd           | no      | no      |
| pdacld           | no      | no      |
| pdmgrproxyd      | no      | no      |
| webseald-default | yes     | yes     |

- c. Si le serveur default-webseald n'est pas en cours d'exécution, démarrez-le en exécutant la commande **pd\_start start**.

**Remarque :** Seul le serveur webseald-default est activé sur le serveur d'application des règles 1. Il est démarré à l'aide de la commande **pd\_start start** et peut être arrêté à l'aide de la commande **pd\_start stop**. Les serveurs sont : pdmgrd est le serveur de règles, pdacld est le serveur d'autorisation, pdmgrproxyd est le serveur proxy et webseald-default est le serveur WebSEAL. Le serveur IBM Security Access Manager WebSEAL est sur les serveurs serveur d'application des règles et les serveurs de règles et d'autorisation IBM Security Access Manager sont sur le serveur de surveillance.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

## Test Sécurité (WebSEAL) [2]

Le test Sécurité (WebSEAL) [2] détermine le statut du serveur IBM Security Access Manager WebSEAL.

## Ressources

Le test Sécurité (WebSEAL) [2] utilise les ressources suivantes :

- IBM Security Access Manager sur le serveur d'application des règles.
- IBM Security Access Manager WebSEAL sur le serveur d'application des règles.

## Identification des problèmes

Si le test Sécurité (WebSEAL) [2] échoue, procédez comme suit pour rechercher et résoudre le problème d'accès.

## Procédure

1. Utilisez l'outil de contrôle de plateforme pour vérifier le statut des composants et les démarrer et les arrêter si nécessaire. Exécutez la commande suivante en appliquant les options souhaitées.
  - Pour contrôler le statut du serveur principal, indiquez `status` pour *action* et `websealpri` pour *composant*.
  - Pour contrôler le statut du serveur de secours, indiquez `status` pour *action* et `websealsby` pour *composant*.
  - Pour démarrer le serveur principal, indiquez `start` pour *action* et `websealpri` pour *composant*.
  - Pour démarrer le serveur de secours, indiquez `start` pour *action* et `websealsby` pour *composant*.
  - Pour arrêter le serveur principal, indiquez `stop` pour *action* et `websealpri` pour *composant*.
  - Pour arrêter le serveur de secours, indiquez `stop` pour *action* et `websealsby` pour *composant*.

Indiquez votre mot de passe de topologie pour `mot_de_passe_de_topologie`.

```
su - ibmadmin
```

```
DOPControl -a action -c composant -p mot_de_passe_de_topologie
```

2. Recherchez les exceptions d'exécution dans les fichiers journaux.
  - a. Sur le serveur d'application des règles, consultez les journaux de IBM Security Access Manager suivants :
    - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
    - `/var/PolicyDirector/log/msg__pdaclد_utf8.log`
  - b. Sur le serveur d'application des règles, consultez les journaux du IBM Security Access Manager suivants :
    - `/var/ibm/tivoli/common/DPW/logs/msg__webseald-default.log`
    - `/var/ibm/tivoli/common/DPW/logs/www-default/log/*.log`
3. Vérifiez que les composants IBM Security Access Manager WebSEAL requis sont en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur de surveillance en tant que superutilisateur.
  - b. Exécutez la commande `pd_start status`. Les résultats seront semblables à ce qui suit :

```
Security Access Manager servers
```

| Server      | Enabled | Running |
|-------------|---------|---------|
| pdmgrd      | yes     | yes     |
| pdaclد      | yes     | yes     |
| pdmgrproxyd | no      | no      |
  - c. Si les serveurs `pdmgrd` ou `pdaclد` ne sont pas en cours d'exécution, démarrez-les en exécutant la commande `pd_start start`.

**Remarque :** Seuls les serveurs `pdmgrd` et `pdaclد` sont activés sur le serveur de surveillance. Les deux sont démarrés à l'aide de la commande `pd_start start` et peuvent être arrêtés à l'aide de la commande `pd_start stop`.

4. Vérifiez que les composants IBM Security Access Manager WebSEAL requis sont en cours d'exécution.
  - a. Connectez-vous à une session de terminal sur le serveur d'application des règles 2 en tant que superutilisateur.
  - b. Exécutez la commande `pd_start status`. Les résultats seront semblables à ce qui suit :

```
Security Access Manager servers
```

| Server | Enabled | Running |
|--------|---------|---------|
|--------|---------|---------|

|                  |     |     |
|------------------|-----|-----|
| pdmgrd           | no  | no  |
| pdacld           | no  | no  |
| pdmgrproxyd      | no  | no  |
| webseald-default | yes | yes |

- c. Si le serveur default-webseald n'est pas en cours d'exécution, démarrez-le en exécutant la commande **pd\_start start**.

**Remarque :** Seul le serveur webseald-default est activé sur le serveur d'application des règles 2. Il est démarré à l'aide de la commande **pd\_start start** et peut être arrêté à l'aide de la commande **pd\_start stop**. Les serveurs sont : pdmgrd est le serveur de règles, pdacld est le serveur d'autorisation, pdmgrproxyd est le serveur proxy et webseald-default est le serveur WebSEAL. Le serveur IBM Security Access Manager WebSEAL est sur les serveurs serveur d'application des règles et les serveurs de règles et d'autorisation IBM Security Access Manager sont sur le serveur de surveillance.

## Que faire ensuite

Résolvez les anomalies ou les erreurs trouvées et relancez le test.

---

## Consignation et analyse des données d'utilisation

IBM Defense Operations Platform consigne les données d'utilisation qui peuvent ensuite être traitées à l'aide d'une application d'analyse d'utilisation.

Ces journaux fournissent des informations sur les activités de session telles que les connexions, les déconnexions, les dépassements de délai d'attente et les échecs de connexion. Les entrées de journal sont conformes à la norme de l'industrie du format combiné NCSA.

En analysant les entrées de journal, vous pouvez surveiller l'utilisation d'IBM Defense Operations Platform.

## Journaux d'analyse d'utilisation

Des enregistrements d'utilisation d'IBM Defense Operations Platform sont écrits dans des fichiers journaux dédiés. WebSphere Portal est configuré pour effectuer un roulement des journaux toutes les six heures. L'intervalle de roulement peut être personnalisé.

Les journaux d'analyse d'utilisation se trouvent sur le serveur d'applications dans un environnement Field Edition et sur le serveur d'applications 1 et serveur d'applications 2 dans Command Center Edition. Ces journaux se trouvent dans le répertoire suivant :

```
wp_root/logs/wp_server_name/SiteAnalyzerLogs
```

où *wp\_root* est le répertoire de base de WebSphere Portal et *wp\_server\_name* est le nom du serveur WebSphere Portal.

Les fichiers journaux sont nommés en utilisant le format suivant : sa\_CREATE\_TIME\_CLOSE\_TIME.log où *CREATE\_TIME* est une valeur d'horodatage du moment où le journal a été créé et *CLOSE\_TIME* est un horodatage du moment où le journal a été fermé. Les horodatages de *CREATE\_TIME* et de *CLOSE\_TIME* sont au format AAAA.MM.JJ - hh.mm.ss, où AAAA est l'année, MM est le mois, JJ est le jour, hh représente l'heure, mm représente les minutes et ss représente les secondes.

La consignation doit être activée pour capturer les données d'analyse d'utilisation. La consignation est activée par défaut.

### Information associée:



Activation de la consignation de l'analyse de site dans WebSphere Portal

## Exécution de l'outil d'analyse d'utilisation

L'outil d'analyse d'utilisation traite les journaux d'analyse d'utilisation et enregistre les données pour les besoins de la génération de rapports en temps réel et de rapports de l'historique.

### Pourquoi et quand exécuter cette tâche

L'outil stocke les informations d'analyse suivantes dans la base de données USAGEAN, dans la table SCHUSAG.USAGEDATA. Les journaux traités sont stockés dans le répertoire/opt/IBM/WebSphere/usageAnalysis/Archive\_date\_heure , où date\_heure est l'horodatage du moment auquel l'outil a été exécuté.

- src\_ip - l'adresse IP source à l'origine de la demande d'URL de WebSphere Portal (req\_url).
- req\_user - l'utilisateur qui a demandé l'URL de WebSphere Portal (req\_url).
- req\_datetime - la date et l'heure auxquelles l'URL de WebSphere Portal (req\_url) a été demandée.
- req\_url - l'URL de WebSphere Portal qui a été demandée par l'utilisateur (req\_user).
- cookies - les cookies qui ont été transmis avec la demande d'URL de WebSphere Portal (req\_url).
- sa\_filename - le nom du fichier journal d'analyse d'utilisation traité.
- p\_server - le serveur WebSphere Portal à l'origine du fichier journal d'analyse d'utilisation (sa\_filename). Ces informations sont utiles pour les installations comportant plusieurs noeuds WebSphere Portal.
- created - la date et l'heure auxquelles l'entrée a été créée dans la base de données.

L'outil d'analyse d'utilisation peut être configuré en modifiant les propriétés suivantes dans le fichier /opt/IBM/WebSphere/usageAnalysis/runAnalysisTool.sh.

- IS\_DEBUG peut être défini sur yes ou no pour indiquer si les instructions de débogage sont affichées lors de l'exécution de l'outil d'analyse d'utilisation. La valeur par défaut est no, ce qui indique que les instructions de débogage ne sont pas affichées.
- IS\_FORCE peut être défini sur yes ou no pour indiquer si un fichier d'analyse d'utilisation traité précédemment doit être à nouveau traité. Lorsque la valeur est yes, les entrées existantes de la base de données sont supprimées et le journal est traité une nouvelle fois.

Pour exécuter l'outil d'analyse d'utilisation, procédez comme suit :

### Procédure

1. Dans Field Edition, connectez-vous au serveur/serveur d'applications en tant qu'utilisateuribmadmin. Dans Command Center Edition, connectez-vous au serveur/serveur d'applications 1 et serveur d'applications 2 successivement, et exécutez les étapes suivantes.
2. Accédez au répertoire *racine\_was/usageAnalysis*, où *racine\_was* est le répertoire de base de WebSphere Application Server. Par exemple, /opt/IBM/WebSphere/usageAnalysis.
3. Exécutez `./runAnalysisTool.sh -h nomhôte_serveur_basededonnées -p mdp_db2inst1`  
Où *nomhôte\_serveur\_basededonnées* est le nom d'hôte du serveur de données ou du serveur de données 1 et *mdp\_db2inst1* est le mot de passe défini par DEFAULT.PWD.DB2 dans le fichier de propriétés de topologie.

### Résultats

Les résultats de l'analyse sont écrits dans la base de données USAGEAN.

---

## Modification du mot de passe d'installation

Le mot de passe d'installation est utilisé pendant le processus d'installation pour chiffrer le fichier de définition de la topologie de la solution et pour y accéder. Le mot de passe est créé pendant le processus d'installation, au moment de la création d'un magasin de clés. En cas de besoin, le mot de passe peut être modifié. Dans ce cas, supprimez le magasin de clés et spécifiez un nouveau mot de passe d'installation.

### Pourquoi et quand exécuter cette tâche

Sur le serveur d'installation, accédez au répertoire dans lequel le module d'installation d'IBM Defense Operations Platform a été copié. Dans ces étapes, ce répertoire est appelé *racine\_install*.

### Procédure

1. Ouvrez une session en tant qu'utilisateur superutilisateur ou accédez au compte superutilisateur en exécutant la commande `su -`.
2. Accédez au répertoire `ép_principal_install/dop16`.
3. Supprimez le fichier `install_home/dop16/resource/ioc.keystore`.
4. Exécutez la commande `./dop.d2.install.sh 3 -p mot_de_passe_installation` pour Field Edition ou la commande `./dop.d1.install.sh 3 -p mot_de_passe_installation` pour Command Center Edition, où `mot_de_passe_installation` représente le mot de passe à créer pour l'installation.
5. Notez le mot de passe pour une utilisation future.

**Important :** Le mot de passe d'installation est nécessaire lorsque vous exécutez ou réexécutez le programme d'installation de ligne de commande. Le mot de passe d'installation d'origine est également utilisé comme mot de passe de topologie. Mais si vous modifiez le mot de passe d'installation via ce processus, cela ne modifie pas le mot de passe de topologie. Pour modifier le mot de passe de topologie, vous devez exécuter une autre procédure.

#### Tâches associées:

«Modification du mot de passe de topologie»

Le mot de passe de topologie est utilisé pour protéger les informations de mot de passe requises pour le fonctionnement et la maintenance d'IBM Defense Operations Platform. Ce mot de passe peut être modifié afin de respecter les conditions applicables au sein de l'entreprise.

---

## Modification du mot de passe de topologie

Le mot de passe de topologie est utilisé pour protéger les informations de mot de passe requises pour le fonctionnement et la maintenance d'IBM Defense Operations Platform. Ce mot de passe peut être modifié afin de respecter les conditions applicables au sein de l'entreprise.

### Pourquoi et quand exécuter cette tâche

Le outil de contrôle de plateforme utilise des mots de passe pour l'exécution des composants logiciels au sein de la topologie. Ces mots de passe sont protégés par IBM Defense Operations Platform grâce à un chiffrement qui s'appuie sur le mot de passe de topologie. Le mot de passe de topologie est utilisé pour le chiffrement et le déchiffrement des informations de mot de passe.

Le mot de passe de topologie initial est le mot de passe d'installation défini lors de l'installation d'IBM Defense Operations Platform. Le mot de passe de topologie peut être modifié, et le fichier correspondant peut être chiffré à l'aide du nouveau mot de passe.

### Procédure

1. Connectez-vous au serveur de messagerie (Field Edition) ou serveur de messagerie 1 (Command Center Edition) en tant qu'utilisateur `ibmadmin`.

2. Exécutez la commande suivante pour chiffrer les mots de passe protégés à l'aide d'un nouveau mot de passe de topologie.

```
iopmgmt-updatePCTpw.sh -p ancien_mot_de_passe_de_topologie -n nouveau_mot_de_passe_de_topologie
```

Où *ancien\_mot\_de\_passe\_de\_topologie* représente le mot de passe de topologie actuel et *nouveau\_mot\_de\_passe\_de\_topologie* le nouveau mot de passe de topologie. Si le mot de passe contient des caractères spéciaux, il doit être placé entre guillemets (par exemple : 'pass\_word').

## Résultats

Le fichier de propriétés de la topologie contenant les mots de passe utilisés par IBM Defense Operations Platform est chiffré à l'aide du nouveau mot de passe de topologie.

## Que faire ensuite

Utilisez le nouveau mot de passe de topologie lorsque vous exécutez l'outil de contrôle de plateforme (DOPControl).

### Tâches associées:

«Modification du mot de passe d'installation», à la page 190

Le mot de passe d'installation est utilisé pendant le processus d'installation pour chiffrer le fichier de définition de la topologie de la solution et pour y accéder. Le mot de passe est créé pendant le processus d'installation, au moment de la création d'un magasin de clés. En cas de besoin, le mot de passe peut être modifié. Dans ce cas, supprimez le magasin de clés et spécifiez un nouveau mot de passe d'installation.

---

## Mise à jour du jeton LTPA pour la connexion unique

IBM Defense Operations Platform utilise un jeton LTPA (Lightweight Third-Party Authentication) pour activer la connexion unique sur plusieurs services. Le jeton et les clés générés au cours de l'installation n'expirent pas. Dans une optique de sécurité, il est recommandé de régénérer régulièrement le jeton LTPA et de mettre à jour les services qui l'utilisent.

## Avant de commencer

Le produit IBM Defense Operations Platform doit être installé et tous les services démarrés avant de mettre à jour le jeton LTPA.

Cette procédure exige que tous les services soient arrêtés et démarrés. Par conséquent, n'effectuez pas la mise à jour lorsque le système est en production. Une interruption de service pourrait se produire et tous les utilisateurs connectés au système risqueraient de perdre des données.

## Procédure

Générez un nouveau jeton LTPA pour le serveur d'applications.

1. Dans Field Edition, sur le serveur d'applications, ouvrez un navigateur Web et accédez à `http://hôte_application:9062/ibm/console`, où *hôte\_application* représente le nom d'hôte du serveur d'applications.
2. Dans Command Center Edition, sur le serveur d'applications 1, ouvrez un navigateur Web et accédez à `http://hôte_application:9062/ibm/console`, où *hôte\_application* représente le nom d'hôte du serveur d'applications 1.
3. Connectez-vous en tant qu'utilisateur admin avec le mot de passe indiqué pour le paramètre WAS.ADMIN.ACCOUNT.PWD dans le fichier de propriétés de la topologie.
4. Cliquez sur **Sécurité** > **Sécurité globale** > **LTPA**.

5. Entrez un mot de passe deux fois pour le nouveau jeton LTPA. Le mot de passe est utilisé pour chiffrer le jeton LTPA. Il sera utilisé lors de l'importation du jeton LTPA. Enregistrez-le en tant que paramètre `WAS.LTPA.PWD` dans le fichier de propriétés de la topologie.
  6. Entrez le chemin et le nom du fichier dans lesquels le jeton LTPA sera sauvegardé, par exemple, `/tmp/newapp.ltpa`. Si vous spécifiez un chemin ou un nom de fichier différent, utilisez-les pour `/tmp/newapp.ltpa` dans la suite de ces étapes.
  7. Cliquez sur **Exporter les clés**. Le nouveau jeton LTPA est sauvegardé dans le fichier `/tmp/newapp.ltpa`.
  8. Cliquez sur **Messages > Sauvegarder**. Les mises à jour sont sauvegardées. Ignorez les avertissements signalant que le domaine de connexion unique n'est pas défini.
  9. Sur le serveur d'applications, connectez-vous en tant qu'utilisateur root et ouvrez une fenêtre de terminal.
  10. Exécutez la commande `cp /tmp/newapp.ltpa /opt/IBM/ISP/stproxy.ltpa`. Le fichier que vous avez créé lors de l'installation d'IBM Defense Operations Platform est remplacé.
- Mise à jour de la connexion unique pour le service de collaboration.
11. Suivez la procédure décrite dans le chapitre «Configuration de la connexion unique pour les services de collaboration», à la page 48 afin de mettre à jour la connexion unique pour le service de collaboration.
- Arrêtez puis redémarrez tous les services.
12. Utilisez l'outil de contrôle de plateforme pour arrêter tous les services.
  13. Utilisez l'outil de contrôle de plateforme pour démarrer tous les services. Des jetons LTPA seront propagés entre WebSphere Application Server et le serveur Lotus Domino.

---

## Définition du délai d'expiration de session

Le délai d'expiration de session détermine la durée pendant laquelle un utilisateur peut rester inactif avant que la session ne soit fermée et que l'utilisateur n'ait à se reconnecter. Ce délai d'attente s'applique également aux administrateurs qui sont connectés via le service de portail.

### Pourquoi et quand exécuter cette tâche

Au moment de l'installation d'IBM Defense Operations Platform, aucun délai d'expiration de session n'est défini. Les utilisateurs restent connectés jusqu'à ce qu'ils décident de se déconnecter, même si la session est inactive.

Si votre organisation a mis en place des règles de sécurité imposant des délais d'expiration de session après une période d'inactivité, utilisez la procédure suivante afin de définir des délais d'expiration de session personnalisés pour votre système IBM Defense Operations Platform.

### Procédure

Configurez les délais d'attente des serveurs.

1. Sur le Field Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications.
2. Sur le Command Center Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications 1.
3. Connectez-vous en tant qu'utilisateur admin avec le mot de passe défini pour `PORTAL.ADMIN.ACCOUNT.PWD` dans le fichier de propriétés de la topologie.
4. Cliquez sur **Serveurs > Type de serveur > WebSphere Application Servers > WebSphere Portal**.
5. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
6. Entrez la valeur de délai d'attente en minutes.

7. Cliquez sur **OK**.
  8. Cliquez sur **Sauvegarder**.
  9. Cliquez sur **Serveurs > Type de serveur > Serveurs d'applications WebSphere > STProxyServer1**.
  10. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
  11. Entrez la valeur de délai d'attente en minutes.
  12. Cliquez sur **OK**.
  13. Cliquez sur **Sauvegarder**.
- Dans Command Center Edition, configurez les serveurs supplémentaires suivants.
14. Cliquez sur **Serveurs > Type de serveur > WebSphere Application Servers > WebSphere\_Portal\_PortalNode2**.
  15. Cliquez sur **Paramètres du conteneur > Gestion de session > Définir le délai d'expiration**.
  16. Entrez la valeur de délai d'attente en minutes.
  17. Cliquez sur **OK**.
  18. Cliquez sur **Sauvegarder**.
- Redémarrez le serveur.
19. Arrêtez et redémarrez le serveur d'applications dans Field Edition ou serveur d'applications 1 dans Command Center Edition à l'aide de l'outil de contrôle de plateforme.

---

## Définition du délai d'expiration de LTPA

Le délai d'expiration de LTPA (Lightweight Third-Party Authentication) détermine la durée pendant laquelle un utilisateur peut rester connecté avant que la session soit fermée et que l'utilisateur ait à se reconnecter. Ce délai d'attente s'applique également aux administrateurs connectés via le service de portail.

### Pourquoi et quand exécuter cette tâche

Une fois IBM Defense Operations Platform installé, un délai d'attente LTPA de 150 minutes est configuré. Les utilisateurs restent connectés jusqu'à ce qu'ils décident de se déconnecter une fois les 150 minutes passées.

Si votre organisation a mis en place des règles de sécurité imposant un arrêt des sessions après une période différente, utilisez la procédure suivante afin de définir des délais d'expiration LTPA pour votre système IBM Defense Operations Platform.

### Procédure

1. Sur le Field Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications.
2. Sur le Command Center Edition, ouvrez un navigateur Web et accédez à `http://serveur_applications:9062/ibm/console`, où `serveur_applications` représente le nom d'hôte du serveur d'applications 1.
3. Connectez-vous en tant qu'utilisateur admin avec le mot de passe défini pour `PORTAL.ADMIN.ACCOUNT.PWD` dans le fichier de propriétés de la topologie.
4. Cliquez sur **Sécurité > Sécurité globale > LTPA**.
5. Entrez la valeur désirée de **délai d'attente LPTA** en minutes.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Sauvegarder**.
8. Arrêtez et redémarrez tous les composants IBM Defense Operations Platform avec l'outil de contrôle de plateforme. Si IBM Defense Operations Platform est toujours en cours d'installation, les serveurs seront relancés pendant la vérification intégrale de l'installation.



---

## Chapitre 4. Traitement des incidents et support

Pour traiter les incidents liés à vos logiciels IBM, vous pouvez utiliser les informations de dépannage et de support qui contiennent des instructions sur l'utilisation des ressources d'identification de problème fournies avec les produits IBM.

---

### Echec du lancement d'IBM Installation Manager

Echec du lancement du programme d'installation ; des messages s'affichent, indiquant la présence d'une exception de point flottant et de cliché du processus core.

#### Symptômes

Des messages similaires au message suivant sont renvoyés lors de l'exécution du programme d'installation.

```
(Launcher:2554): Glib-GObject-WARNING **: invalid (NULL) pointer instance
(Launcher:2554): Glib-GObject-CRITICAL **: g_signal_connect_data: assertion `G_TYPE_CHECK_INSTANCE (instance)' failed
(Launcher:2554): Pango-CRITICAL **: pango_layout_get_line_count: assertion `layout != NULL' failed
Floating point exception (core dumped)
```

#### Résolution du problème

Les mises à jour WebSphere Application Server et WebSphere Portal installées par IBM Installation Manager doivent être exécutées en tant qu'utilisateur `ibmadmin`. Les erreurs de lancement du programme d'installation peuvent être liées au fait qu'IBM Installation Manager a déjà été exécuté précédemment en tant qu'utilisateur `root`. Les fichiers requis sont verrouillés et appartiennent à l'utilisateur `root` ; l'utilisateur `ibmadmin` ne peut pas y accéder. Pour résoudre le problème, procédez comme suit :

1. Sur le serveur d'applications sur lequel le composant WebSphere Application Server or WebSphere Portal nécessite des mises à jour, ouvrez une session et connectez-vous en tant qu'utilisateur `root`.
2. Exécutez les commandes suivantes :

```
chown -R ibmadmin:ibmadmins /opt/IBM/InstallationManager
su - ibmadmin
cd /opt/IBM/InstallationManager/eclipse
./launcher
```
3. IBM Installation Manager devrait maintenant fonctionner correctement.

---

### Les composants WebSphere ne démarrent pas

outil de contrôle de plateforme (DOPControl) ne parvient pas à démarrer WebSphere Application Server Network Deployment, l'agent de noeud WebSphere ou WebSphere Application Server.

#### Symptômes

outil de contrôle de plateforme (DOPControl) indique qu'un ou plusieurs composants WebSphere n'ont pas pu être démarrés et que le fichier WebSphere `startServer.log` contient un message identique au message suivant :

```
[MM/DD/YY HH:MM:SS:nnn XXX] 00000000 AdminTool A ADMU3011E: Server launched but failed
initialization. Server logs, startServer.log, and other log files under
/opt/IBM/...../logs/..... should contain failure information.
```

## Résolution du problème

Les composants WebSphere Application Server doivent être démarrés via l'outil de contrôle de plateforme (DOPControl) exécuté en tant qu'utilisateur `ibmadmin`. Les erreurs de démarrage de composants peuvent avoir pour origine une exécution antérieure des commandes de démarrage en tant qu'utilisateur `root`. Dans ce cas, les fichiers requis sont verrouillés et appartiennent à l'utilisateur `root` ; l'utilisateur `ibmadmin` ne peut donc pas y accéder. Pour résoudre ce problème, procédez comme suit :

1. Sur le serveur sur lequel le composant WebSphere Application Server n'a pas pu être démarré, ouvrez une session et connectez-vous en tant qu'utilisateur `root`.
2. Exécutez la commande suivante :  

```
chown -R ibmadmin:ibmadmins repertoire_profil_websphere
```

Où le tableau 22 spécifie la valeur de `repertoire_profil_websphere` en fonction du composant DOPControl qui n'a pas pu être démarré.

Tableau 22. Valeur de `repertoire_profil_websphere` spécifiée en fonction du composant DOPControl qui n'a pas pu être démarré

| Valeur <code>repertoire_profil_websphere</code>                    | Composants DOPControl Command Center Edition | Composants DOPControl Field Edition |
|--------------------------------------------------------------------|----------------------------------------------|-------------------------------------|
| <code>/opt/IBM/WebSphere/AppServer/profiles/dmgr</code>            | <code>appdmgrpri</code>                      | <code>appdmgr</code>                |
| <code>/opt/IBM/WebSphere/AppServer/profiles/IopProfile1</code>     | <code>ioppri</code>                          | <code>iop</code>                    |
| <code>/opt/IBM/WebSphere/AppServer/profiles/IopProfile2</code>     | <code>iopsby</code>                          | Non applicable                      |
| <code>/opt/IBM/WebSphere/wp_profile</code>                         | <code>wpepri, wpesby</code>                  | <code>wpe</code>                    |
| <code>/opt/IBM/WebSphere/AppServer7/profiles/isim1</code>          | <code>isimpri</code>                         | <code>isim</code>                   |
| <code>/opt/IBM/WebSphere/AppServer7/profiles/STPAppProfile1</code> | <code>stproxypri</code>                      | <code>stproxy</code>                |
| <code>/opt/IBM/WebSphere/AppServer/profiles/bmpProfile1</code>     | <code>bpmpri</code>                          | Non applicable                      |
| <code>/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1</code>    | <code>wsrrpri</code>                         | Non applicable                      |
| <code>/opt/IBM/WebSphere/AppServer85/profiles/dmgr</code>          | <code>prodmgmpri</code>                      | Non applicable                      |
| <code>/opt/IBM/WebSphere/AppServer85/profiles/odmcdProfile1</code> | <code>odmcdpri</code>                        | Non applicable                      |
| <code>/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1</code>   | <code>odmpri</code>                          | Non applicable                      |

3. Exécutez l'outil de contrôle de plateforme (DOPControl) en tant qu'utilisateur `ibmadmin` afin de démarrer le composant qui n'avait pas pu être démarré précédemment.

---

## Impossible de démarrer le serveur LDAP à l'aide de Tivoli Directory Server Web Administration Tool

Lorsque vous essayez de démarrer le serveur LDAP à l'aide de l'outil de contrôle de plateforme (DOPControl) en tant qu'utilisateur `ibmadmin`, une erreur HTTP 500 est renvoyée et le serveur LDAP ne démarre pas.

## Résolution du problème

Démarrez Tivoli Directory Server à l'aide de l'outil de contrôle de plateforme.

### Concepts associés:

«Démarrage, arrêt et interrogation du statut dans Field Edition», à la page 57  
l'outil de contrôle de plateforme permet à un utilisateur d'arrêter, de démarrer et d'interroger les composants IBM Defense Operations Platform qui s'exécutent dans Field Edition. Un outil de contrôle de plateforme est également disponible pour IBM Defense Operations Platform s'exécutant dans Command Center Edition.

«Démarrage, arrêt, gestion et interrogation du statut dans Command Center Edition», à la page 62  
outil de contrôle de plateforme permet à un utilisateur d'arrêter, de démarrer et d'interroger les services  
IBM Defense Operations Platform qui s'exécutent dans Command Center Edition. Un outil outil de  
contrôle de plateforme est également disponible pour IBM Defense Operations Platform s'exécutant dans  
Field Edition.



## Chapitre 5. Référence

Il est important de comprendre la configuration du système IBM Defense Operations Platform installé. Ces références vous aident à comprendre les produits installés, les ports utilisés, les processus qui nécessitent des droits d'accès d'utilisateur root et les fonctions d'accessibilité. Sont également incluses des références juridiques supplémentaires.

### Produits et composants installés avec IBM Defense Operations Platform Field Edition

La solution IBM Defense Operations Platform installe un certain nombre de produits et de composants logiciels pour la Field Edition.

Les produits et composants logiciels, ainsi que les serveurs sur lesquels ils sont installés dans un environnement à haute disponibilité, sont présentés dans le tableau 23.

Tableau 23. Produits installés avec IBM Defense Operations Platform

| Produit                                                                                             | Serveur d'applications          | Serveur de messagerie           | Serveur de données                                                                                            |
|-----------------------------------------------------------------------------------------------------|---------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| Tivoli Directory Server 6.3.0.18                                                                    | non installé                    | non installé                    | installé                                                                                                      |
| Tivoli Directory Server Application Web 6.3.0.18                                                    | installé                        | non installé                    | non installé                                                                                                  |
| DB2 Enterprise Server Edition 10.1.0.1                                                              | non installé                    | non installé                    | installé                                                                                                      |
| DB2 10.1.0.1 Client                                                                                 | installé                        | non installé                    | non installé                                                                                                  |
| Tivoli Directory Integrator 7.1.1.2                                                                 | fonctions de plug-in installées | fonctions de plug-in installées | installé                                                                                                      |
| Tivoli Directory Integrator Dispatcher 6.0.6                                                        | non installé                    | non installé                    | installé                                                                                                      |
| Tivoli Directory Integrator Adaptateur POSIX 6.0.24                                                 | non installé                    | non installé                    | installé                                                                                                      |
| IBM Installation Manager 1.6.0                                                                      | installé                        | non installé                    | installé (facultatif)                                                                                         |
| WebSphere Application Server 7.0.0.29                                                               | installé                        | non installé                    | non installé                                                                                                  |
| WebSphere Application Server Network Deployment 8.0.0.7                                             | installé                        | non installé                    | non installé                                                                                                  |
| WebSphere Application Server 1.1.0.3 Feature Pack for Web 2.0 and Mobile                            | installé                        | non installé                    | non installé                                                                                                  |
| WebSphere Portal 8.0.0.1.CF05                                                                       | installé                        | non installé                    | non installé                                                                                                  |
| IBM HTTP Server 8.0.0.7                                                                             | installé                        | non installé                    | non installé                                                                                                  |
| WebSphere MQ7.5                                                                                     | non installé                    | installé                        | non installé                                                                                                  |
| WebSphere Message Broker 8.0.0.1                                                                    | non installé                    | installé                        | non installé                                                                                                  |
| IBM Java 1.7.0 SR5                                                                                  | non installé                    | installé                        | non installé                                                                                                  |
| Lotus Domino 8.5.3 (pack de mise à niveau 1)                                                        | installé                        | non installé                    | non installé                                                                                                  |
| Lotus Sametime Entry 8.5.2.1                                                                        | installé                        | non installé                    | non installé                                                                                                  |
| IBM Worklight Consumer Edition 6.0.0 (disponible en option via les services IBM Industry Solutions) | installé                        | non installé                    | non installé                                                                                                  |
| Lotus Sametime Proxy 8.5.2                                                                          | installé                        | non installé                    | non installé                                                                                                  |
| IBM Security Identity Manager 6.0                                                                   | installé                        | non installé                    | non installé                                                                                                  |
| Data Studio 3.2.0 (composant facultatif)                                                            | non installé                    | non installé                    | Remarque : IBM Installation Manager 1.6.0 sera également installé sur ce serveur si Data Studio est installé. |

### Produits et composants installés avec IBM Defense Operations Platform Command Center Edition

La solution IBM Defense Operations Platform installe un certain nombre de produits et de composants logiciels pour la Command Center Edition.

Les produits et composants logiciels, ainsi que les serveurs sur lesquels ils sont installés dans un environnement à haute disponibilité, sont présentés dans le tableau 24.

Tableau 24. Produits installés avec IBM Defense Operations Platform

| Produit                          | Serveur d'applications 1 | Serveur d'applications 2 | Serveur de messagerie 1 | Serveur de messagerie 2 | Serveur de données 1 | Serveur de données 2 | Serveur d'application des règles 1 | Serveur d'application des règles 2 | Serveur de surveillance | Serveur de processus |
|----------------------------------|--------------------------|--------------------------|-------------------------|-------------------------|----------------------|----------------------|------------------------------------|------------------------------------|-------------------------|----------------------|
| Tivoli Directory Server 6.3.0.18 | non installé             | non installé             | non installé            | non installé            | installé             | installé             | non installé                       | non installé                       | non installé            | non installé         |

Tableau 24. Produits installés avec IBM Defense Operations Platform (suite)

| Produit                                                                                             | Serveur d'applications 1        | Serveur d'applications 2        | Serveur de messagerie 1         | Serveur de messagerie 2         | Serveur de données 1                                                                                          | Serveur de données 2                                                                                          | Serveur d'application des règles 1 | Serveur d'application des règles 2 | Serveur de surveillance         | Serveur de processus            |
|-----------------------------------------------------------------------------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------|---------------------------------|---------------------------------|
| Tivoli Directory Server Proxy 6.3.0.18                                                              | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Tivoli Directory Server Application Web 6.3.0.18                                                    | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| DB2 Enterprise Server Edition 10.1.0.1                                                              | non installé                    | non installé                    | non installé                    | non installé                    | installé                                                                                                      | installé                                                                                                      | non installé                       | non installé                       | installé                        | non installé                    |
| DB2 10.1.0.1 Client                                                                                 | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Tivoli Directory Integrator 7.1.1.2                                                                 | fonctions de plug-in installées | toutes les fonctions installées                                                                               | fonctions de plug-in installées                                                                               | fonctions de plug-in installées    | fonctions de plug-in installées    | fonctions de plug-in installées | fonctions de plug-in installées |
| Tivoli Directory Integrator Dispatcher 6.0.6                                                        | non installé                    | non installé                    | non installé                    | non installé                    | installé                                                                                                      | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Tivoli Directory Integrator Adaptateur POSIX 6.0.24                                                 | non installé                    | non installé                    | non installé                    | non installé                    | installé                                                                                                      | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM Installation Manager 1.6.0                                                                      | installé                        | installé                        | non installé                    | non installé                    | installé (facultatif)                                                                                         | installé (facultatif)                                                                                         | non installé                       | non installé                       | non installé                    | installé                        |
| WebSphere Application Server 7.0.0.29                                                               | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| WebSphere Application Server 8.5.5                                                                  | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | installé                        |
| WebSphere Application Server Network Deployment 8.0.0.7                                             | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | installé                        |
| WebSphere Application Server 1.1.0.3 Feature Pack for Web 2.0 and Mobile                            | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | installé                        |
| WebSphere Portal 8.0.0.1.CF05                                                                       | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM Security Access Manager Web Portal Manager 7.0.0.1                                              | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM HTTP Server 8.0.0.7                                                                             | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | installé                        |
| WebSphere MQ7.5                                                                                     | non installé                    | non installé                    | installé                        | installé                        | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| WebSphere MQ Explorer 7.5                                                                           | non installé                    | non installé                    | installé                        | installé                        | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| WebSphere Message Broker 8.0.0.1                                                                    | non installé                    | non installé                    | installé                        | installé                        | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM Java 1.7.0 SR5                                                                                  | non installé                    | non installé                    | installé                        | installé                        | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Lotus Domino 8.5.3 FP1                                                                              | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Lotus Sametime Entry 8.5.2.1                                                                        | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM Worklight Consumer Edition 6.0.0 (disponible en option via les services IBM Industry Solutions) | installé                        | installé                        | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Lotus Sametime Proxy 8.5.2                                                                          | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| IBM Security Identity Manager 6.0                                                                   | installé                        | non installé                    | non installé                    | non installé                    | non installé                                                                                                  | non installé                                                                                                  | non installé                       | non installé                       | non installé                    | non installé                    |
| Data Studio 3.2.0 (composant facultatif)                                                            | non installé                    | non installé                    | non installé                    | non installé                    | Remarque : IBM Installation Manager 1.6.0 sera également installé sur ce serveur si Data Studio est installé. | Remarque : IBM Installation Manager 1.6.0 sera également installé sur ce serveur si Data Studio est installé. | non installé                       | non installé                       | non installé                    | non installé                    |
| Tivoli Access Manager WebSEAL 7.0.0.1                                                               | non installé                                                                                                  | non installé                                                                                                  | installé                           | installé                           | non installé                    | non installé                    |

Tableau 24. Produits installés avec IBM Defense Operations Platform (suite)

| Produit                                           | Serveur d'applications 1 | Serveur d'applications 2 | Serveur de messagerie 1 | Serveur de messagerie 2 | Serveur de données 1 | Serveur de données 2 | Serveur d'application des règles 1 | Serveur d'application des règles 2 | Serveur de surveillance | Serveur de processus |
|---------------------------------------------------|--------------------------|--------------------------|-------------------------|-------------------------|----------------------|----------------------|------------------------------------|------------------------------------|-------------------------|----------------------|
| Tivoli Netcool/OMNIBus 7.4.0.2                    | non installé             | non installé             | non installé            | non installé            | non installé         | non installé         | non installé                       | non installé                       | installé                | non installé         |
| IBM Security Access Manager 7.0.0.1               | non installé             | non installé             | non installé            | non installé            | non installé         | non installé         | non installé                       | non installé                       | installé                | non installé         |
| Tivoli Application Performance Manager 7.6.0.1    | agents uniquement        | agents uniquement        | agents uniquement       | agents uniquement       | agents uniquement    | agents uniquement    | agents uniquement                  | agents uniquement                  | installé                | agents uniquement    |
| WebSphere Service Registry and Repository 8.0.0.2 | non installé             | non installé             | non installé            | non installé            | non installé         | non installé         | non installé                       | non installé                       | non installé            | installé             |
| WebSphere Operational Decision Management 8.5     | non installé             | non installé             | non installé            | non installé            | non installé         | non installé         | non installé                       | non installé                       | non installé            | installé             |
| WebSphere Business Process Management 8.0.1.1     | non installé             | non installé             | non installé            | non installé            | non installé         | non installé         | non installé                       | non installé                       | non installé            | installé             |

## Ports utilisés par les serveurs Command Center Edition

IBM Defense Operations Platform Command Center Edition utilise des ports spécifiques.

Les ports utilisés par Command Center Edition sont affichés dans le tableau 25.

Tableau 25. Ports utilisés par Command Center Edition

| Serveur                            | Ports requis pour l'utilisation du produit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serveur d'applications 1           | 80, 84, 389, 443, 1352, 1516, 1533, 1920, 1976, 2810, 2811, 2812, 2813, 2814, 3538, 3661, 5000, 5001, 5002, 5003, 5004, 5005, 6014, 7272, 7273, 7274, 7756, 7278, 7287, 8008, 8082, 8878, 8879, 8881, 8883, 8884, 8885, 8886, 9044, 9045, 9047, 9061, 9062, 9064, 9081, 9082, 9083, 9092, 9094, 9101, 9102, 9104, 9105, 9201, 9202, 9203, 9204, 9205, 9206, 9352, 9355, 9356, 9357, 9358, 9359, 9404, 9405, 9407, 9409, 9414, 9415, 9416, 9417, 9444, 9445, 9446, 9629, 9630, 9631, 9632, 9634, 9636, 9637, 9809, 9811, 9900, 9902, 9904, 10025, 10029, 10030, 10033, 10034, 10035, 10036, 10037, 10039, 10110, 14206, 18302, 20831, 20832, 60148 |
| Serveur d'applications 2           | 80, 443, 1920, 2809, 2810, 3661, 5000, 5001, 5002, 5003, 6014, 7272, 8008, 8878, 8879, 8885, 9048, 9083, 9105, 9201, 9202, 9203, 9204, 9353, 9354, 9359, 9446, 9629, 9630, 9637, 9812, 9900, 9902, 10043, 10044, 10045, 10047, 10048, 10050, 10051, 10053, 10056, 10110, 14206                                                                                                                                                                                                                                                                                                                                                                    |
| Serveur de données 1               | 389, 523, 1098, 1099, 1920, 3538, 3661, 3766, 6014, 7756, 10110, 11852, 14206, 15948, 18001, 50001, 50002, 55002, 55003, 55044, 55005, 55006, 55007, 55013, 55014, 55015, 55016, 55017, 55018, 55019, 55020, 55021, 55022, 55023, 55024, 55025                                                                                                                                                                                                                                                                                                                                                                                                    |
| Serveur de données 2               | 389, 523, 1098, 1099, 1920, 3538, 3661, 3766, 6014, 7756, 10110, 11852, 14206, 15948, 18001, 50001, 50002, 55002, 55003, 55044, 55005, 55006, 55007, 55013, 55014, 55015, 55016, 55017, 55018, 55019, 55020, 55021, 55022, 55023, 55024, 55025                                                                                                                                                                                                                                                                                                                                                                                                    |
| Serveur de messagerie 1            | 1920, 3661, 4414, 6014, 10110, 14206                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Serveur de messagerie 2            | 1920, 3661, 4414, 6014, 10110, 14206                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Serveur d'application des règles 1 | 80, 443, 1920, 3661, 6014, 7234, 7756                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Serveur d'application des règles 2 | 80, 443, 1920, 3661, 6014, 7234, 7756                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Serveur de surveillance            | 523, 1918, 1920, 3660, 3661, 4100, 4200, 6014, 7135, 7136, 7137, 7756, 9998, 9999, 10110, 11852, 14206, 15001, 15200, 15201, 15202, 15203, 15204, 15205, 15206, 15207, 15208, 15210, 15211, 15214, 15948, 20044, 50001                                                                                                                                                                                                                                                                                                                                                                                                                            |

Tableau 25. Ports utilisés par Command Center Edition (suite)

| Serveur              | Ports requis pour l'utilisation du produit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serveur de processus | 80, 443, 1920, 2809, 2810, 2811, 2812, 2815, 3661, 5000, 5001, 5002, 5003, 5004, 5005, 5006, 5007, 6014, 7060, 7062, 7063, 7272, 7273, 7274, 7275, 7277, 7756, 7282, 7283, 7290, 7291, 8008, 8878, 8879, 8880, 8881, 8882, 8883, 8884, 8887, 8888, 9043, 9044, 9045, 9049, 9050, 9060, 9061, 9062, 9066, 9067, 9080, 9081, 9084, 9085, 9100, 9101, 9102, 9106, 9107, 9201, 9202, 9203, 9204, 9205, 9206, 9207, 9208, 9352, 9353, 9354, 9355, 9356, 9357, 9358, 9361, 9362, 9402, 9403, 9405, 9406, 9408, 9409, 9420, 9421, 9423, 9424, 9425, 9443, 9444, 9447, 9448, 9629, 9630, 9631, 9632, 9633, 9634, 9635, 9638, 9639, 9809, 9810, 9811, 9812, 9900, 9902, 9904, 9906, 10110, 11003, 11004, 11005, 11006, 11007, 11008, 11009, 11010, 11011, 11012, 11852, 14206, 15948 |

## Ports utilisés par les serveurs Field Edition

IBM Defense Operations Platform Field Edition utilise des ports spécifiques.

Les ports utilisés par Field Edition sont affichés dans le tableau 26.

Tableau 26. Ports utilisés par Field Edition

| Serveur                | Ports requis pour l'utilisation du produit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serveur d'applications | 80, 84, 443, 1352, 1516, 1533, 2810, 2811, 2812, 2813, 2814, 5000, 5001, 5002, 5003, 5004, 5005, 7272, 7273, 7274, 7278, 7287, 8082, 8878, 8879, 8881, 8883, 8884, 8885, 8886, 9044, 9045, 9047, 9061, 9062, 9064, 9081, 9082, 9083, 9092, 9094, 9100, 9101, 9102, 9104, 9105, 9201, 9202, 9203, 9204, 9205, 9206, 9352, 9355, 9356, 9357, 9358, 9359, 9404, 9407, 9409, 9414, 9415, 9416, 9417, 9444, 9445, 9446, 9629, 9630, 9631, 9632, 9634, 9636, 9637, 9809, 9811, 9900, 9902, 9904, 10025, 10029, 10030, 10033, 10034, 10035, 10036, 10037, 10039, 10788, 20831, 20832, 60148 |
| Serveur de données     | 389, 523, 3538, 3766, 18001, 50001, 50002                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Serveur de messagerie  | 4414                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Processus en cours d'exécution dans le compte superutilisateur

Une fois l'installation terminée, certains processus doivent toujours s'exécuter avec le compte root.

Les processus qui s'exécutent avec le compte superutilisateur peuvent être vulnérables si un utilisateur ou un processus peut obtenir des privilèges de superutilisateur via l'escalade de privilèges. Ce n'est normalement un problème que pour les demandes d'utilisateur de traitement de services. Les demandes d'utilisateur peuvent être des entrées configurées de façon malhonnête susceptibles de compromettre le serveur. Les demandes d'utilisateur de traitement de services sont des systèmes fournissant des interfaces utilisateur ou des API (interfaces de programme d'application).

Les démons Linux ne courent normalement aucun risque car, généralement, ils se contentent de démarrer, de s'arrêter ou de répondre à des événements système bien définis. Dans de nombreux cas, ces démons doivent s'exécuter avec le compte superutilisateur afin de pouvoir contrôler d'autres processus ou de répondre à des événements système critique. Tant qu'un serveur auquel un utilisateur a accès ne s'exécute pas avec le compte superutilisateur, les démons qui s'exécutent avec le compte superutilisateur ne présentent pas un risque aussi important.

Le tableau 27, à la page 203 répertorie les processus qui continuent à s'exécuter avec le compte superutilisateur une fois l'installation terminée.

Tableau 27. Processus de l'environnement IBM Defense Operations Platform qui s'exécutent avec un compte superutilisateur

| Serveur                                                                                              | Produit                     | Nom de processus                                                                                                                                     | Explication                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| serveur de données                                                                                   | DB2                         | db2wdog                                                                                                                                              | Ce processus démon reçoit des événements système et les propage à plusieurs processus enfant. Le processus db2wdog gère les processus db2sync et nécessite une gestion au niveau superutilisateur.                                                                                                                                                                                                                                         |
| serveur de données                                                                                   | DB2                         | db2chkpwd                                                                                                                                            | Ce démon authentifie l'ID et le mot de passe de l'utilisateur ou de l'application qui se connecte à une base de données. Le processus db2chkpwd doit lire le fichier de mots de passe /etc/shadow.                                                                                                                                                                                                                                         |
| serveur de données                                                                                   | DB2                         | /opt/IBM/DB2/bin/db2fmcd                                                                                                                             | Ce démon sert de coordinateur de moniteur d'erreur. Il doit s'exécuter avec le compte superutilisateur pour surveiller toutes les instances DB2.                                                                                                                                                                                                                                                                                           |
| serveur de données                                                                                   | DB2                         | /usr/sbin/rcst/bin/rmcd et /usr/sbin/rcst/bin/IBM.ConfigRMd                                                                                          | Ces commandes gèrent la solution à haute disponibilité pour DB2. Elles doivent accéder à toutes les bases de données des serveurs configurés pour la haute disponibilité.                                                                                                                                                                                                                                                                  |
| serveur de données                                                                                   | DB2                         | /sbin/srcmstr                                                                                                                                        | Ce serveur démarre et surveille tous les démons de l'environnement TSAMP/RSCST (Tivoli System Automation for Multiplatforms Reliable Scalable Cluster Technology).                                                                                                                                                                                                                                                                         |
| serveur d'application des règles                                                                     | IBM HTTP Server             | httpd -d, http -f                                                                                                                                    | Linux a besoin des droits d'accès de l'utilisateur root pour écouter les ports inférieurs à 1024. Les ports HTTP standard vont de 80 à 443. IBM Defense Operations Platform utilise le port 82. Les processus httpd -d et http -f doivent s'exécuter avec le compte superutilisateur. Toute autre configuration doit être effectuée au moment de l'installation dans le cadre de règles sécurité et de configurations complètes du réseau. |
| serveur d'applications, serveur de messagerie, serveur de données, serveur d'application des règles, | Tivoli Directory Integrator | /opt/IBM/TDI/V7.1/jvm/jre/bin/java .... /pwd_plugins/pam/pwsync_dop.props, /opt/IBM/TDI/V7.1/jvm/jre/bin/java .... /pwd_plugins/tds/pwsync_dop.props | Les processus Tivoli Directory Server et Linux Password Synchronizer Java Proxy doivent s'exécuter en tant que root pour intercepter les demandes de changement de mot de passe.                                                                                                                                                                                                                                                           |

## Accessibilité

Les fonctions d'accessibilité facilitent aux utilisateurs à mobilité réduite ou malvoyants l'utilisation des logiciels.

Les fonctions d'accessibilité principales de ce produit permettent aux utilisateurs d'effectuer les actions suivantes :

- Utiliser les technologies d'assistance, notamment des lecteurs d'écran et des synthétiseurs vocaux numériques, pour entendre la description de ce qui est affiché à l'écran. Pour plus d'informations sur l'utilisation de ces technologies d'assistance aux personnes, consultez la documentation du produit.
- Utiliser des fonctions spécifiques ou équivalentes à l'aide du clavier uniquement.
- Agrandir ce qui s'affiche à l'écran.

De plus, la documentation a été modifiée afin d'inclure les fonctions suivantes pour faciliter l'accessibilité :

- L'intégralité de la documentation est accessible au format XHTML afin d'optimiser l'application du logiciel de lecture d'écran.
- Toutes les images de la documentation sont fournies avec un texte de remplacement afin que les utilisateurs malvoyants puissent comprendre le contenu des images.

---

## Mention de droits d'auteur et marques

---

### Mention de droits d'auteur

© Copyright IBM Corporation 2011, 2013. All rights reserved. Peut être utilisé uniquement conformément à un contrat de licence logiciel IBM. Aucune partie de cette publication ne doit être reproduite, transmise, transcrite, conservée dans un système d'archivage ou convertie en un quelconque langage machine, sous quelque forme ou quelque moyen que ce soit, électronique, mécanique, magnétique, optique, chimique, manuel ou autre, sans autorisation écrite préalable d'IBM Corporation. IBM Corporation vous accorde des droits limités vous autorisant à imprimer ou à effectuer d'autres reproductions de toute documentation informatique pour votre propre utilisation, dans la mesure où ces reproductions comportent la notice de copyright d'IBM Corporation. Nul autre droit sous copyright n'est accordé sans autorisation écrite préalable de IBM Corporation. Le document n'est pas destiné à la production et est fourni "en l'état" sans garantie d'aucune sorte. **Toutes les garanties de ce document sont déclinées par la présente, y compris la garantie de non contrefaçon et les garanties d'aptitude à l'exécution d'un travail donné.**

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

---

### Marques

Cognos, CPLEX, IBM, ibm.com, DB2, Domino, GDDM, ILOG, Lotus, Notes, Passport Advantage, Rational, Sametime, Tivoli, Service Request Manager, Smarter Cities, SPSS, Redbooks, WebSphere et Worklight sont des marques d'IBM Corporation aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Internet Explorer, Windows, et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Intel et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Adobe, Acrobat, Portable Document Format (PDF), et PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

Oracle, Javascript, JavaBeans, et Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

D'autres noms peuvent être des marques de leurs propriétaires respectifs. Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

---

### Considérations relatives aux règles de confidentialité

Les produits IBM Software, y compris les solutions logicielles en tant que service, ("Offres logicielles") sont susceptibles d'utiliser des cookies ou d'autres technologies pour obtenir des informations sur l'utilisation du produit, pour aider à améliorer l'expérience de l'utilisateur final, pour créer des interactions avec lui ou pour toute autre raison. Dans de nombreux cas, les Offres logicielles ne collectent aucune information permettant d'identifier l'utilisateur. Quelques-unes de nos offres logicielles peuvent vous permettre de collecter des informations personnelles. Si cette offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont présentées ci-après.

Cette Offre logicielle n'utilise pas de cookies ni d'autre technologie pour collecter des informations permettant d'identifier l'utilisateur.

Cette offre logicielle utilise des cookies pour la gestion de sessions et la configuration du code d'accès unique. Si vous désactivez les cookies, vous ne pourrez pas accéder au système.

Si les configurations déployées pour cette offre logicielle vous offrent en tant que client la capacité de collecter des informations identifiant les utilisateurs finaux par le biais de cookies et d'autres technologies, vous devez vous-même vous renseigner sur les lois en vigueur relatives à la collecte de telles données, y compris toute exigence en matière de notification et d'accord.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy>, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/details>, ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse <http://www.ibm.com/software/info/product-privacy>.



---

## Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations  
IBM Canada Ltd  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse IBM suivante :

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRÉSENT DOCUMENT EST LIVRE "EN L'ÉTAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation  
Department T81B F6/Building 503  
4205 S. Miami Boulevard  
Durham NC 27709-9990  
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le programme sous licence décrit dans ce document et tout le matériel sous licence disponible pour ce programme, sont fournis par IBM conformément aux termes du contrat client IBM (IBM Customer Agreement), de l'accord de licence du programme international d'IBM (IBM International Program License Agreement) ou de tout contrat équivalent entre nous.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

#### LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "TELS QUELS" sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

---

## Marques

Cognos, CPLEX, IBM, ibm.com, DB2, Domino, GDDM, ILOG, Lotus, Notes, Passport Advantage, Rational, Sametime, Tivoli, Service Request Manager, Smarter Cities, SPSS, Redbooks, WebSphere et Worklight sont des marques d'IBM Corporation aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Internet Explorer, Windows, et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Intel et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Adobe, Acrobat, Portable Document Format (PDF), et PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

Oracle, Javascript, JavaBeans, et Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

D'autres noms peuvent être des marques de leurs propriétaires respectifs. Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.



---

## Index

### M

marques 204

### R

remarques 204





