

DevTest Solutions

Administration

Version 8.0



La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2014 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse <http://www.ca.com/worldwide>.

Table des matières

Chapitre 1: Administration générale 9

Numéros de port par défaut	9
Numéros de port par défaut de DevTest Server	9
Numéros de port par défaut de DevTest Workstation	11
Numéros de port par défaut du serveur de démonstration	12
Type d'installation partagée.....	13
Structure des répertoires	14
Répertoires de DevTest Workstation.....	15
Répertoires de DevTest Server.....	17
Exécution des composants de serveur comme services	19
Exécution de DevTest Solutions avec Ant et JUnit	21
Exécution de tests DevTest comme tests JUnit	22
Tâches Ant pour DevTest Solutions.....	22
Exemples d'utilisation de Ant et JUnit	26
Exemples d'utilisation de JUnit	27
intégration à CruiseControl.....	30
Exemple supplémentaire de fichiers de compilation.....	30
Paramètres de mémoire	31
Modification de la mémoire allouée	32
Conditions requises pour des fichiers Third-Party	34
Activation des langages de script supplémentaires	40

Chapitre 2: Administration de base de données 41

Configuration de la base de données interne	41
Configuration de la base de données de registre externe	42
Configuration de DevTest pour utiliser DB2	44
Configuration de DevTest pour utiliser MySQL.....	46
Configuration de DevTest pour utiliser Oracle.....	48
Configuration de DevTest pour utiliser SQL Server.....	50
Configuration de la base de données de tableau de bord Enterprise Dashboard externe.....	52
Maintenance de la base de données	53
Maintenance de la génération de rapports automatique.....	54
Suppression automatique d'entrées du journal d'audit	56
Suppression automatique de transactions	56
Suppression automatique de scénarios	57

Chapitre 3: Administration de licence 59

Licence Honor-Based (Basée sur honneur)	59
Fonctionnement de l'interaction entre les licences, les listes de contrôle d'accès et les rapports d'audit	61
Rapport d'audit d'utilisation de DevTest Solutions	64
Exemple de calcul de nombre	67
Types d'utilisateurs	68

Chapitre 4: Security (Sécurité) 73

Utilisation du protocole SSL pour sécuriser la communication	74
Certificats SSL	75
Création de votre propre certificat auto-signé	76
Utilisation du protocole SSL avec plusieurs certificats	79
Authentification réciproque (bidirectionnelle)	80
Utilisation de la communication HTTPS avec la console DevTest	80
Générez une nouvelle paire de clés et un certificat	81
Copie du nouveau référentiel de clés dans LISA_HOME	82
Mise à jour des propriétés Webserver	83
Utilisation de l'authentification Kerberos	84
(Liste de contrôle d'accès	86
Présentation de ACL	87
Outils ou API de liste de contrôle d'accès et de ligne de commande	91
Types de droits	92
Types d'utilisateur standard et rôles standard	93
Autorisations standard	107
Utilisateurs standard	120
Affichage des informations d'utilisateur à partir de DevTest Workstation	124
Gestion des utilisateurs et des rôles	125
Configuration de la liste de contrôle d'accès pour l'utilisation de l'authentification LDAP	133
Autorisation des utilisateurs authentifiés par LDAP	135
groupes de ressources	137

Chapitre 5: Logging (Journalisation) 141

Présentation des fichiers journaux	141
Fichiers journaux principaux	142
Fichiers journaux du serveur de démonstration	143
Fichier de propriétés de journalisation	144
Messages relatifs au statut pour les composants de serveur	145
Fils de discussion automatiques	146
Enregistreur d'étape de test	147

Chapitre 6: surveillance 149

Service Manager (Gestionnaire de services)	149
Options du gestionnaire de services	150
Exemples du gestionnaire de services	152
Ouverture de la console du serveur	153
Affichage du récapitulatif d'intégrité des composants	154
Affichage du détail des performances des composants.....	155
Création d'images mémoires de segment de mémoire et de fils de discussion	156
Nettoyage de la mémoire forcé	157
Utilisation du moniteur de registre	158
Moniteur de registre - Onglet Test	159
Moniteur de registre - Onglet Simulators (Simulateurs)	159
Moniteur de registre - Onglet Coordinator Servers (Serveurs de coordination)	160
Moniteur de registre - Onglet Virtual Environments (Environnements virtuels).....	160
Utilisation du tableau de bord Enterprise Dashboard	160
Ouverture du tableau de bord d'entreprise.....	161
Réactivation d'un registre ou du tableau de bord Enterprise Dashboard	167
Maintenance des registres.....	168
Exportation des données du tableau de bord.....	170
Exportation des données d'audit d'utilisation	172
Purge des données de tableau de bord	173

Glossaire 175

Chapitre 1: Administration générale

Ce chapitre traite des sujets suivants :

[Numéros de port par défaut](#) (page 9)
[Type d'installation partagée](#) (page 13)
[Structure des répertoires](#) (page 14)
[Exécution des composants de serveur comme services](#) (page 19)
[Exécution de DevTest Solutions avec Ant et JUnit](#) (page 21)
[Paramètres de mémoire](#) (page 31)
[Conditions requises pour des fichiers Third-Party](#) (page 34)
[Activation des langages de script supplémentaires](#) (page 40)

Numéros de port par défaut

Cette rubrique définit chaque numéro de port par défaut utilisé par les différents composants de DevTest.

- [DevTest Server](#) (page 9)
- [DevTest Workstation](#) (page 11)
- [Serveur de démonstration](#) (page 12)

Numéros de port par défaut de DevTest Server

La table suivante répertorie les numéros de port par défaut utilisés par divers composants dans DevTest Server. La table inclut également la propriété qui définit chaque numéro de port.

Port	Composant de DevTest	Property (Propriété)
1505	Embedded web server (Serveur Web intégré)	lisa.webserver.port
1506	Tableau de bord Enterprise Dashboard (serveur Web intégré)	dradis.webserver.port
1507	Portail DevTest	devtest.port
1528	Derby database (Base de données Derby)	lisadb.internal.port, lisadb.pool.common.url
1529	Demo server (Serveur de démonstration)	Non applicable
1530	Port de base de données Derby du tableau de bord Enterprise Dashboard	dradisdbs.internal.port

2003	Port réseau du tableau de bord Enterprise Dashboard	lisa.net.15.port
2004	Port réseau du gestionnaire de VSE	lisa.net.9.port
2005	Port réseau de l'utilitaire Test Runner (Exécuteur de tests)	lisa.net.5.port
2006	Port réseau de ServiceManager (Gestionnaire de services)	lisa.net.11.port
2008	Port réseau de la Worstation (Station de travail)	lisa.net.0.port
2009	Port réseau du Broker (Intermédiaire)	lisa.pathfinder.broker.port
2010	Port réseau de registre	lisa.net.3.port
2011	Port réseau du coordinateur	lisa.net.2.port
2012	Port réseau de JUnit exec	lisa.net.4.port
2013	Port réseau du VSE	lisa.net.8.port
2014	Port réseau du simulateur	lisa.net.1.port
2999	JDBC simulation driver (Pilote de simulation JDBC)	Non applicable
3128	Proxy HTTP	laf.httpproxy.port
3997	Agent LPAR	lisa.mainframe.bridge.server.port
8443	Embedded web server (Serveur Web intégré) (si SSL est activé)	lisa.webserver.ssl.port
61617	Agent LPAR	lisa.mainframe.bridge.port

Si plusieurs simulateurs sont créés sur le même ordinateur, les numéros de port des nouveaux simulateurs commencent à partir de 2014. Par exemple, les numéros de port 2015, 2016 et 2017 seraient attribués à trois simulateurs supplémentaires.

En général, il existe un coordinateur par laboratoire. Toutefois, si vous créez plusieurs coordinateurs, définissez le port dans la ligne de commande. Par exemple :

```
CoordinatorServer --name=tcp://hostname:2468/Coordinator2
```

Le fichier **lisa.properties** définit la plupart des numéros de port par défaut.

Si vous voulez changer un ou plusieurs numéros de port après l'installation, ajoutez la propriété au fichier **site.properties** et définissez la nouvelle valeur. Ne mettez pas à jour le fichier **lisa.properties**.

Vous pouvez changer le numéro de port pour le pilote de simulation JDBC en modifiant l'étape Virtual JDBC Listener (Ecouteur virtuel JDBC) dans DevTest Workstation.

Numéros de port par défaut de DevTest Workstation

Les numéros de port par défaut dans une installation de DevTest Workstation forment un sous-ensemble des numéros de port par défaut dans DevTest Server.

Port	Composant de DevTest	Property (Propriété)
1505	Embedded web server (Serveur Web intégré)	lisa.webserver.port
2004	VSE Manager (Gestionnaire d'environnements de services virtuel)	lisa.net.9.port
2005	Utilitaire Test Runner (Exécuteur de tests)	lisa.net.5.port
2006	ServiceManager	lisa.net.11.port
2009	Intermédiaire	lisa.pathfinder.broker.port
2999	JDBC simulation driver (Pilote de simulation JDBC)	Non applicable
3128	Proxy HTTP	laf.httpproxy.port
8443	Embedded web server (Serveur Web intégré) (si SSL est activé)	lisa.webserver.ssl.port

Numéros de port par défaut du serveur de démonstration

La table suivante répertorie les numéros de port par défaut utilisés par le serveur de démonstration.

Port	Composant de DevTest
1098	JNDI
1099	JNDI
1528	Derby database (Base de données Derby)
8080	HTTP

Les fichiers suivants définissent les numéros de port par défaut :

- lisa-demo-server/jboss/server/default/conf/jboss-service.xml
- lisa-demo-server/jboss/server/default/deploy/jboss-web.deployer/server.xml

Si vous voulez changer un ou plusieurs numéros de port après l'installation, vous pouvez mettre à jour ces fichiers directement.

Type d'installation partagée

Le type d'installation partagée est conçu pour des environnements avec les caractéristiques suivantes :

- Plusieurs utilisateurs partagent une installation de DevTest à partir de plusieurs ordinateurs.
- Chaque utilisateur dispose de données distinctes.

Dans une installation partagée, toutes les données et les fichiers temporaires sont stockés dans des répertoires spécifiés par l'utilisateur. Chaque utilisateur dispose de ses données personnelles, mais tous partagent une installation DevTest commune. Dans une installation partagée, les utilisateurs requièrent uniquement des droits d'accès en lecture au répertoire de programmes de DevTest.

Si vous sélectionnez le type d'installation partagée dans le programme d'installation, vous êtes invité à spécifier le répertoire de données et le répertoire de fichiers temporaires. L'emplacement par défaut de chaque répertoire est **USER_HOME**.

Dans une installation partagée, le fichier **lisa.user.properties** est ajouté au répertoire **LISA_HOME** et au répertoire **USER_HOME** pour l'utilisateur qui exécute l'installation. Ce fichier contient les propriétés **lisa.data.dir** et **lisa.tmpdir**. Pour spécifier l'emplacement du fichier, définissez la propriété système de **lisa.user.properties** ou la variable d'environnement **LISA_USER_PROPERTIES**. Si l'une des propriétés a été définie en tant que propriété système, la définition de la propriété système est prioritaire.

Remarque : Même si **lisa.tmpdir** permet de changer l'emplacement de stockage de vos fichiers temporaires, CA Technologies recommande de ne pas modifier cette propriété pour enregistrer les fichiers temporaires à un emplacement de point de montage externe ou de partage externe. Si vous rencontrez des problèmes d'instabilité de produit et que vous utilisez un partage externe pour le stockage de fichiers temporaires, la service de support peut vous indiquer de revenir à l'utilisation d'un disque local pour le stockage de fichiers temporaires pour obtenir une prise en charge continue de votre environnement.

Les nouveaux utilisateurs connectés à partir de différents ordinateurs doivent manuellement configurer leur propre fichier **lisa.user.properties** dans le répertoire **USER_HOME** correspondant avant d'accéder à une installation partagée. Vous pouvez copier le fichier à partir du répertoire **LISA_HOME** ou le créer manuellement si vous voulez utiliser des répertoires différents.

Si vous tentez de démarrer les composants de DevTest avant de configurer ce fichier de propriétés, le démarrage échouera. Un message d'erreur s'affiche dans la fenêtre et dans les fichiers journaux, indiquant une erreur lors de la lecture du fichier **lisa.user.properties**.

Structure des répertoires

Cette rubrique décrit la structure des répertoires de [DevTest Workstation](#) (page 15) et de [DevTest Server](#) (page 17).

Dans cette rubrique, le type local a été sélectionné pour l'installation de DevTest Solutions. Si le [type d'installation partagé](#) (page 13) a été sélectionné, les répertoires suivants peuvent être situés à un emplacement différent de **LISA_HOME** :

- cvsMonitors
- database (base de données)
- hotDeploy
- locks (verrous)
- tmp

Répertoires de DevTest Workstation

Le répertoire **LISA_HOME** pour DevTest Workstation contient les répertoires suivants :

Remarque : Le répertoire locks (verrous) doit disposer d'autorisations en lecture/écriture.

.install4j

Contient le programme d'installation.

addons

Contient les modules complémentaires de DevTest.

agent

Contient les fichiers de l'agent pour DevTest.

bin

Contient les fichiers exécutables pour DevTest Workstation et d'autres composants.

database (base de données)

Contient les fichiers DDL pour diverses bases de données.

defaults

Contient le document d'audit et les documents de simulation communs à tous les projets. Les documents de simulation spécifiques à un projet sont disponibles dans le répertoire Projects (Projets).

doc

Contient l'accord de licence.

examples

Projet par défaut contenant des exemples qui utilisent le serveur de démonstration

examples_src

Exemple de fichiers sources et de fichiers liés au kiosque

hotDeploy

Répertoire surveillé par DevTest. Ce répertoire contient des classes Java et des fichiers .jar. Les classes Java et les fichiers .jar de ce répertoire sont disponibles dans le classpath de DevTest. Les nouveaux fichiers ou répertoires ajoutés à ce répertoire sont ajoutés de manière dynamique au classpath de DevTest.

incontainer

Contient les instructions de test dans un conteneur.

jre

Contient le JRE requis.

lib

Contient les fichiers .jar requis.

licenses

Contient les fichiers de licence requis pour l'exécution de DevTest.

locks (verrous)

Contient les fichiers de verrouillage utilisés pour l'accès simultané interprocessus.

reports (rapports)

Contient les rapports de test de type XML créés par DevTest.

snmp

Contient les fichiers SNMP requis.

tmp

Contient les fichiers de journalisation créés par DevTest. Si vous communiquez avec le service de support sur un problème, il peut vous être demandé d'envoyer un ou plusieurs fichiers de ce répertoire.

umetrics

Contient les fichiers associés à la collecte de mesures.

Lorsque vous créez un projet dans DevTest Workstation, le répertoire **Projects (Projets)** est ajouté.

Répertoires de DevTest Server

Le répertoire **LISA_HOME** pour DevTest Server contient les répertoires suivants :

Remarque : Le répertoire locks (verrous) doit disposer d'autorisations en lecture/écriture.

.install4j

Contient le programme d'installation.

addons

Contient les modules complémentaires de DevTest.

agent

Contient les fichiers de l'agent pour DevTest.

bin

Contient les fichiers exécutables pour le registre, le coordinateur, le simulateur, le VSE, DevTest Workstation et d'autres composants. Ce répertoire contient également les fichiers de commandes suivants :

- startdefservers.bat - démarre les serveurs par défaut.
- stopdefservers.bat - arrête les serveurs par défaut.

cvsMonitors

Contient les moniteurs de service de validation en continu déployés.

database (base de données)

Contient les fichiers DDL pour diverses bases de données.

defaults

Contient le document d'audit et les documents de simulation communs à tous les projets. Les documents de simulation spécifiques à un projet sont disponibles dans le répertoire Projects (Projets).

doc

Contient l'accord de licence.

examples

Projet par défaut contenant des exemples qui utilisent le serveur de démonstration

examples_src

Exemple de fichiers sources et de fichiers liés au kiosque

hotDeploy

Répertoire surveillé par DevTest. Ce répertoire contient des classes Java et des fichiers .jar. Les classes Java et les fichiers .jar de ce répertoire sont disponibles dans le classpath de DevTest. Les nouveaux fichiers ou répertoires ajoutés à ce répertoire sont ajoutés de manière dynamique au classpath de DevTest.

incontainer

Contient les instructions de test dans un conteneur.

jre

Contient le JRE requis.

lib

Contient les fichiers .jar requis.

licenses

Contient les fichiers de licence requis pour l'exécution de DevTest.

locks (verrous)

Contient les fichiers de verrouillage utilisés pour l'accès simultané interprocessus.

reports (rapports)

Contient les rapports de test de type XML créés par DevTest.

snmp

Contient les fichiers SNMP requis.

tmp

Contient les fichiers de journalisation créés par DevTest. Si vous communiquez avec le service de support sur un problème, il peut vous être demandé d'envoyer un ou plusieurs fichiers de ce répertoire.

umetrics

Contient les fichiers associés à la collecte de mesures.

webserver

Contient les fichiers de serveur Web.

Lorsque vous créez un projet dans DevTest Workstation, le répertoire **Projects (Projets)** est ajouté.

Exécution des composants de serveur comme services

Si vous prévoyez de laisser les composants de serveur en exécution la plupart du temps, vous pouvez utiliser les fichiers exécutables de service dans le répertoire **LISA_HOME\bin**.

Les noms par défaut des composants de serveur sont utilisés lorsqu'ils sont démarrés à partir de la ligne de commande sans nom spécifique. Le fichier `lisa.properties` est installé avec les propriétés et les valeurs par défaut suivantes :

- `lisa.registryName=Registry`
- `lisa.coordName=Coordinator`
- `lisa.simulatorName=Simulator`
- `lisa.vseName=VSE`

Si vous voulez remplacer une valeur par défaut pour l'une de ces propriétés, spécifiez la nouvelle valeur dans votre fichier **local.properties**.

Il est recommandé de démarrer et d'arrêter les composants dans l'ordre affiché.

Pour démarrer des composants de serveur comme services :

Entrez les commandes suivantes :

```
EnterpriseDashboardService start
RegistryService start
PortalService start
BrokerService start
CoordinatorService start
SimulatorService start
VirtualServiceEnvironmentService start
```

Pour arrêter des composants de serveur comme services :

Entrez les commandes suivantes :

```
SimulatorService stop
CoordinatorService stop
VirtualServiceEnvironmentService stop
BrokerService stop
PortalService stop
RegistryService stop
```

EnterpriseDashboardService stop

Pour configurer le démarrage automatique des services sous UNIX, consultez votre administrateur système.

Si DevTest Workstation a démarré la base de données de rapports (Derby), cette base de données se fermera lors de l'arrêt de DevTest Workstation.

Si le coordinateur a démarré la base de données (Derby), cette base de données ne se fermera pas lors de l'arrêt du coordinateur.

Exécution de DevTest Solutions avec Ant et JUnit

Vous pouvez exécuter des tests DevTest en tant que tests JUnit dans le chemin d'exécution d'un fichier de compilation Ant.

Cette fonctionnalité fournit des perspectives réelles de compilation automatisée et d'intégration de test. Vous pouvez combiner la flexibilité d'Ant et la simplicité de JUnit à la puissance de DevTest Solutions pour répondre aux besoins d'automatisation suivants :

- Intégration
- Load (Charger)
- Contrainte
- Surveillance de la production

Ant est un outil Java open source de création de logiciel automatisé. Ant est étendu à l'aide de la prise en charge de nombreux outils tiers, y compris JUnit. Pour plus d'informations, consultez <http://ant.apache.org/>.

JUnit est une structure Java de test d'unités de code source ouvert. JUnit est largement utilisé par des outils de test tiers, y compris DevTest Solutions. Pour plus d'informations, consultez <http://www.junit.org>.

- L'étape Execute JUnit Test Case/Suite (Exécuter un scénario de test ou une suite JUnit) peut exécuter un test JUnit. Les [tâches Ant pour DevTest](#) (page 22) peuvent exécuter un test ou une suite DevTest et les rendre similaires à des tests JUnit.
- Les rapports et les fichiers journaux JUnit sont générés uniquement lorsque la tâche Ant **junitlisa** est utilisée pour exécuter des tests.
- L'étape JUnit permet d'intégrer des scénarios de test JUnit existants au flux de travaux de test. Vous pouvez utiliser DevTest pour encapsuler les tests JUnit et les exécuter via DevTest.
- La tâche **junitlisa** permet l'automatisation des tests sans passer par l'interface utilisateur de DevTest. La tâche **junitlisa** génère un rapport HTML, car aucune interface utilisateur n'est disponible pour l'envoi des résultats.

Exécution de tests DevTest comme tests JUnit

L'étape JUnit prend en charge des scénarios de test et des suites de tests JUnit3 et JUnit4. Cette procédure décrit les étapes requises pour exécuter de tests DevTest comme tests JUnit et de les signaler comme tests natifs JUnit.

Procédez comme suit:

1. Vérifiez qu'Ant et JUnit sont disponibles sur votre PC et que le chemin ANT_HOME\bin est défini.
2. Copiez **junit.jar** à partir de votre installation de JUnit vers ANT_HOME\lib.
3. Définissez la propriété système **LISA_HOME** et définissez sa valeur sur le répertoire d'installation de DevTest.
4. Utilisez la tâche **junitlisa** pour exécuter des tests DevTest comme tests JUnit.
5. (Facultatif) Utilisez la tâche **junitlisareport** pour créer des rapports HTML à partir de la sortie XML de JUnit.

La sortie de la journalisation est écrite dans un fichier **junitlisa_log.log** dans le répertoire **user.home\lisatmp**.

Le niveau de journalisation utilisé est identique à celui défini dans le fichier **LISA_HOME\logging.properties**.

Pour modifier le niveau de journalisation :

Remplacez la première ligne de ce fichier :

```
log4j.rootCategory=INFO,A1
```

à

```
log4j.rootCategory=DEBUG,A1
```

La sortie de JUnit standard est disponible dans le fichier **user.home/lisatmp/junit/index.html**.

Tâches Ant pour DevTest Solutions

Les tâches Ant suivantes sont fournies avec DevTest Solutions :

- [junitlisa](#) (page 23)
- [junitlisareport](#) (page 26)

tâche Ant de junitlisa

La tâche **junitlisa** est un remplacement par substitution de la tâche JUnit disponible avec Ant, mais qui exécute des tests DevTest au lieu de tests JUnit. La plupart des systèmes de compilation continus reconnaissent les fichiers de sortie XML et intègrent le tableau de bord de compilation aux résultats de test.

Cette tâche est une sous-classe directe de la tâche JUnit. Par conséquent, les attributs et éléments imbriqués de la tâche **junitlisa** sont identiques à ceux de la tâche JUnit. Toutefois, tenez compte des différences suivantes dans le comportement :

- Vous ne pouvez pas définir l'attribut **fork (réplication)** sur **false**.
- Vous ne pouvez pas ajouter d'éléments de **test** imbriqués. Utilisez l'attribut **test** à la place.
- Vous ne pouvez pas ajouter d'éléments **batchtest** imbriqués. Utilisez l'attribut **suite** à la place.
- Un classpath implicite comprenant **LISA_HOME\bin*.jar**, **LISA_HOME\lib*.jar**, ***.zip** et **LISA_HOME\lib\endorsed*.jar** est ajouté.
- Une propriété système **java.endorsed.dirs** implicite pointant vers **LISA_HOME\lib\endorsed** est ajoutée.
- Si aucun formateur n'est spécifié, un formateur par défaut de type **xml** sera ajouté.
- L'attribut **printsummary** est défini par défaut sur **true**.
- L'attribut **maxmemory** est défini par défaut sur 1024 m.
- L'attribut **showoutput** est défini par défaut sur **true**.

Hormis les attributs hérités de la tâche JUnit, la tâche **junitlisa** a les attributs suivants :

suite

Nom de fichier d'un document de suite.

Exemple : suite="AllTestsSuite.ste"

test

Nom de fichier d'un scénario de test.

Exemple : test="multi-tier-combo.tst"

stagingDoc

Nom de fichier d'un document de simulation.

Exemple : stagingDoc="Run1User1Cycle.stg"

config

Ensemble de configurations internes nommé ou nom de fichier.

Exemple : config="project.config"

outfile (fichier de sortie)

Nom du fichier utilisé pour écrire des données de génération de rapports. Si la valeur ne respecte pas le schéma de nom standard pour junitlisareport, spécifiez plutôt une tâche junitreport entièrement configurée.

Exemple : outfile="report"

registry (registre)

Pointeur vers le registre à utiliser lorsque vous voulez simuler les scénarios de test à distance.

Exemple : registry="tcp://testbox:2010/Registry"

preview (prévisualiser)

Permet d'écrire le nom et la description de chaque scénario de test, sans les exécuter.

Exemple : preview="true"

user (utilisateur)

Spécifie le nom d'utilisateur pour l'authentification ACL.

Exemple : user="admin"

password (mot de passe)

Spécifie le mot de passe pour l'authentification ACL.

Exemple : password="admin"

mar

Nom de fichier d'un document MAR.

Exemple : mar="example.mar"

mari

Nom de fichier d'un document d'informations MAR.

Exemple : mari="example.mari"

La tâche **junitlisa** inclut un élément imbriqué appelé **lisatest**. Cet élément inclut les attributs suivants :

suite

Nom de fichier d'un document de suite.

Exemple : suite="AllTestsSuite.ste"

test

Nom de fichier d'un scénario de test.

Exemple : test="multi-tier-combo.tst"

stagingDoc

Nom de fichier d'un document de simulation.

Exemple : stagingDoc="Run1User1Cycle.stg"

mar

Nom de fichier d'un document MAR.

Exemple : mar="example.mar"

mari

Nom de fichier d'un document d'informations MAR.

Exemple : mari="example.mari"

Les valeurs d'attribut peuvent utiliser des accolades, qui sont résolues de manière habituelle.

Vous devez spécifier au moins un test ou une suite. Vous pouvez spécifier un test ou une suite dans un élément imbriqué **lisatest** ou dans l'attribut **test** ou **suite**. Vous pouvez spécifier plusieurs tests et suites en ajoutant plusieurs éléments **lisatest**. Les tests et les suites sont exécutés dans l'ordre d'apparition dans le fichier XML.

Lorsque vous exécutez un test unique avec l'attribut **test**, le comportement par défaut du test est le suivant :

- Simulation avec un utilisateur virtuel unique
- Une seule exécution
- Délai de réflexion de 100 %

Pour changer ce comportement par défaut, encapsulez le test dans une suite et spécifiez un autre document de simulation.

Tâche Ant de junitlisareport

Vous pouvez produire des rapports HTML avec la tâche **junitlisareport** ou la tâche **junitreport** standard.

La tâche **junitlisareport** est une sous-classe de l'élément standard **junitreport**, à ceci près que les valeurs par défaut sensibles sont spécifiées. Elle est équivalente au code suivant :

```
<junitreport todir="${testReportDir}">

  <fileset dir="<todir specified in the junitreport tag">">
    <include name="TEST-*.xml"/>
  </fileset>

  <report format="frames" todir="<todir specified in the junitreport tag">">/>

</junitreport>
```

Vous pouvez spécifier votre propre définition de fichier et votre propre rapport. La tâche étant une sous-classe directe de **junitreport**, tous les attributs et éléments imbriqués que **junitreport** possède sont pris en charge.

Il est recommandé de spécifier l'attribut **toDir** hérité dans la plupart des cas, bien qu'il soit remplacé par défaut par le répertoire de travail actuel.

Exemples d'utilisation de Ant et JUnit

Exemple : fichier Ant Build complet

Le fichier **build.xml** dans le répertoire **LISA_HOME\examples** est un fichier de compilation Ant complet.

Le fichier de compilation contient deux cibles :

- La cible **lisaTests** exécute une suite comme tests JUnit. La suite est spécifiée avec l'élément imbriqué **lisatest**.
- La cible **oneTest** exécute un scénario de test comme test JUnit. Le scénario de test est spécifié avec l'attribut **test**.

Le fichier de compilation suppose que le contrôle d'accès (liste de contrôle d'accès) est activé. Par conséquent, les attributs **user** (utilisateur) et **password** (mot de passe) sont inclus.

Exemple : tâche junitlisa pour un scénario de test

La tâche **junitlisa** suivante est configurée pour exécuter un scénario de test unique sur un registre distant.

```
<junitlisa test="MyTest.tst"
  config="dev"
  registry="tcp://testbox:2010/Registry"
  toDir="${testReportDir}"
  haltOnError="no"
  errorProperty="test.failure">
  <jvmarg value="-DmySystemProp=someValue"/>
</junitlisa>
```

Exemples d'utilisation de JUnit

[Scénarios de test JUnit3](#) (page 28)

[Suites de test JUnit3](#) (page 28)

[Scénarios de test JUnit4](#) (page 29)

[Suites de test JUnit4](#) (page 29)

Scénarios de test JUnit3

Dans le cas de scénarios de test JUnit3, suivez les conventions JUnit pour écrire votre scénario de test. Notamment :

- Votre classe de test doit étendre `junit.framework.TestCase`.
- Les noms de méthode doivent commencer par `test`.

Par exemple :

```
import junit.framework.TestCase;

public class JUnit3TestCase extends TestCase {

    public void testOneIsOne() {
        assertEquals (1, 1);
    }

    public void testTwoIsThree() {
        assertEquals (2, 3);
    }

}
```

Suites de test JUnit3

Dans le cas de suites de test JUnit3, il n'est pas nécessaire que la suite étende `junit.framework.TestSuite`. Toutefois, elle doit implémenter la méthode `suite()`, avec des scénarios de test encapsulés par `JUnit4TestAdapter`.

Par exemple :

```
import junit.framework.JUnit4TestAdapter;
import junit.framework.TestSuite;

public class JUnit3VanillaTestSuite {

    public static TestSuite suite() {
        TestSuite suite = new TestSuite();
        suite.addTest ( new JUnit4TestAdapter ( MyJUnit3TestCase.class ) );
        return suite;
    }

}
```

Scénarios de test JUnit4

Dans le cas de scénarios de test JUnit4, les méthodes de test doivent comprendre l'annotation `@org.junit.Test`, comme requis par JUnit4.

Par exemple :

```
import static org.junit.Assert.assertEquals;

import org.junit.Test;

public class JUnit4TestCase {

    @Test
    public void oneIsOne() { assertEquals (1, 1); }

    @Test
    public void twoIsThree() { assertEquals (2, 3); }

}
```

Suites de test JUnit4

Pour implémenter une suite de test JUnit4, ajoutez les annotations `@RunWith` et `@Suite.SuiteClasses` pour marquer la classe comme suite de tests.

Par exemple :

```
import org.junit.runner.RunWith;
import org.junit.runners.Suite;

@RunWith(Suite.class)

@Suite.SuiteClasses ( { JUnit4TestCase.class } )

public class JUnit4VanillaTestSuite { // empty }
```

Remarque : Si le chargement du test JUnit renvoie un exception `IllegalArgumentException` à l'étape de JUnit, vérifiez que vous avez ajouté **.class** à la fin du nom de la classe. Vous pouvez vérifier manuellement l'orthographe du nom de la classe ou utiliser le navigateur du classpath pour rechercher la classe.

intégration à CruiseControl

Si vous utilisez CruiseControl pour fournir une intégration continue, vous pouvez le configurer pour inclure des échecs de test dans son panneau de configuration.

Dans la tâche Ant de JUnit illustrée dans les exemples d'utilisation de [Ant et JUnit](#) (page 26), `${testReportDir}` est défini comme `${LISA_HOME}/bin/lisa-core.jar`.

L'exemple de test suivant illustre un fichier **CruiseControl config.xml** standard :

```
<project name="myproj " buildafterfailed="false">
  <log>
    <merge dir="/home/cruise/build"/>
    <merge dir="/path/to/lisajunit/output"/>
  </log>
  .
  .
  .
</project>
```

Exemple supplémentaire de fichiers de compilation

En plus du fichier **build.xml** décrit dans les exemples d'utilisation de [Ant et JUnit](#) (page 26), le répertoire **LISA_HOME\examples** contient les exemples de fichiers suivants pour l'automatisation de projets DevTest :

- **automated-build.xml** : fichier de compilation principale que vous placez dans la partie supérieure de la hiérarchie de projet
- **lisa-project-build.xml** : Le fichier de compilation que vous placez dans chaque projet. Le nom de fichier doit être remplacé par **build.xml**.
- **common.xml** : fichier que vous placez dans chaque sous-répertoire entre la racine et le projet
- **common-macros.xml** : ce fichier contient des macros pour effectuer différentes tâches avec des composants de DevTest Server. Par exemple, vous pouvez démarrer le registre, exécuter une suite de tests ou déployer un service virtuel. Ce fichier n'est pas un fichier de compilation autonome et est destiné à être inclus dans des structures Ant existantes.

Pour plus d'informations, consultez les commentaires dans chaque fichier.

Paramètres de mémoire

Sous des systèmes d'exploitation Windows, la limite de mémoire par défaut pour DevTest Workstation est de 512 Mo (-Xmx512m).

Pour un système Windows, il est recommandé d'installer DevTest Server sous Windows 64 bits pour utiliser davantage de mémoire si nécessaire.

Modification de la mémoire allouée

Les fichiers **.vmoptions** sont utilisés pour transférer des paramètres supplémentaires à un processus Java pour modifier les paramètres par défaut utilisés pour la machine virtuelle Java. Ces fichiers sont utilisés pour personnaliser les paramètres d'allocation de mémoire pour chacun des processus DevTest utilisés dans le serveur. Lorsque vous installez le DevTest Server, le dossier LISA_HOME\bin est rempli avec un fichier .vmoption portant le même nom que chaque fichier exécutable. Une liste complète de paramètres de la machine virtuelle Java est détaillée dans le site Web d'Oracle, sous la section Configuring the Default JVM and Java Arguments.

Pour changer la taille du segment de mémoire Java sous Windows et UNIX :

1. Ouvrez le fichier cible portant l'extension **.vmoptions**.

Par exemple, ouvrez le fichier **RegistryService.vmoptions**, avec le contenu suivant :

```
# Enter one VM parameter per line
# For example, to adjust the maximum memory usage to 512 MB, uncomment the following
line:
# -Xmx512m
# To include another file, uncomment the following line:
# -include-options [path to other .vmoption file]
```

2. Pour modifier la mémoire maximum à allouer (Xmx), supprimez les marques de commentaires dans la ligne suivante :

```
# -Xmx512m
```

3. Pour modifier la mémoire minimum à allouer (Xms), ajoutez l'argument VM sur une autre ligne.

```
-Xms128M
```

Le fichier spécifiera alors la plage d'allocation de mémoire comme dans l'exemple suivant.

```
-Xms128M
```

```
-Xmx512M
```

4. Enregistrez le fichier texte dans le dossier **LISA_HOME\bin**.

Pour changer la taille du segment de mémoire Java sous Mac OS X :

Accédez à **LISAWorkstation.app** et modifiez le fichier **Info.plist**.

Le chemin d'accès est **LisaHome/bin/LISAWorkstation.app/Contents/Info.plist**. Vous pouvez modifier le fichier **Info.plist**, mais vos modifications s'appliquent uniquement à la station de travail DevTest Workstation.

Pour ajuster la mémoire pour des processus spécifiques :

Vous pouvez ajuster la mémoire pour les programmes suivants :

- Intermédiaire
- BrokerService (service de l'intermédiaire)
- CoordinatorServer (serveur de coordination)
- CoordinatorService (serveur de coordination)
- Registre
- RegistryService (service du registre)
- Simulator (Simulateur)
- SimulatorService (service de simulateur)
- VirtualServiceEnvironment (environnement de services virtuels)
- VirtualServiceEnvironmentService (service de l'environnement de services virtuels)
- Station de travail

Pour ajuster la mémoire pour tous les processus, vous pouvez modifier les fichiers de script spécifiques. Par exemple, vous pouvez allouer 128 M au registre et 1024 M au simulateur.

Si vous réinstallez DevTest Solutions, ces modifications seront écrasées par le programme d'installation.

Vous pouvez également copier ces fichiers et modifier les copies. Par exemple, vous pouvez copier Registry et le modifier par MyRegistry, puis ajuster/améliorer MyRegistry.

Conditions requises pour des fichiers Third-Party

Pour utiliser DevTest Solutions avec différentes applications tierces, les fichiers .jar des applications tierces doivent être disponibles pour DevTest. Sauf indication contraire spécifiée dans les sections suivantes, vous pouvez utiliser l'une des méthodes suivantes :

- Placez les fichiers dans le répertoire **LISA_HOME\hotDeploy**.
- Placez les fichiers dans le répertoire **LISA_HOME\lib**.
- Définissez la variable **LISA_POST_CLASSPATH**.

L'exemple suivant illustre la variable **LISA_POST_CLASSPATH** sur un ordinateur Windows. Dans cet exemple, il s'agit de fichiers WebSphere MQ.

```
LISA_POST_CLASSPATH="C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mq.commonservices.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mq.headers.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mq.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mq.jmqi.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mq.pcf.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\com.ibm.mqjms.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\connector.jar;C:\Program  
Files\IBM\MQSeries\Java\lib\dhbcore.jar"
```

CA ne fournit pas les fichiers tiers répertoriés dans cette rubrique.

Remarque : Dans cette rubrique, le type local a été sélectionné pour l'installation de DevTest Solutions. Si le [type d'installation partagé](#) (page 13) a été sélectionné, le répertoire **hotDeploy** peut être situé à un emplacement différent de **LISA_HOME**.

Conditions requises pour des fichiers JCAPS

Si vous utilisez l'étape JCAPS Messaging (Native) (Messagerie JCAPS, Native), consultez la documentation de JCAPS pour obtenir des informations sur les fichiers .jar dont vous pourriez avoir besoin.

Si vous utilisez l'étape JCAPS Messaging (Messagerie JCAPS, JNDI), le fichier **com.stc.jms.stcjms.jar** sera requis. Pour obtenir des informations sur d'autres fichiers .jar dont vous pourriez avoir besoin, consultez la documentation JCAPS.

Les fichiers .jar sont disponibles dans le répertoire **lib** de l'installation JCAPS.

Conditions requises pour les fichiers de messagerie JMS

Si vous utilisez l'étape JMS Messaging (JNDI) (Messagerie JCAPS, JNDI), consultez la documentation du fournisseur JMS pour obtenir des informations sur les fichiers .jar dont vous pourriez avoir besoin.

Conditions requises pour les fichiers Oracle OC4J

Les fichiers .jar suivants sont requis :

- dms.jar
- oc4j.jar
- oc4jclient.jar

Consultez la documentation OC4J pour obtenir des informations sur les fichiers .jar dont vous pourriez avoir besoin. Les fichiers .jar sont disponibles dans le répertoire **lib** de l'installation OC4J.

Conditions requises pour des fichiers SAP

Les fichiers .jar suivants sont requis :

- sapjdoc3.0.8/sapidoc3.jar, requis pour les étapes SAP IDoc et la virtualisation
- sapjco3.0.9/sapjco3.jar
- sapjco3.0.9/*plate-forme*/, un fichier de bibliothèque natif de la plate-forme, où *plate-forme* correspond à votre système informatique (osx_64, windows_x86, etc.). Requis pour l'étape RFC SAP, les étapes SAP IDoc et la virtualisation

Conditions requises pour la virtualisation SAP IDoc

1. Créez une destination RFC de type T sur le client et le serveur SAP. DevTest utilise cette destination RFC pour recevoir des documents IDoc à partir des deux systèmes.
2. Mettez à jour le profil de partenaire de sortie sur le client et le serveur SAP. Mettez à jour le paramètre de sortie dans le profil de partenaire pour que le type de document IDoc respectif soit envoyé au numéro de port associé aux destinations RFC créées à l'étape 1. Ainsi, DevTest peut recevoir des documents IDoc à partir des systèmes de client et de serveur SAP.
3. Créez et importez les fichiers de propriété de connexion dans votre projet sous le répertoire Data (Données).
 - a. Créez la connexion RFC (avec les propriétés provenant de .jcoServer) pour la destination RFC sur le client créée à l'étape 1.

- b. Créez le fichier de propriété de connexion au système (avec les propriétés provenant de .jcoDestination) pour le client SAP.
- c. Créez la connexion RFC (avec les propriétés provenant de .jcoServer) pour la destination RFC sur le serveur créée à l'étape 1.
- d. Créez le fichier de propriété de connexion au système (avec les propriétés provenant de .jcoDestination) pour le serveur SAP.

Avant de commencer l'enregistrement, vous devez également créer et importer les fichiers de propriété de connexion dans votre projet sous le répertoire **Data** (Données). Ces fichiers sont requis pour démarrer les serveurs JCo afin de recevoir et d'envoyer les documents IDoc au client et au serveur SAP. Les fichiers de propriété pour la connexion RFC (avec les propriétés provenant de .jcoServer) et la connexion système (avec les propriétés provenant de .jcoDestination) sont également requis. Ces fichiers sont requis pour démarrer les serveurs JCo afin de recevoir et d'envoyer les documents IDoc au client et au serveur SAP. Pour en savoir plus sur la procédure de remplissage de ces fichiers de propriété, consultez votre administrateur SAP.

Conditions requises pour la virtualisation SAP RFC

1. Créez une destination RFC de type T sur le client SAP. DevTest utilise cette destination RFC pour intercepter les appels de fonction distants effectués par le client.
2. Mettez à jour le code ABAP qui effectue l'appel de fonction distant afin d'utiliser la nouvelle destination.
3. Créez et importez les fichiers de propriété de connexion dans votre projet sous le répertoire Data (Données). Pour en savoir plus sur la procédure de remplissage de ces fichiers de propriété, consultez votre administrateur SAP.
 - a. Créez la connexion RFC (avec les propriétés provenant de .jcoServer) pour la destination RFC sur le client créée à l'étape 1. Ce fichier ne doit pas spécifier la propriété `jco.server.repository_destination`.
 - b. Créez le fichier de propriété de connexion au référentiel (avec les propriétés provenant de .jcoDestination) pour le système défini en tant que référentiel RFC. Il s'agit en général du même système sur lequel le RFC a été exécuté.
 - c. Créez le fichier de propriété de connexion au système (avec les propriétés provenant de .jcoDestination) pour le système sur lequel le RFC est exécuté. Si s'agit du même fichier que pour la connexion au référentiel, un seul fichier de propriétés est nécessaire.

Conditions requises pour des fichiers SonicMQ

Les fichiers .jar suivants sont requis :

- mfcontext.jar
- sonic_Client.jar

- sonic_XA.jar

Les fichiers .jar sont disponibles dans le répertoire **lib** de l'installation SonicMQ.

Conditions requises pour des fichiers TIBCO

Les conditions requises pour TIBCO varient selon l'application.

Copiez les fichiers .jar de TIBCO dans le répertoire **LISA_HOME\lib** ou définissez la variable **LISA_POST_CLASSPATH**. Ne copiez pas les fichiers dans le répertoire **LISA_HOME\hotDeploy**.

Etape TIBCO Rendezvous Messaging (Messagerie TIBCO Rendezvous)

Les fichiers .jar suivants sont requis :

- tibrvj.jar
- tibrvjms.jar
- tibrvjds.jar
- tibrvjweb.jar
- tibrvnative.jar
- tibrvnativesd.jar

Les fichiers TIBCO Rendezvous .dll sont également requis. Copie tous les fichiers .dll du répertoire **bin** de TIBCO Rendezvous vers le répertoire **LISA_HOME\bin**. Référez l'emplacement **LISA_HOME\bin** dans votre environnement **PATH**.

Ajoutez également le répertoire **bin** de TIBCO Rendezvous à votre variable d'environnement **PATH**.

TIBCO EMS Messaging (Messagerie TIBCO EMS) ou TIBCO Direct JMS

Les fichiers .jar suivants sont requis :

- tibjms.jar
- tibjmsadmin.jar
- tibjmsapps.jar
- tibrvjms.jar

Mesures TIBCO Hawk Metrics (Mesures TIBCO Hawk)

Les fichiers .jar suivants sont requis :

- console.jar

- talon.jar
- util.jar

Les fichiers .jar de TIBCO Rendezvous et/ou TIBCO EMS, selon le type de transport utilisé par TIBCO Hawk, doivent également être copiés dans le répertoire **LISA_HOME\lib**.

Conditions requises pour des fichiers WebLogic

Le fichier **weblogic.jar** est requis. Si vous utilisez la sécurité ou JMX, d'autres fichiers .jar peuvent être requis.

Consultez la documentation WebLogic pour obtenir des informations sur les fichiers .jar dont vous pourriez avoir besoin. Les fichiers .jar sont disponibles dans le répertoire **lib** de l'installation WebLogic.

Conditions requises pour les fichiers webMethods

Les fichiers .jar suivants sont requis :

- (Serveur d'intégration webMethods 8.2) Copiez le fichier wm-isclient.jar de votre installation de webMethods vers le répertoire installation_directory\lib\shared de DevTest.
- (Serveur d'intégration webMethods 7.1 et version ultérieure)
installation_directory\lib\shared\wm-isclient.jar
- (Serveur d'intégration webMethods 7.0 et version antérieure)
installation_directory\lib\client.jar
- wm-enttoolkit.jar
- wmbrokerclient.jar
- wmjmsadmin.jar
- wmjmsclient.jar
- wmjmsnaming.jar

Les fichiers .jar sont disponibles dans le répertoire **lib** de l'installation WebMethods.

Conditions requises pour les fichiers WebSphere MQ

Copiez les fichiers .jar de WebSphere MQ dans le répertoire **LISA_HOME\lib** ou définissez la variable **LISA_POST_CLASSPATH**. Ne copiez pas les fichiers dans le répertoire **LISA_HOME\hotDeploy**.

Remarque : Si le système d'exploitation est une version japonaise, utilisez les fichiers répertoriés pour WebSphere MQ 7.

Les fichiers .jar suivants sont requis pour WebSphere MQ 5.2 :

- com.ibm.mqjms.jar
- com.ibm.mqbind.jar
- com.ibm.mq.pcf.jar
- com.ibm.mq.jar
- connector.jar

Les fichiers .jar suivants sont requis pour WebSphere MQ 6 :

- com.ibm.mq.jar
- com.ibm.mq.pcf.jar
- com.ibm.mqjms.jar
- connector.jar
- dhbcore.jar

Les fichiers .jar suivants sont requis pour WebSphere MQ 7 :

- com.ibm.mq.commonservices.jar
- com.ibm.mq.headers.jar
- com.ibm.mq.jar
- com.ibm.mq.jmqi.jar
- com.ibm.mq.pcf.jar
- com.ibm.mqjms.jar
- connector.jar
- dhbcore.jar

Les fichiers .jar sont disponibles dans le répertoire **MQ_HOME\java\lib**.

Activation des langages de script supplémentaires

Pour permettre aux utilisateurs d'utiliser d'autres langages JSR-223 dans l'étape de test Execute Script (Exécuter un script), l'assertion Scriptable (Prenant en charge les scripts), l'éditeur de scripts de correspondance et le protocole de données prenant en charge les scripts, vous pouvez activer des langages supplémentaires.

Pour activer un langage de script supplémentaire, placez le fichier .jar du langage dans le répertoire **hotdeploy** du coordinateur distant, du serveur, ou du CA Service Virtualization. Lors du démarrage suivant, le langage supplémentaire figurera dans la liste déroulante Language dans la station de travail DevTest Workstation.

Chapitre 2: Administration de base de données

Ce chapitre traite des sujets suivants :

[Configuration de la base de données interne](#) (page 41)

[Configuration de la base de données de registre externe](#) (page 42)

[Configuration de la base de données de tableau de bord Enterprise Dashboard externe](#) (page 52)

[Maintenance de la base de données](#) (page 53)

Configuration de la base de données interne

La base de données Derby d'Apache est fournie comme base de données préconfigurée de sorte à disposer d'un système opérationnel lorsque vous vous préparez à modifier la solution de base de données d'entreprise pour votre organisation. La base de données Derby n'est pas prise en charge comme solution de base de données d'entreprise. Cette base de données préconfigurée est disponible dans le répertoire

LISA_HOME\database\lisa.db. Pour éviter des problèmes liés à la migration manuelle de données, il est recommandé de configurer les bases de données d'entreprise comme tâche de post-installation.

Les composants suivants interagissent avec une base de données :

- Génération de rapports
- Contrôle des accès (liste de contrôle d'accès)
- Intermédiaire de l'agent Java
- VSE
- Enterprise Dashboard (Tableau de bord d'entreprise)

Utilisez vos procédures propres à chaque site pour sauvegarder les bases de données d'entreprise que vous utilisez pour DevTest Solutions.

Remarque : Pour obtenir des informations sur la configuration système requise pour la base de données, reportez-vous à la section *Installation*.

Configuration de la base de données de registre externe

Vous pouvez configurer DevTest pour utiliser une base de données externe en modifiant le fichier **site.properties** dans le répertoire **LISA_HOME**.

Remarques :

- Pour obtenir des informations sur la configuration système requise pour la base de données, reportez-vous à la section *Installation*.
- Le tableau de bord Enterprise Dashboard ne prend pas en charge la base de données DB2 d'IBM.

Le répertoire **LISA_HOME\database** inclut un fichier modèle **site.properties** pour chacune des bases de données prises en charge :

- **db2-site.properties** : IBM DB2
- **derby-site.properties** : Derby
- **mysql-site.properties** : MySQL
- **oracle-site.properties** : Oracle
- **sqlserver-site.properties** : Microsoft SQL Server

Si vous exécutez DevTest Server, il n'est pas nécessaire de reconfigurer chaque installation de DevTest Workstation. La configuration de **site.properties** est propagée à chaque station de travail, VSE, coordinateur, serveur de simulation et tout autre composant DevTest connecté au registre.

La procédure générale se présente comme suit :

1. Copiez le fichier modèle **_site.properties** approprié dans le répertoire **LISA_HOME** et remplacez le nom par **site.properties**.
2. Pour modifier le nouveau fichier **site.properties**, changez les propriétés décrites dans la section **Propriétés à configurer** pour qu'elles correspondent à la base de données cible.
3. Lors de la configuration d'une base de données externe prise en charge par DevTest, telle que Oracle, DB2, MySQL ou SQL Server :
 - a. Supprimez les commentaires dans les propriétés suivantes pour cette base de données externe dans la section appropriée.

Par exemple :

```
lisadb.pool.common.driverClass=oracle.jdbc.driver.OracleDriver  
lisadb.pool.common.url
```

```
lisadb.pool.common.url=jdbc:oracle:thin:@HOST:1521:SID
```

- b. Mettez à jour la propriété **lisadb.pool.common.url** avec les valeurs de nom d'hôte, de port et de SID appropriées.

- c. Mettez à jour les propriétés d'utilisateur et de mot de passe suivantes avec les valeurs correctes pour accéder à la base de données :

lisadb.pool.common.user

lisadb.pool.common.password

- d. Commentez les deux propriétés suivantes pour la base de données Derby :

#lisadb.pool.common.driverClass=org.apache.derby.jdbc.ClientDriver

#lisadb.pool.common.url=jdbc:derby://localhost:1528/database/lisa.db;create=true

- e. Définissez la propriété suivante sur false:

lisadb.internal.enabled=false

4. Démarrez le registre ou DevTest Workstation.

Tables ACL

La fonctionnalité de contrôle d'accès (liste de contrôle d'accès) utilise les tables suivantes :

- ACL_ACTIVITIES
- ACL_ACTIVITIES_ITEMS
- ACL_ACTIVITY_LIST_ITEMS
- ACL_ACTIVITY_NUMERIC_LIMITS
- ACL_AUDIT_LOG
- ACL_CUSTOM_ACTIVITY_INFO
- ACL_NUMERIC_LIMITS
- ACL_RESOURCES
- ACL_RESOURCE_GROUPS
- ACL_RESOURCE_GROUPS_RESOURCES
- ACL_RESOURCE_GROUPS_ROLES
- ACL_ROLE_ACTIVITY_ITEM
- ACL_ROLE_CUSTOM_ACT_INFO
- ACL_ROLE_NUMERIC_LIMITS
- ACL_ROLES
- ACL_ROLES_ACTIVITIES
- ACL_USERS
- ACL_USERS_ROLES

Configuration de DevTest pour utiliser DB2

Cette rubrique décrit la procédure de configuration de DevTest pour utiliser une base de données IBM DB2.

La procédure suivante consiste à configurer la version DB2 du fichier **site.properties**. Les propriétés suivantes dans ce fichier s'appliquent à la configuration de la base de données :

```
lisadb.reporting.poolName=common
lisadb.vse.poolName=common
lisadb.acl.poolName=common
lisadb.broker.poolName=common

lisadb.pool.common.driverClass=com.ibm.db2.jcc.DB2Driver
lisadb.pool.common.url=jdbc:db2://HOSTNAME:PORT/DATABASENAME
lisadb.pool.common.user=database_username
lisadb.pool.common.password=database_password

lisadb.pool.common.minPoolSize=0
lisadb.pool.common.initialPoolSize=0
lisadb.pool.common.maxPoolSize=10
lisadb.pool.common.acquireIncrement=1
lisadb.pool.common.maxIdleTime=45
lisadb.pool.common.idleConnectionTestPeriod=5
```

Pour réduire le nombre de connexions à la base de données, la mise en pool de connexions est utilisée. L'implémentation sous-jacente de la fonctionnalité de mise en pool est c3p0. Pour des informations détaillées sur les paramètres, reportez-vous au fichier http://www.mchange.com/projects/c3p0/index.html#configuration_properties. Par défaut, tous les composants utilisent le pool de connexions commun. Toutefois, vous pouvez définir un pool distinct pour chaque composant ou combiner les deux.

Pour la base de données de génération de rapports, il est recommandé de disposer de 10 Go minimum pour des performances optimales. Une base de données pour VSE est requise uniquement si vous utilisez des images héritées créées dans une version antérieure à 6.0.

La valeur de chaque propriété qui finit par **password (mot de passe)** est automatiquement chiffrée lors du démarrage.

Remarque : Les installations à distance de la station de travail DevTest Workstation, du coordinateur, du serveur de simulation, de VSE ou d'un autre composant DevTest distant ne requièrent aucune configuration supplémentaire. Ils reçoivent tous **site.properties** à partir du registre lorsqu'ils se connectent et configurent leur accès à la base de données en conséquence.

Procédez comme suit:

1. Vérifiez que la page de codes de la base de données DB2 est 1208.

2. Vérifiez que la taille de page de la base de données DB2 est d'au moins 8 Ko.
3. Copiez le fichier **db2-site.properties** du répertoire **LISA_HOME\database** vers le répertoire **LISA_HOME**.
4. Remplacez le nom du fichier par **site.properties**.
5. Ouvrez le fichier **site.properties**.
6. Configurez les propriétés de configuration de la base de données.
En général, vous mettez à jour les propriétés suivantes :
 - **lisadb.pool.common.url**
 - **lisadb.pool.common.user**
 - **lisadb.pool.common.password**
7. Le schéma est automatiquement créé dans la base de données lors du premier démarrage du registre. Toutefois, si vous ne voulez pas que l'utilisateur DevTest dispose de droits DBA, vous pouvez créer manuellement le schéma à l'avance. Le fichier **db2.ddl** dans le répertoire **LISA_HOME\database** contient des instructions SQL qui peuvent servir de base pour la création des tables de génération de rapports et des index.
8. Définissez la propriété **lisadb.internal.enabled** sur false.
9. Ajoutez le pilote JDBC pour DB2 aux répertoires **LISA_HOME\lib\shared** et **LISA_HOME\webserver\phoenix\phoenix-1.0.0\WEB-INF\lib**.
Important : Le pilote JDBC doit être ajouté aux deux répertoires.
10. Démarrez le registre.

Configuration de DevTest pour utiliser MySQL

Cette rubrique décrit la procédure de configuration de DevTest pour utiliser une base de données MySQL.

La procédure suivante consiste à configurer la version MySQL du fichier **site.properties**. Les propriétés suivantes dans ce fichier s'appliquent à la configuration de la base de données :

```
lisadb.reporting.poolName=common
lisadb.vse.poolName=common
lisadb.acl.poolName=common
lisadb.broker.poolName=common

lisadb.pool.common.driverClass=com.mysql.jdbc.Driver
lisadb.pool.common.url=jdbc:mysql://DBHOST:DBPORT/DBNAME
lisadb.pool.common.user=database_username
lisadb.pool.common.password=database_password

lisadb.pool.common.minPoolSize=0
lisadb.pool.common.initialPoolSize=0
lisadb.pool.common.maxPoolSize=10
lisadb.pool.common.acquireIncrement=1
lisadb.pool.common.maxIdleTime=45
lisadb.pool.common.idleConnectionTestPeriod=5
```

Pour réduire le nombre de connexions à la base de données, la mise en pool de connexions est utilisée. L'implémentation sous-jacente de la fonctionnalité de mise en pool est c3p0. Pour des informations détaillées sur les paramètres, reportez-vous au fichier http://www.mchange.com/projects/c3p0/index.html#configuration_properties. Par défaut, tous les composants utilisent le pool de connexions commun. Toutefois, vous pouvez définir un pool distinct pour chaque composant ou combiner les deux.

La base de données MySQL doit fournir un classement et un jeu de caractères prenant en charge le codage UTF-8 ; les caractères à deux octets sont stockés dans la liste de contrôle d'accès (ACL) et les tables de génération de rapports. La page de codes par défaut pour la base de données doit être codée en UTF-8 ; la définition de votre base de données uniquement en UTF-8 n'est pas suffisante. Si le codage de la base de données MySQL n'est pas UTF-8, des erreurs d'exécution se produiront.

Pour la base de données de génération de rapports, il est recommandé de disposer de 10 Go minimum pour des performances optimales. Une base de données pour VSE est requise uniquement si vous utilisez des images héritées créées dans une version antérieure à 6.0.

La valeur de chaque propriété qui finit par **password (mot de passe)** est automatiquement chiffrée lors du démarrage.

Remarque : Les installations à distance de la station de travail DevTest Workstation, du coordinateur, du serveur de simulation, de VSE ou d'un autre composant DevTest distant ne requièrent aucune configuration supplémentaire. Ils reçoivent tous **site.properties** à partir du registre lorsqu'ils se connectent et configurent leur accès à la base de données en conséquence.

Procédez comme suit:

1. Copiez le fichier **mysql-site.properties** du répertoire **LISA_HOME\database** vers le répertoire **LISA_HOME**.
2. Remplacez le nom du fichier par **site.properties**.
3. Ouvrez le fichier **site.properties**.
4. Configurez les propriétés de configuration de la base de données.

En général, vous mettez à jour les propriétés suivantes :

- **lisadb.pool.common.url**
 - **lisadb.pool.common.user**
 - **lisadb.pool.common.password**
5. Le schéma est automatiquement créé dans la base de données lors du premier démarrage du registre. Toutefois, si vous ne voulez pas que l'utilisateur DevTest dispose de droits DBA, vous pouvez créer manuellement le schéma à l'avance. Le fichier **mysql.ddl** dans le répertoire **LISA_HOME\database** contient des instructions SQL qui peuvent servir de base pour la création des tables de génération de rapports et des index.
 6. Définissez la propriété **lisadb.internal.enabled** sur false.
 7. Ajoutez le pilote JDBC pour MySQL aux répertoires **LISA_HOME\lib\shared** et **LISA_HOME\webserver\phoenix\phoenix-1.0.0\WEB-INF\lib**. La version minimum du pilote JDBC MySQL est 5.1.25.

Important : Le pilote JDBC doit être ajouté aux deux répertoires.

8. Démarrez le registre.

Configuration de DevTest pour utiliser Oracle

Cette rubrique décrit la procédure de configuration de DevTest pour utiliser une base de données Oracle.

La procédure suivante consiste à configurer la version Oracle du fichier **site.properties**. Les propriétés suivantes dans ce fichier s'appliquent à la configuration de la base de données :

```
lisadb.reporting.poolName=common
lisadb.vse.poolName=common
lisadb.acl.poolName=common
lisadb.broker.poolName=common

lisadb.pool.common.driverClass=oracle.jdbc.driver.OracleDriver
lisadb.pool.common.url=jdbc:oracle:thin:@HOST:1521:SID
lisadb.pool.common.user=oracle_username
lisadb.pool.common.password=oracle_password

lisadb.pool.common.minPoolSize=0
lisadb.pool.common.initialPoolSize=0
lisadb.pool.common.maxPoolSize=10
lisadb.pool.common.acquireIncrement=1
lisadb.pool.common.maxIdleTime=45
lisadb.pool.common.idleConnectionTestPeriod=5
```

Pour réduire le nombre de connexions à la base de données, la mise en pool de connexions est utilisée. L'implémentation sous-jacente de la fonctionnalité de mise en pool est c3p0. Pour des informations détaillées sur les paramètres, reportez-vous au fichier http://www.mchange.com/projects/c3p0/index.html#configuration_properties. Par défaut, tous les composants utilisent le pool de connexions commun. Toutefois, vous pouvez définir un pool distinct pour chaque composant ou combiner les deux.

Pour la base de données de génération de rapports, il est recommandé de disposer de 10 Go minimum pour des performances optimales. Une base de données pour VSE est requise uniquement si vous utilisez des images héritées créées dans une version antérieure à 6.0.

La valeur de chaque propriété qui finit par **password (mot de passe)** est automatiquement chiffrée lors du démarrage.

Remarque : Les installations à distance de la station de travail DevTest Workstation, du coordinateur, du serveur de simulation, de VSE ou d'un autre composant DevTest distant ne requièrent aucune configuration supplémentaire. Ils reçoivent tous **site.properties** à partir du registre lorsqu'ils se connectent et configurent leur accès à la base de données en conséquence.

Procédez comme suit:

1. Vérifiez que le jeu de caractères de la base de données Oracle prend en charge le codage Unicode.
2. Copiez le fichier **oracle-site.properties** du répertoire **LISA_HOME\database** vers le répertoire **LISA_HOME**.
3. Remplacez le nom du fichier par **site.properties**.
4. Ouvrez le fichier **site.properties**.
5. Configurez les propriétés de configuration de la base de données.

En général, vous mettez à jour les propriétés suivantes :

- **lisadb.pool.common.url**
- **lisadb.pool.common.user**
- **lisadb.pool.common.password**

Pour la propriété **lisadb.pool.common.url**, vous pouvez utiliser le nom de service.

6. Le schéma est automatiquement créé dans la base de données lors du premier démarrage du registre. Toutefois, si vous ne voulez pas que l'utilisateur DevTest dispose de droits DBA, vous pouvez créer manuellement le schéma à l'avance. Le fichier **oracle.ddl** dans le répertoire **LISA_HOME\database** contient des instructions SQL qui peuvent servir de base pour la création des tables de génération de rapports et des index.
7. Définissez la propriété **lisadb.internal.enabled** sur **false**.
8. Ajoutez le pilote JDBC pour Oracle aux répertoires **LISA_HOME\lib\shared** et **LISA_HOME\webserver\phoenix\phoenix-0.0\WEB-INF\lib**.

Vous pouvez télécharger le pilote à partir de

<http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html>.

Il est recommandé de télécharger la dernière version du pilote, même si vous utilisez un serveur de base de données antérieur. Dans la plupart des cas, **ojdbc7.jar** est le pilote correct pour Java 1.7 (fourni avec DevTest). Si vous utilisez Java 1.6, utilisez **ojdbc6.jar**. Si vous utilisez Java 1.5, utilisez **ojdbc5.jar**.

Important : Le pilote JDBC doit être ajouté aux deux répertoires.

9. Démarrez le registre.

Configuration de DevTest pour utiliser SQL Server

Cette rubrique décrit la procédure de configuration de DevTest pour utiliser une base de données Microsoft SQL Server.

La procédure suivante consiste à configurer la version SQL Server du fichier **site.properties**. Les propriétés suivantes dans ce fichier s'appliquent à la configuration de la base de données :

```
lisadb.reporting.poolName=common
lisadb.vse.poolName=common
lisadb.acl.poolName=common
lisadb.broker.poolName=common

lisadb.pool.common.driverClass=com.microsoft.sqlserver.jdbc.SQLServerDriver
lisadb.pool.common.url=jdbc:sqlserver://SERVER:PORT;databaseName=DATABASENAME
lisadb.pool.common.user=database_username
lisadb.pool.common.password=database_password

lisadb.pool.common.minPoolSize=0
lisadb.pool.common.initialPoolSize=0
lisadb.pool.common.maxPoolSize=10
lisadb.pool.common.acquireIncrement=1
lisadb.pool.common.maxIdleTime=45
lisadb.pool.common.idleConnectionTestPeriod=5
```

Pour réduire le nombre de connexions à la base de données, la mise en pool de connexions est utilisée. L'implémentation sous-jacente de la fonctionnalité de mise en pool est c3p0. Pour des informations détaillées sur les paramètres, reportez-vous au fichier http://www.mchange.com/projects/c3p0/index.html#configuration_properties. Par défaut, tous les composants utilisent le pool de connexions commun. Toutefois, vous pouvez définir un pool distinct pour chaque composant ou combiner les deux.

Pour la base de données de génération de rapports, il est recommandé de disposer de 10 Go minimum pour des performances optimales. Une base de données pour VSE est requise uniquement si vous utilisez des images héritées créées dans une version antérieure à 6.0.

La valeur de chaque propriété qui finit par **password (mot de passe)** est automatiquement chiffrée lors du démarrage.

Remarque : Les installations à distance de la station de travail DevTest Workstation, du coordinateur, serveur de simulation, du VSE, ou d'un autre composant DevTest distant ne requièrent aucune configuration supplémentaire. Ils reçoivent tous **site.properties** à partir du registre lorsqu'ils se connectent et configurent leur accès à la base de données en conséquence.

Procédez comme suit:

1. Copiez le fichier **sqlserver-site.properties** du répertoire **LISA_HOME\database** vers le répertoire **LISA_HOME**.
2. Remplacez le nom du fichier par **site.properties**.
3. Ouvrez le fichier **site.properties**.
4. Configurez les propriétés de configuration de la base de données.
En général, vous mettez à jour les propriétés suivantes :
 - **lisadb.pool.common.url**
 - **lisadb.pool.common.user**
 - **lisadb.pool.common.password**
5. Le schéma est automatiquement créé dans la base de données lors du premier démarrage du registre. Toutefois, si vous ne voulez pas que l'utilisateur DevTest dispose de droits DBA, vous pouvez créer manuellement le schéma à l'avance. Le fichier **sqlserver.ddl** dans le répertoire **LISA_HOME\database** contient des instructions SQL qui peuvent servir de base pour la création des tables de génération de rapports et des index.
6. Définissez la propriété **lisadb.internal.enabled** sur false.
7. Ajoutez le pilote JDBC pour SQL Server aux répertoires **LISA_HOME\lib\shared** et **LISA_HOME\webserver\phoenix\phoenix-x.0.0\WEB-INF\lib**.
Important : Le pilote JDBC doit être ajouté aux deux répertoires.
8. Démarrez le registre.

Configuration de la base de données de tableau de bord Enterprise Dashboard externe

Le tableau de bord Enterprise Dashboard utilise une base de données Derby interne par défaut. Il est recommandé d'utiliser une base de données externe à la place.

Procédez comme suit:

1. Connectez-vous au serveur sur lequel le tableau de bord Enterprise Dashboard est installé.
2. Accédez à LISA_HOME et ouvrez le fichier lisa.properties.
3. Recherchez les lignes suivantes dans la section Enterprise Dashboard Options (Options du tableau de bord Enterprise Dashboard), qui spécifie si la base de données Derby interne doit être utilisée dans le tableau de bord Enterprise Dashboard.

```
# Should we start the internal Derby DB instance in the Enterprise Dashboard?  
dradisdb.internal.enabled=true
```
4. Définissez la valeur sur false.

```
dradisdb.internal.enabled=false
```
5. Commentez les propriétés suivantes.

```
# Internal Derby DB network interface to use (0,0,0,0 == all network interfaces)  
#dradisdb.internal.host=0.0.0.0  
# Internal Derby DB port number to use  
#dradisdb.internal.port=1530
```
6. Pour utiliser une **base de données Oracle**, modifiez les propriétés suivantes pour définir des valeurs sur une base de données externe comme suit :

```
lisadb.pool.dradis.driverClass=oracle.jdbc.driver.OracleDriver  
lisadb.pool.dradis.url=jdbc:oracle:thin:10.130.150.36:1521:ORCL  
lisadb.pool.dradis.user=dradis21  
lisadb.pool.dradis.password=dradis21
```
7. Pour utiliser une base de données **SQL Server**, modifiez les propriétés suivantes pour définir des valeurs sur une base de données externe comme suit :

```
lisadb.pool.dradis.driverClass=com.microsoft.sqlserver.jdbc.SQLServerDriver  
lisadb.pool.dradis.url=jdbc:sqlserver://SERVER:PORT;databaseName=DATABASENAME  
lisadb.pool.dradis.user=dradis21  
lisadb.pool.dradis.password=dradis21
```
8. Pour utiliser une base de données **MySQL**, modifiez les propriétés suivantes pour définir des valeurs sur une base de données externe comme suit :

```
lisadb.pool.dradis.driverClass=com.mysql.jdbc.Driver  
lisadb.pool.dradis.url=jdbc:mysql://DBHOST:DBPORT/DBNAME  
lisadb.pool.dradis.user=dradis21  
lisadb.pool.dradis.password=dradis21
```
9. Copiez les propriétés modifiées pour le type de votre base de données externe dans les étapes 6, 7, ou 8.

10. Enregistrez le fichier lisa.properties.
11. Ouvrez local.properties et collez les lignes copiées à la fin du fichier.
12. Enregistrez le fichier local.properties.

Maintenance de la base de données

Vous pouvez utiliser différentes propriétés pour la gestion de la quantité de données dans la base de données.

- Pour plus d'informations sur les propriétés de génération de rapports, reportez-vous à la section [Maintenance de la génération de rapports automatique](#) (page 54).
- Pour plus d'informations sur les propriétés de contrôle d'accès (ACL), consultez la section [Suppression automatique d'entrées du journal d'audit](#) (page 56).
- Pour plus d'informations sur les propriétés de CA Continuous Application Insight, reportez-vous aux sections [Suppression automatique de transactions](#) (page 56) et [Suppression automatique de scénarios](#) (page 57).

Maintenance de la génération de rapports automatique

Deux processus exécutés en arrière-plan affectent la génération de rapports :

- Performance Summary Calculator (Calculatrice de récapitulatif de performances)
- Report Cleaner (Processus de nettoyage de rapports)

Performance Summary Calculator (Calculatrice de récapitulatif de performances)

Ce processus permet de calculer les statistiques d'une exécution de test ou de suite. La plupart des graphiques dans le portail de génération de rapports dépendent de ce processus ; vous ne pouvez donc pas le désactiver. Vous pouvez modifier la planification de la calculatrice de récapitulatif de performances en changeant les propriétés suivantes :

rpt.summary.initDelayMin=7

Détermine la durée d'attente en minutes après le démarrage du registre avant le démarrage de ce processus.

rpt.summary.pulseMin=1

Détermine la durée d'attente entre les exécutions du processus.

Report Cleaner (Processus de nettoyage de rapports)

Ce processus est chargé de supprimer les rapports expirés exécutés à partir de la base de données.

perfmgr.rvwiz.whatrpt.autoExpire=true

Vous pouvez activer ou désactiver le processus de nettoyage de rapports en définissant la propriété suivante. S'il est désactivé, le processus de nettoyage de rapports n'est pas exécuté et les autres propriétés ne s'appliqueront pas.

perfmgr.rvwiz.whatrpt.expireTimer=30d

Définit la valeur d'expiration d'une suite ou d'un test. Lorsqu'une suite (ou un test) est plus ancienne que cette valeur, elle (ou le test) sera supprimée. La valeur de la propriété est un nombre suivi d'un suffixe. Les suffixes suivants sont valides, **t** étant la valeur par défaut :

- t=millisecondes
- s=seconde
- m=minutes
- h=heures
- d=jours

■ w=semaines

Tenez compte du fait que les tests et les suites sont supprimés environ au même moment du jour de leur création. L'ajout de plusieurs heures peuvent réduire la suppression de processus exécutés pendant le jour. Toutefois, il n'existe aucune manière absolue d'assurer les heures d'exécution d'un processus de suppression.

perfmgr.rvwiz.whatrpt.forceCompleteTimer=24h

Permet de forcer la finalisation d'un test (dans la base de données de génération de rapports). Certaines suites ou certains tests dont la finalisation correcte échoue ne sont jamais marqués comme finished (terminé) dans la base de données. Les tests non marqués finished (terminés) ne seront pas supprimés par le processus de nettoyage de rapports et n'effectuent aucun calcul de récapitulatif de performances. Un test plus ancien que cette valeur sera marqué comme terminé dans la base de données. Les tests terminés seront supprimés de la base de données uniquement lorsque la valeur expireTimer est prise en compte. Si vous avez des tests qui s'exécutent pendant une durée supérieure à 24 heures par défaut, augmentez la valeur de ce processus.

Vous pouvez modifier la planification du processus de nettoyage de rapports en changeant les propriétés suivantes :

rpt.cleaner.initDelayMin=10

Détermine la durée d'attente en minutes après le démarrage du registre avant le démarrage de ce processus.

rpt.cleaner.pulseMin=60

Détermine la durée d'attente entre les exécutions du processus.

Suppression automatique d'entrées du journal d'audit

La fonction access control (ACL) (Liste de contrôle d'accès) stocke le [journal d'audit](#) (page 131) dans la base de données de DevTest. De manière régulière, le registre exécute un processus pour supprimer d'anciennes entrées du journal d'audit de la base de données.

Les propriétés suivantes contrôlent ce comportement :

`lisa.acl.audit.logs.delete.frequency`

Spécifie la fréquence d'exécution du processus de suppression automatique. La valeur par défaut est **1d**, c'est-à-dire que le processus s'exécute une fois par jour. Les unités de temps valides sont d, h, m et s (d pour jours, h pour heures, m pour minutes et s pour secondes).

`lisa.acl.audit.logs.delete.age`

Spécifie l'ancienneté minimum des entrées de journal d'audit que le processus de suppression automatique doit supprimer. La valeur par défaut est 30d, c'est-à-dire que les entrées seront considérées comme anciennes après 30 jours. Les unités de temps valides sont d, h, m et s (d pour jours, h pour heures, m pour minutes et s pour secondes).

La valeur par défaut de chaque propriété est disponible dans le fichier **`lisa.properties`**. Si vous voulez changer la valeur par défaut, ajoutez la propriété au fichier **`local.properties`**.

Suppression automatique de transactions

Vous pouvez configurer CA Continuous Application Insight pour supprimer automatiquement d'anciennes transactions de la base de données DevTest.

Par défaut, la suppression automatique des transactions est activée.

Les propriétés disponibles sont les suivantes :

Enable cleaner (Activer le nettoyeur)

Permet d'activer la suppression automatique des transactions.

Cleanup frequency (Fréquence de nettoyage)

Spécifie la fréquence à laquelle le processus de nettoyage s'exécute. La valeur est exprimée en minutes.

Maximum age (Ancienneté maximum)

Spécifie l'ancienneté des transactions que le processus de nettoyage supprime. La valeur est exprimée en minutes.

Vous pouvez configurer ces propriétés dans la fenêtre Agents du portail DevTest. Les propriétés s'affichent dans l'onglet Settings (Paramètres).

Suppression automatique de scénarios

Vous pouvez configurer CA Continuous Application Insight pour supprimer automatiquement d'anciens scénarios de la base de données DevTest.

Par défaut, la suppression automatique des scénarios est activée.

Les propriétés disponibles sont les suivantes :

Enable cleaner (Activer le nettoyeur)

Permet d'activer la suppression automatique des scénarios.

Cleanup frequency (Fréquence de nettoyage)

Spécifie la fréquence à laquelle le processus de nettoyage s'exécute. La valeur est exprimée en minutes.

Maximum age (Ancienneté maximum)

Spécifie l'ancienneté des scénarios que le processus de nettoyage supprime. La valeur est exprimée en minutes.

Vous pouvez configurer ces propriétés dans la fenêtre Agents du portail DevTest. Les propriétés s'affichent dans l'onglet Settings (Paramètres).

Chapitre 3: Administration de licence

Ce chapitre traite des sujets suivants :

[Licence Honor-Based \(Basée sur honneur\)](#) (page 59)

[Fonctionnement de l'interaction entre les licences, les listes de contrôle d'accès et les rapports d'audit](#) (page 61)

[Rapport d'audit d'utilisation de DevTest Solutions](#) (page 64)

[Exemple de calcul de nombre](#) (page 67)

[Types d'utilisateurs](#) (page 68)

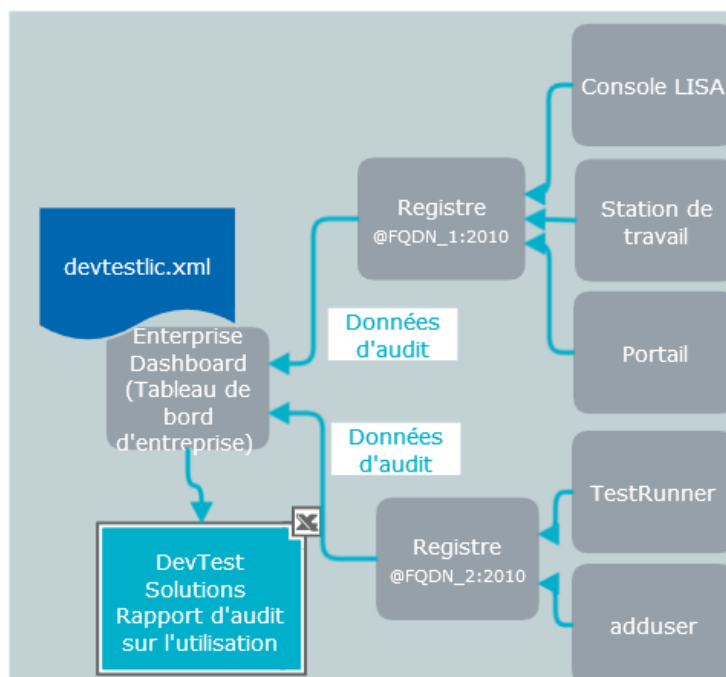
Licence Honor-Based (Basée sur honneur)

Présentation de la licence Honor-Based (Basée sur honneur)

- Le contrat de licence repose sur un nombre maximum de sessions d'utilisateur simultanées autorisées par type d'utilisateur. Si vous avez des questions concernant votre contrat de licence spécifique, contactez votre équipe chargée de votre compte.
- La licence est basée sur des fichiers, l'un d'eux étant destiné à l'entreprise. Ce fichier active DevTest Solutions lors du premier démarrage à l'issue de l'installation.
- Les serveurs Local License Server (LLS) et Internet Based License Server ne sont plus pris en charge pour DevTest Solutions 8.0.
- Les données d'utilisation simultanée par type d'utilisateur sont automatiquement collectées.
- Le tableau de bord Enterprise Dashboard génère des rapports sur l'utilisation de la licence.
- Un rapport d'audit d'utilisation, qui indique l'utilisation simultanée maximum par type d'utilisateur, est un outil qui permet d'évaluer la conformité au contrat de licence. Les utilisateurs disposant de droits d'administration peuvent accéder à ce rapport.

Pour plus d'informations, consultez la section [Fonctionnement de l'interaction entre les licences, les listes de contrôle d'accès et les rapports d'audit](#) (page 61).

Le diagramme suivant illustre l'activation de DevTest Solutions à l'aide d'un fichier de licence stocké avec le tableau de bord Enterprise Dashboard. Les registres collectent les données d'audit à partir des interfaces utilisateur et des interfaces de ligne de commande auxquelles les utilisateurs se connectent, y compris la console DevTest, la Workstation (Station de travail), le portail et les utilitaires de ligne de commande tels que TestRunner (Exécuteur de tests) et adduser (Ajout d'utilisateurs). Les registres transmettent les données d'audit au tableau de bord Enterprise Dashboard. Les administrateurs peuvent générer un rapport d'audit d'utilisation de DevTest Solutions pour vérifier la conformité au contrat de licence.



Fonctionnement de l'interaction entre les licences, les listes de contrôle d'accès et les rapports d'audit

La rubrique inclut les sections suivantes :

- Contrat de licence basé sur l'utilisation
- Activation de la licence basée sur des fichiers
- Activation de liste de contrôle d'accès
- Conformité basée sur l'honneur
- Collecte continue de données d'utilisation par type d'utilisateur
- Rapport d'audit d'utilisation

Usage-Based License Agreement

Votre contrat de licence avec CA Technologies est basé sur le nombre maximum de sessions d'utilisateur simultanées par type d'utilisateur. Les types d'utilisateur sont les suivants :

- Runtime User (Utilisateur d'exécution)
- Test Power User (Utilisateur avancé de test)
- SV Power User (Utilisateur avancé SV)
- CAI Power User (Utilisateur avancé CAI)

Chaque activité réalisable par un utilisateur avec DevTest Solutions correspond à une autorisation. Chaque autorisation est associée à un rôle ; chaque rôle est associé à un type d'utilisateur. Les administrateurs affectent les autorisations aux utilisateurs.

Activation de la licence

L'activation de licence de DevTest Solutions est basée sur un fichier. CA Technologies vous fournit un fichier de licence (devtestlic.xml). Lors de l'installation ou de la mise à niveau de DevTest Solutions, l'assistant d'installation place le fichier dans le répertoire LISA_HOME de l'hôte sur lequel le tableau de bord Enterprise Dashboard est installé. Les installations ultérieures du composant de serveur (DevTest Server) référencent l'URL du tableau de bord Enterprise Dashboard. La licence est activée lors du premier démarrage du tableau de bord Enterprise Dashboard et des registres. Aucun autre composant ne requiert l'activation de la licence.

Si vous procédez à une mise à niveau, demandez une nouvelle licence devtestlic.xml auprès de CA Technologies. Le processus de génération de clés de licence actuel est utilisé pour générer une clé de produit livrée via le fichier devtestlic.xml. Cette clé est utilisée pour activer ou déverrouiller le tableau de bord Enterprise Dashboard.

Activation de liste de contrôle d'accès

La liste de contrôle d'accès est activée par défaut. Avant de pouvoir accéder à DevTest Solutions, les utilisateurs doivent être authentifiés avec des informations d'identification valides, puis être autorisés à effectuer les tâches associées à leur rôle. L'onglet Administration de la console de serveur permet de définir un nom d'utilisateur, un mot de passe et un rôle composé d'un ensemble d'autorisations pour chaque utilisateur. Les rôles sont liés aux types d'utilisateur.

Les utilisateurs doivent se connecter à l'aide d'informations d'identification valides pour accéder à une interface utilisateur ou une interface de ligne de commande. Lorsqu'un utilisateur ouvre la station de travail, accède au portail, ou à la console DevTest, une boîte de dialogue de connexion s'ouvre. L'utilisateur se connecte à l'aide des informations d'identification définies dans DevTest ou dans LDAP, si vous avez configuré DevTest pour utiliser des informations d'identification LDAP. Si les informations d'identification saisies correspondent à celles d'un utilisateur autorisé, l'interface utilisateur s'ouvre. Les fonctionnalités présentées à l'utilisateur reposent sur les autorisations accordées à cet utilisateur.

Dans le cas de la rétrocompatibilité, il existe une exception. Même lorsque la liste de contrôle d'accès est activée, les utilisateurs autorisés peuvent exécuter des tests et démarrer des services virtuels sans spécifier un nom d'utilisateur et un mot de passe de connexion valides.

Remarque : Il est recommandé de [modifier les mots de passe des utilisateurs](#) (page 123) standard de sorte que seuls les utilisateurs authentifiés puissent accéder à DevTest Solutions.

Conformité basée sur l'honneur

Le client est responsable de la conformité de l'utilisation de la licence aux conditions du contrat. La licence émise n'applique pas l'accès simultané maximum par type d'utilisateur. Comme indiqué dans la section Rapport d'audit d'utilisation, les rapports d'audit d'utilisation DevTest Solutions sont envoyés à CA Technologies sur demande. Le responsable des ventes CA peut vous contacter pour évaluer votre intérêt quant au développement de votre accord d'achat si les rapports d'audit indiquent que l'utilisation simultanée d'un type d'utilisateur dépasse ce contrat.

Les clients qui souhaitent évaluer les fonctionnalités qu'ils n'ont pas acquises doivent contacter l'équipe chargée de leur compte pour obtenir une version d'évaluation Preuve de concept, ou aborder des questions relatives aux nouvelles fonctionnalités. Tout dossier d'assistance qui serait déclenché à propos de fonctionnalités de produit non achetées sera considéré comme non pertinent.

Collecte continue de données d'utilisation par type d'utilisateur

Lorsque les utilisateurs se connectent à l'une des interfaces utilisateur ou de ligne de commande de DevTest Solutions, chaque registre capture les données de session par type d'utilisateur et les envoie au tableau de bord Enterprise Dashboard au début de chaque heure. Si la connexion entre les registres et le tableau de bord Enterprise Dashboard est perdue, les données d'audit d'utilisation seront accumulées dans les registres jusqu'au rétablissement de la connexion. Le tableau de bord Enterprise Dashboard compile les données d'utilisation dans l'entreprise et compte les sessions simultanées par type d'utilisateur.

Rapport d'audit d'utilisation

Régulièrement, un administrateur se connecte au tableau de bord Enterprise Dashboard et génère le rapport d'audit d'utilisation pour une période spécifique. Les données d'interfaces utilisateur ou de ligne de commande spécifiques auxquelles les utilisateurs se connectent y sont consignées. Les sessions simultanées comptant le nombre maximum d'utilisateurs d'un type spécifiques sont utilisées dans les calculs du rapport. Le rapport ajoute les nombres d'utilisation simultanée par type d'utilisateur dans les registres. Pour chaque type d'utilisateur comportant des données, le générateur de rapports crée un onglet avec des détails supplémentaires. Vous pouvez comparer les informations d'accès détaillées dans les rapports d'audit au contrat de licence pour déterminer le niveau de conformité. Vous pouvez évaluer ce rapport au regard de votre contrat de licence pour vérifier la conformité ou déterminer si une mise à niveau de votre contrat est nécessaire.

Rapport d'audit d'utilisation de DevTest Solutions

Un rapport d'audit d'utilisation de DevTest Solutions est généré au format de classeur Excel avec les onglets suivants :

- Premier onglet : Overview (Présentation)
- Onglets de types d'utilisateur : Admin User (Administrateur), PF Power User (Utilisateur avancé PF), SV Power User (Utilisateur avancé SV), Test User (Utilisateur test), Runtime User (Utilisateur d'exécution)

Un onglet est créé pour chaque type d'utilisateur et contient toutes les activités réalisées pendant la période, qu'il s'agisse d'utilisation simultanée ou unique. Bien que l'administrateur soit inclus dans le rapport, il n'est pas nécessaire de le prendre en compte lors de l'évaluation de la conformité à votre contrat de licence.

- Dernier onglet : Component by User (Composant par utilisateur), comprenant une colonne pour chaque interface utilisateur ou interface de ligne de commande indiquant l'accès pendant cette période. Les entrées de cet onglet ne représentent pas nécessairement l'accès simultané.

Présentation

L'onglet Overview (Présentation) fournit des détails sur l'étendue de l'utilisation du nombre d'utilisateurs actuels de chaque type autorisé par la licence octroyée à une entreprise. Un rapport spécifique fournit des données à partir de tous les registres pour une plage de dates spécifique. Les données Count (Nombre) sont indiquées par type d'utilisateur.

Informations sur le rapport

La section Report information (Informations sur le rapport) répertorie des informations de licence et la plage de dates pour ce rapport d'audit.

- Company (Société) : nom de la société qui a généré ce rapport.
- Key ID (ID de clé) : L'identificateur de la clé de licence
- Expiration : date d'expiration de la licence
- Reporting Period Start (Début de la période du rapport) : date de début de ce rapport
- Reporting Period End (Fin de la période du rapport) : date de fin de ce rapport

User Type and Count (Type et nombre d'utilisateurs)

Les types d'utilisateur indiqués incluent PF Power User (Utilisateur avancé PF), SV Power User (Utilisateur avancé SV), Test User (Utilisateur test) et Runtime User (Utilisateur d'exécution). L'administrateur est également indiqué, même s'il n'est pas considéré comme un type d'utilisateur au titre de la licence.

Si l'utilisateur se voit accorder des autorisations associées à plusieurs types d'utilisateur, le type d'utilisateur le plus élevé sera utilisé. La hiérarchie de types d'utilisateur se présente comme suit (ordre décroissant) :

- a. PF Power User (Utilisateur avancé PF) ou SV Power User (Utilisateur avancé SV) (types d'utilisateur équivalent)
- b. Test Power User (Utilisateur avancé de test)
- c. Runtime User (Utilisateur d'exécution)
- d. Admin User (Administrateur)

Consultez la section [Types d'utilisateur](#) (page 68).

Tous les registres collectent de manière continue des données d'utilisation à partir des services qui prennent en charge les interfaces utilisateur et les interfaces de ligne de commande. Les données brutes sont conservées à des fins d'utilisation simultanée par le même type d'utilisateur dans l'entreprise, où les sessions de connexion simultanées sont enregistrées par registre.

L'utilisation simultanée se produit lorsque deux ou plusieurs utilisateurs du même type accèdent à une interface utilisateur DevTest ou une interface de ligne de commande DevTest et que leurs sessions coïncident dans le temps.

Les calculs de nombre pour le rapport sont basés sur les nombres de groupes pour lesquels le nombre maximum de sessions simultanées est atteint. Les écarts Min, Max et Standard transmettent la répartition aux registres.

Consultez la section [Exemple de calcul de nombre](#) (page 67).

Onglets de types d'utilisateur (Admin User (Administrateur), PF Power User (Utilisateur avancé PF), SV Power User (Utilisateur avancé SV), Test User (Utilisateur test), Runtime User (Utilisateur d'exécution))

Chaque onglet Type d'utilisateur indique les mesures et les statistiques sur des groupes d'accès simultané ayant atteint le nombre maximum de sessions simultanées pendant la période du rapport.

- Average (Moyenne) :
 - La moyenne est calculée pour chaque registre qui fait partie du groupe d'accès simultané.
 - Le total concerne le type d'utilisateur. Cette valeur s'affiche également sur la page Overview (Présentation).
- STDEV : écart calculé pour chaque échantillon de registres défini
- Minimum : Valeur la plus faible pour chaque échantillon de registres défini
- Maximum : Valeur la plus élevée pour chaque échantillon de registres défini

Component By User (Composant par utilisateur)

L'onglet Component By User (Composant par utilisateur) indique les données de session d'utilisateur issues de chaque registre connecté au tableau de bord Enterprise Dashboard.

Registre

Les noms de registre sont au format suivant :

registry@FQDN:2010

User name (Nom d'utilisateur)

Noms des utilisateurs qui se sont connectés à une interface utilisateur ou une interface de ligne de commande pendant au moins une session.

Type d'utilisateur

Type d'utilisateur affecté à l'utilisateur associé. Les types d'utilisateur sont affichés comme suit :

- ADMIN_USER
- PF_POWER_USER
- SV_POWER_USER
- TEST_POWER_USER
- SVT_RUNTIME_USER

Total sessions

Somme des nombres à partir des colonnes signalées pour l'utilisateur associé, les colonnes représentant une session d'interface utilisateur ou une session d'interface de ligne de commande. Les interfaces utilisateur incluent la console DevTest, la station de travail DevTest Workstation et le portail. Les exemples d'interfaces de ligne de commande incluent AddUser (Ajout d'utilisateur) et TestRunner (Exécuteur de tests). Les colonnes peuvent varier en fonction des rapports, selon les éléments auxquelles les utilisateurs sont connectés. Voici quelques exemples :

- Add User (Ajout d'utilisateur) : nombre d'initialisations de l'utilitaire de ligne de commande adduser par cet utilisateur
- Console : nombre de connexions à la console DevTest par cet utilisateur pour ce registre
- Workstation (Station de travail) : nombre d'ouvertures d'une station de travail DevTest Workstation, de connexions à celle-ci et de connexions au registre associé par cet utilisateur
- Portail (Portail) : nombre d'accès et de connexion à `http://hostname:1507/devtest` par cet utilisateur pour ce registre

Remarque : Pour plus d'informations sur la génération de ce rapport, reportez-vous à la section [Exportation des données d'audit d'utilisation](#) (page 172).

Exemple de calcul de nombre

Le calcul de Count (Nombre) pour le [rapport d'audit d'utilisation de DevTest Solutions](#) (page 64) est un processus comprenant trois étapes.

1. Lorsqu'un accès simultané est détecté dans l'entreprise, un nombre de groupe est enregistré pour tous les registres impliqués. Examinez l'exemple suivant pour le groupe d'utilisateurs Test Power User (Utilisateur avancé Test).
2. A des fins de génération de rapports, les nombres de groupe avec le nombre d'accès simultané maximum sont utilisés. Dans cet exemple, les lignes grisées (1, 3 et 4) sont utilisées.

Test Power User (Utilisateur avancé de test)				
Timestamp (Horodatage)	Registre 1	Registre 2	Registre 3	Nombre de groupes
1	1	0	3	4
2	0	0	2	2
3	1	2	1	4
4	0	0	4	4
5	1	1	1	3

3. Une fois les données de nombre de groupe maximum par registre identifiées, la moyenne des nombres par registre est calculée. Les valeurs des nombres minimum et maximum sont stockées. Ces trois valeurs (moyenne, minimum, et maximum) s'affichent dans le rapport.

Test Power User (Utilisateur avancé de test)						
Registre	Nombre 1	Nombre 2	Nombre 3	Moy	Min	Max
Registre 1	1	1	0	0.67	0	1
Registre 2	0	2	0	0.67	0	2
Registre 3	3	1	4	2.67	1	4
TOTAL				4	1	7

Ces données sont résumées sur la page Overview (Présentation) du rapport comme Use Type (Type d'utilisateur) et Count (Nombre). Les données de Count (Nombre) affichées sont combinées pour chaque type d'utilisateur. Les données sont calculées en tenant compte de la moyenne du total des nombres maximum et minimum dans les registres de l'échantillon pour chaque type d'utilisateur. Ce nombre représente le nombre de sessions simultanées maximum pour ce type d'utilisateur, car l'échantillon est composé uniquement des nombres de groupe avec l'accès simultané maximum.

Type d'utilisateur	Count (Nombre)
Test Power User (Utilisateur avancé de test)	4

Types d'utilisateurs

La liste de contrôle d'accès a les types d'utilisateur suivants :

- PF Power User (Utilisateur avancé PF)
- SV Power User (Utilisateur avancé SV)
- Test Power User (Utilisateur avancé de test)
- Runtime User (Utilisateur d'exécution)

Remarque : Le type d'utilisateur Admin User (Administrateur), affiché dans la page Roles comme combinaison PF Power User (Utilisateur avancé PF) et SV Power User (Utilisateur avancé SV), n'est pas pris en compte dans la licence. Toutefois, l'administrateur est inclus dans le Rapport d'audit d'utilisation de DevTest Solutions à titre informatif.

Un utilisateur peut être associé à un ou plusieurs rôles. Chaque rôle est associé à un seul type d'utilisateur. Par exemple, le type d'utilisateur Runtime User (Utilisateur d'exécution) a trois rôles (Administrateur système, exécution et invité), mais le rôle Runtime (Exécution) est uniquement associé au type Runtime User (Utilisateur d'exécution).

Un utilisateur peut recevoir un ou plusieurs rôles. Dans le cas de rôles multiples, le rôle associé au type d'utilisateur le plus élevé sera utilisé à des fins d'audit d'utilisation. La hiérarchie de types d'utilisateur se présente comme suit :

- Les utilisateurs PF Power User (Utilisateur avancé PF) et SV Power User (Utilisateur avancé SV) sont égaux dans la hiérarchie et les deux sont les plus élevés.
- L'utilisateur Test Power User (Utilisateur avancé de test) est inférieur au PF Power User (Utilisateur avancé PF) et au SV Power User (Utilisateur avancé SV), mais supérieur au Runtime User (Utilisateur d'exécution).
- L'utilisateur Runtime User (Utilisateur d'exécution) est le type le plus faible.

Exemple de méthode permettant de déterminer le type d'utilisateur à des fins d'audit

Les autorisations associées à un rôle affecté à un utilisateur déterminent les tâches qu'un utilisateur est autorisé à effectuer. Un administrateur peut affecter un ou plusieurs rôles à un utilisateur. En général, les administrateurs affectent un seul rôle à chaque utilisateur, car les autorisations des rôles intégrés sont affectées en tenant compte de la hiérarchie de types d'utilisateur. Par exemple, le rôle PF Power User (Utilisateur avancé PF) dispose des autorisations qui sont également associées aux rôles Test Power (Avancé de test) et Runtime (Exécution).

Pour accorder des autorisations d'utilisateurs non associées au rôle le plus élevé, vous pouvez leur affecter plusieurs rôles.

Examinez cet exemple dans lequel les rôles suivants sont affectés à un utilisateur :

- Test Administrator (Administrateur de test)
- Exécution

The screenshot shows a 'Add User' dialog box with two main sections: 'User Information' and 'Roles for the User'.

User Information:

- User ID: fakeID (with a note '(* required)')
- Password: [masked with dots]
- Re-type Password: [masked with dots]
- Name: fakeName

Roles for the User:

- ☒ Test Administrator
- ☐ System Administration
- ☐ PF Power
- ☐ SV Power
- ☐ Test Power
- ☒ Runtime
- ☐ Test Runner
- ☐ Test Observer

Différents types d'utilisateur sont associés aux rôles affectés :

- Le rôle Test Administrator (Administrateur de tests) est associé au type d'utilisateur SV Power User (Utilisateur avancé SV).
- Le rôle Runtime (Exécution) est associé au type d'utilisateur Runtime User (Utilisateur d'exécution).

Remarque : Pour plus d'informations, consultez la section [Types d'utilisateur standard et rôles standard](#) (page 93).

Les types d'utilisateur sont hiérarchiques.

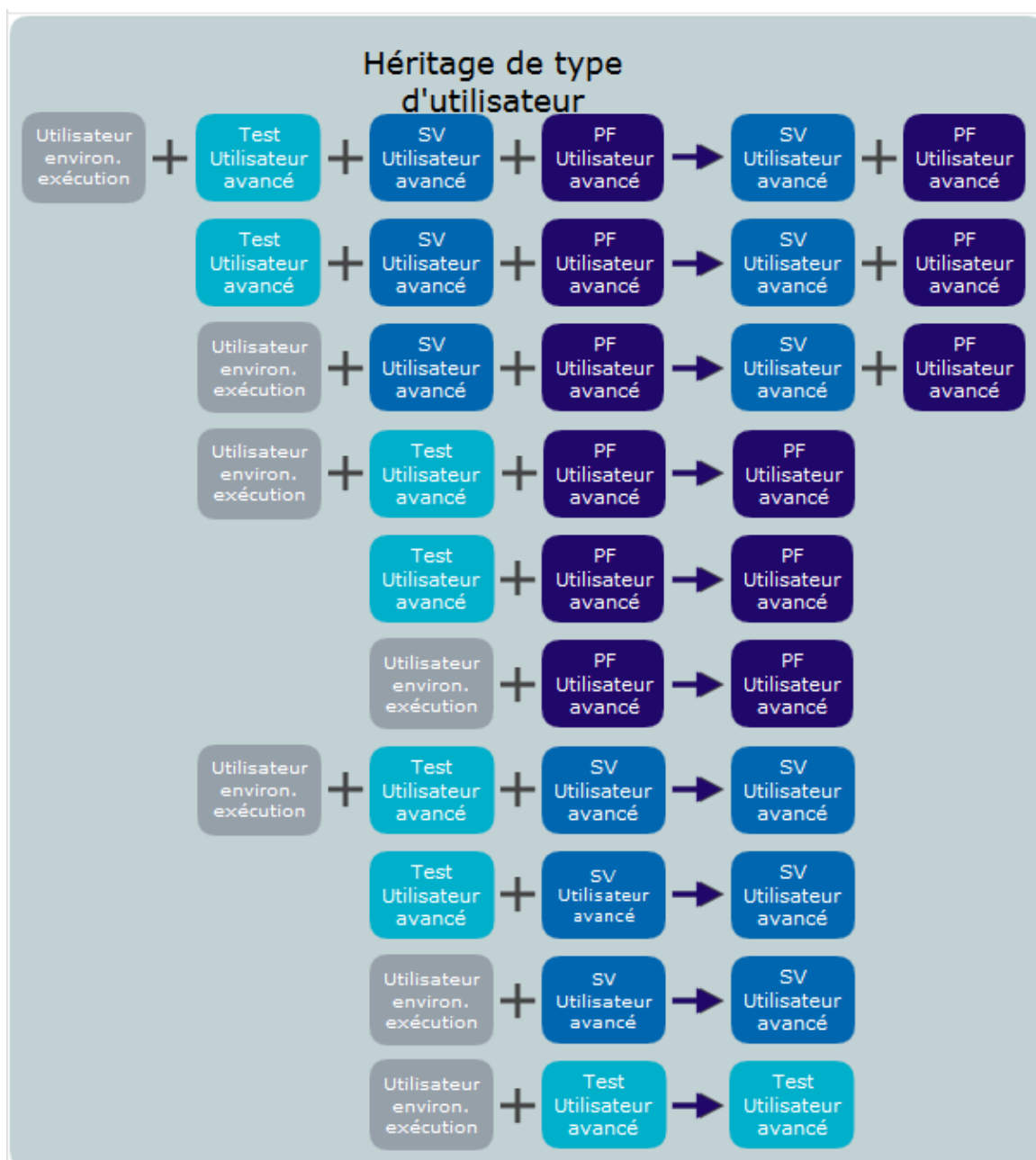


A des fins de génération du rapport d'audit d'utilisation de DevTest Solutions, le type d'utilisateur sous lequel un utilisateur est compté est le type d'utilisateur le plus élevé associé à un rôle affecté. Dans cet exemple, lorsque l'utilisateur *fakeName* se connecte à une interface utilisateur ou interface de ligne de commande DevTest, la session d'utilisateur est auditée comme appartenant au type d'utilisateur SV Power User (Utilisateur avancé SV), même si *fakeName* effectue uniquement des tâches associées au rôle Runtime (Exécution), telles que l'administration de rapports.



Graphique de l'héritage des types d'utilisateur

Le diagramme suivant illustre tous les cas de figure permettant de déterminer le type de l'utilisateur connecté lorsque plusieurs rôles à de différents types d'utilisateur lui sont affectés. Le type d'utilisateur le plus élevé est prioritaire sur tous les types inférieurs.



Chapitre 4: Security (Sécurité)

Ce chapitre traite des sujets suivants :

[Utilisation du protocole SSL pour sécuriser la communication](#) (page 74)

[Utilisation de la communication HTTPS avec la console DevTest](#) (page 80)

[Utilisation de l'authentification Kerberos](#) (page 84)

[Liste de contrôle d'accès](#) (page 86)

Utilisation du protocole SSL pour sécuriser la communication

Par défaut, les communications entre les composants utilisent un protocole non chiffré. Si nécessaire, vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour chiffrer le trafic réseau. Par exemple, vous exécutez un laboratoire dans un cloud public et vous voulez assurer le chiffrement du trafic transmis à partir de votre station de travail.

La méthode la plus simple permettant d'activer le protocole SSL est de définir une propriété DevTest.

```
lisa.net.default.protocol=ssl
```

Vous ne pouvez pas spécifier cette propriété dans le fichier **site.properties**, car cela est impossible lors de la phase d'amorçage. Vous devez la spécifier dans le fichier **local.properties** ou à partir de la ligne de commande.

Si vous démarrez un registre sans paramètres supplémentaires (par exemple, il écoute sur le port 2010, le port habituel, mais les clients doivent utiliser le protocole SSL), le nom de service pour le registre est `ssl://hostname:2010/Registry`.

Pour vous connecter à ce registre à partir de DevTest Workstation, utilisez `ssl://hostname:2010/Registry` plutôt que l'adresse `tcp://hostname:2010/Registry` habituelle. Si vous lancez un simulateur sur le même ordinateur, il est disponible à l'adresse `ssl://hostname:2014/Simulator` et se connecte automatiquement au registre via l'adresse `ssl://hostname:2010/Registry` sans aucune modification des propriétés.

Vous pouvez également combiner les protocoles et utiliser les protocoles SSL et TCP normaux. Si vous conservez la valeur par défaut (tcp) de la propriété **lisa.net.default.protocol**, vous pouvez activer des services spécifiques pour le protocole SSL en spécifiant le nom du service avec le préfixe de protocole `ssl:`, plutôt que le préfixe `tcp:` par défaut. Par exemple, pour démarrer un registre en mode SSL :

```
Registry --name=ssl://reghost.company.com:2010/Registry
```

Pour activer le protocole SSL, utilisez `ssl` dans les noms de service au lieu de `tcp`. Par exemple :

```
Registry --name=ssl://reghost.company.com:2010/Registry
```

démarre le registre avec le protocole SSL activé.

Pour connecter un simulateur à ce registre, démarrez le simulateur avec l'adresse complète du registre :

```
Simulator --name=ssl://simhost.company.com:2014/Simulator  
--registry=ssl://reghost.company.com:2010/Registry
```

Cette commande indique au simulateur d'utiliser le protocole SSL pour communiquer avec le registre tout en sécurisant le simulateur. Si vous voulez utiliser une connexion non sécurisée pour le simulateur, procédez comme suit :

```
Simulator --registry=ssl://reghost.company.com:2010/Registry
```

Il n'est pas habituel d'utiliser à la fois des serveurs sécurisés et non sécurisés. Toutefois, des serveurs non sécurisés peuvent être présents dans votre pare-feu des serveurs sécurisés dans un cloud public. Il existe un délai système avec le chiffrement SSL, qui varie considérablement en fonction du matériel.

La propriété **`lisa.net.default.protocol`** définit le protocole par défaut pour les connexions ActiveMQ. La propriété n'influence pas le protocole utilisé lors du démarrage des composants de DevTest.

Certificats SSL

Par défaut, un certificat autosigné chiffre et déchiffre les messages échangés entre les composants. VSE utilise également ce certificat lors de l'enregistrement du trafic Web de style `https://`. Le certificat figure dans le fichier **`LISA_HOME\webreckeys.ks`**.

Lorsque vous définissez le protocole par défaut sur SSL et que vous n'effectuez aucun autre changement, vous utilisez un certificat DevTest interne. Tous les utilisateurs de DevTest (pas seulement votre organisation) partagent ce certificat interne. L'utilisation de ce certificat permet de chiffrer le trafic réseau, mais n'empêche pas les utilisateurs non autorisés de se connecter à votre simulateur dans un cloud public. Pour empêcher ce type d'accès non autorisé, utilisez votre propre certificat. Vous pouvez également continuer d'utiliser le certificat de DevTest connu, mais activez le contrôle d'accès.

Si vous voulez utiliser votre propre certificat, vous pouvez remplacer le référentiel de clés de certificat en spécifiant les propriétés suivantes :

```
lisa.net.keyStore=/path/to/keystore.ks
```

```
lisa.net.keyStore.password=plaintextPassword
```

Lors de sa première lecture par DevTest, le mot de passe en texte brut est converti en propriété chiffrée :

```
lisa.net.keyStore.password_enc=33aa310aa4e18c114dacf86a33cee898
```

Création de votre propre certificat auto-signé

Dans cet exemple, l'utilitaire `keytool`, inclus avec l'environnement d'exécution Java (JRE), est utilisé.

Pour créer votre propre certificat auto-signé :

1. Entrez les réponses appropriées aux invites.

```
prompt>keytool -genkey -alias serverA -keyalg RSA -validity 365  
-keystore keystore.ks
```

```
Enter keystore password: MyNewSecretPassword <the actual  
plaintext won't be shown>
```

```
Re-enter new password: MyNewSecretPassword
```

```
What is your first and last name?
```

```
[Unknown]: serverA
```

```
What is the name of your organizational unit?
```

```
[Unknown]: dev
```

```
What is the name of your organization?
```

```
[Unknown]: ITK0
```

```
What is the name of your City or Locality?
```

```
[Unknown]: Dallas
```

```
What is the name of your State or Province?
```

```
[Unknown]: TX
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: US
```

```
Is CN=serverA, OU=dev, O=ITK0, L=Dallas, ST=TX, C=US correct?
```

```
[no]: yes
```

```
Enter key password for <serverA>
```

```
(RETURN if same as keystore password) <just hit return>
```

L'utilitaire crée un fichier contenant un certificat valide pendant 365 jours.

2. Copiez le fichier dans `LISA_HOME` et mettez à jour **local.properties** :

```
lisa.net.keyStore={{LISA_HOME}}keystore.ks
```

```
lisa.net.keyStore.password=MyNewSecretPassword
```

3. Lors de sa première lecture par DevTest, le mot de passe en texte brut est converti en propriété chiffrée :

```
lisa.net.keyStore.password_enc=33aa310aa4e18c114dacf86a33cee898
```

Le côté serveur de la configuration de connexion est terminé.

4. Configurez le client.

Ce certificat étant auto-signé, indiquez explicitement aux clients de faire confiance au certificat. Généralement, lorsque vous vous connectez à un service SSL (par exemple, à l'aide d'un navigateur à l'adresse <https://www.MyBank.com>), une autorité de certification fiable certifie le certificat. Vous devez ajouter le certificat dans un référentiel d'approbations, car les tiers approuvés ne certifient pas les certificats auto-signés :

```
lisa.net.trustStore={{LISA_HOME}}trustStore.ts
```

```
lisa.net.trustStore.password=MyNewSecretPassword
```

Le même utilitaire keytool manipule les référentiels d'approbations. En général, un référentiel de clés contient un certificat et un référentiel d'approbations contient un ou plusieurs certificats.

5. Exportez le certificat à partir du référentiel de clés du serveur :

```
keytool -exportcert -rfc -alias serverA -keystore keyStore.ks  
-file serverA.cer
```

-rfc indique d'exporter le certificat sous forme de texte ASCII au lieu du format binaire, pour simplifier l'utilisation des fonctions copier et coller. Dans notre exemple, le fichier **serverA.cer** résultant est similaire à l'exemple suivant :

```
-----BEGIN CERTIFICATE-----
```

```
MIICEzCCAXygAwIBAgIEThZnYzANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJ  
DQjELMAKGA1UE
```

```
CBM420Ix CzA JBgNVBAcTAKNCMQswCQYDVQQKEwJDQjELMAKGA1UECxMCQ0Ix CzA  
JBgNVBAMTAkNC
```

```
MB4XDTEyMDcwODAyMTE0N1oXDTEyMDcwNzAyMTE0N1owTJELMAKGA1UEBhMCQ0I  
xCzA JBgNVBAgT
```

```
AKNCMQswCQYDVQQHEwJDQjELMAKGA1UECDMCQ0Ix CzA JBgNVBAcTAKNCMQswCQY  
DVQQDEwJDQjCB
```

```
nzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAhYfaN+dCrKQwYZ+KaaPUI8DeXN  
iQ/mS+KGnXnh
```

```
Pz08vdX/7HDLW4pzFhntjmkxx0i9dMw102thTD1c0xI571PotenMENo4nyiUAEn  
MK9MTiWEYr2cQ
```

```
b6/TUueBCjRJ9I0GPCI0WPS+0Na2Q/wq8gPCHmDRpw1Xgo4uZ1v6C/ECAwEAATAN  
BgkqhkiG9w0B
```

```
AQUFAA0BgQByCsX9EoBFIghcSwoRwEvapIrv8wTaqP0KKyeIevSmbnERRu6+oi  
+cJftbdEfw6GG
```

```
CBddJH+dGZ9VeqLU8zBGasBU+JPzG5El0g0XcUGeQQEaM1YMv6XWrIwNSljQk/M  
PZSt3R0tJ0lae
```

```
JPKJXSQ610xof9+yLHH0ebUGhUjd1Q==
```

-----END CERTIFICATE-----

6. Ajoutez ce certificat au référentiel d'approbations client.

Etant donné que vous créez un fichier de référentiel d'approbations, vous devez indiquer le mot de passe deux fois. Si vous ajoutez d'autres certificats à ce référentiel d'approbations client, vous devez l'entrer une seule fois.

```
prompt> keytool -importcert -file serverA.cer -keystore trustStore.ts
```

Enter keystore password:

Re-enter new password:

Owner: CN=serverA, OU=dev, O=itko, L=Dallas, ST=Texas, C=US

Issuer: CN=serverA, OU=dev, O=itko, L=Dallas, ST=Texas, C=US

Serial number: 4e155338

Valid from: Thu Jul 07 16:33:28 EST 2011 until: Wed Oct 05 17:33:28 EST 2011

Certificate fingerprints:

MD5: 5B:10:F6:C8:02:3E:36:F5:AA:6D:FC:10:EF:F5:7F:54

SHA1:

09:DA:8E:71:7C:D5:BB:44:89:14:13:07:F4:A1:C7:06:35:CD:BE:B1

Signature algorithm name: SHA1withRSA

Version: 3

Trust this certificate? (Faire confiance à ce certificat) [no]: yes

Le certificat a été ajouté au référentiel de clés

Vous disposez désormais d'une méthode cryptographique forte pour communiquer avec vos serveurs DevTest dans le cloud public. Le certificat doit être placé des deux côtés de deux composants DevTest pour qu'ils puissent communiquer.

7. Si votre client communique avec plusieurs serveurs SSL distants, exécutez la même commande keytool pour importer le certificat dans le référentiel d'approbations.

Remarque : Hormis la sécurité de niveau de transport (SSL), vous pouvez toujours activer des listes de contrôle d'accès précises. Les listes de contrôle d'accès permettent de demander l'authentification des utilisateurs par nom d'utilisateur et mot de passe. Ce type de sécurité est similaire à un site Web d'opérations bancaires qui utilise le protocole HTTPS, mais qui vous demande toujours de vous identifier.

Utilisation du protocole SSL avec plusieurs certificats

Pour configurer votre copie locale de DevTest de sorte à communiquer de façon sécurisée avec plusieurs certificats de serveur, ajoutez chaque certificat de serveur à votre fichier trustStore local.

Dans cet exemple, nous avons le serverA, le serverB et une station de travail.

L'administrateur de serverA veut exporter le certificat à l'aide de keytool :

```
serverA> keytool -exportcert -alias lisa -file serverA.cer -keystore serverA.ks
```

De même, l'administrateur de serverB veut exporter le certificat du serverB :

```
serverB> keytool -exportcert -alias lisa -file serverB.cer -keystore serverB.ks
```

Obtenez une copie de **serverA.cer** et de **serverB.cer**, puis importez-les dans votre référentiel d'approbations client :

```
workstation>keytool -importcert -alias serverA -file serverA.cer  
-keystore trustStore.ts
```

```
workstation>keytool -importcert -alias serverB -file serverB.cer  
-keystore trustStore.ts
```

Entrez le mot de passe de votre référentiel d'approbations client pour le modifier.

Assurez-vous que votre station de travail utilise votre référentiel d'approbations client, qui contient maintenant des certificats pour le serverA et pour le serverB.

Copiez ce fichier dans **LISA_HOME** et mettez à jour **local.properties** comme suit :

```
lisa.net.trustStore={{LISA_HOME}}trustStore.ts
```

```
lisa.net.trustStore.password_enc=33aa310aa4e18c114dacf86a33cee898
```

Lorsque vous exécutez DevTest Workstation, vous pouvez sélectionner des registres.

ssl://serverA:2010/Registry

et

ssl://serverB:2010/Registry

Si vous tentez de vous connecter à **ssl://serverC:2010/Registry**, DevTest refuse la connexion, car vous ne disposez pas du certificat requis.

Authentification réciproque (bidirectionnelle)

Vous pouvez configurer DevTest de sorte que le serveur et le client doivent s'authentifier réciproquement. Ce type d'authentification requiert la définition d'une propriété côté serveur :

```
lisa.net.clientAuth=true
```

Hormis le fait que chaque client requiert un certificat de serveur dans son référentiel d'approbations, le composant de serveur requiert un certificat client pour chaque client dans son référentiel d'approbations :

```
serverA>keytool -importcert -alias clientX -file clientX.cer  
-keystore trustStore.ts
```

```
serverA>keytool -importcert -alias clientY -file clientY.cer  
-keystore trustStore.ts
```

Si le clientZ tente de se connecter au serverA, la connexion échouera, car le serverA n'inclut pas le certificat du clientZ dans son référentiel d'approbations. Cet échec se produit même si le référentiel d'approbations du clientZ contient le certificat du serverA.

Utilisation de la communication HTTPS avec la console DevTest

Effectuez les tâches suivantes pour activer la communication HTTPS pour la console DevTest :

1. [Générez une nouvelle paire de clés et un certificat.](#) (page 81)
2. [Copie du nouveau référentiel de clés dans LISA_HOME](#) (page 82)
3. [Mettez à jour les propriétés lisa.webserver.](#) (page 83)

Générez une nouvelle paire de clés et un certificat.

La façon la plus simple de générer des clés et des certificats est d'utiliser l'application keytool fournie avec le kit de développement Java. Cette application génère des clés et des certificats directement dans le référentiel de clés.

Pour plus d'informations, consultez le site http://wiki.eclipse.org/Jetty/Howto/Configure_SSL.

Procédez comme suit:

1. Ouvrez une invite de commande.
2. Saisissez la commande suivante :
`cd JAVA_HOME\bin`
3. Saisissez la commande suivante :
`keytool -keystore keystore -alias jetty -genkey -keyalg RSA`

Remarque : Vous devez utiliser jetty comme alias.

Cette commande vous invite à spécifier des informations sur le certificat et des mots de passe pour protéger le référentiel de clés et les clés qu'il contient.

4. Répondez aux invites suivantes.

Enter the keystore password: (Entrer le mot de passe du référentiel de clés)

Le mot de passe respecte la casse. Le texte de votre mot de passe ne s'affiche pas.

Re-enter new password:

Le mot de passe respecte la casse. Le texte de votre mot de passe ne s'affiche pas.

What is your first and last name?

[Unknown]: (Inconnu)

Entrez le même nom d'ordinateur que celui utilisé pour le nom de registre. Normalement, il s'agit du nom d'hôte incomplet du serveur. Par exemple, pour un ordinateur nommé jetty.eclipse.org, vous entrez **jetty.eclipse.org**.

Toutefois, il est possible de démarrer le registre avec le paramètre de ligne de commande -m, à l'aide d'une adresse IP ou d'un nom d'hôte complet. Dans ce cas, le nom d'hôte du certificat SSL doit correspondre pour empêcher les erreurs de certificat dans le navigateur Web.

Remarque : Seule cette invite est obligatoire.

What is the name of your organizational unit?

[Unknown]: (Inconnu)

What is the name of your organization?

[Unknown]: (Inconnu)

What is the name of your City or Locality?

[Unknown]: (Inconnu)

What is the name of your State or Province?

[Unknown]: (Inconnu)

What is the two-letter country code for this unit?

[Unknown]: (Inconnu)

Une confirmation de vos entrées s'affiche.

5. Cliquez sur **yes** (oui) pour valider votre choix.

L'invite suivante s'affiche.

Enter key password for <jetty> (Entrer le mot de passe de clé pour)

<RETURN if same as keystore password>:

6. Appuyez sur Entrée.

L'utilitaire crée un nouveau fichier nommé **keystore** dans le répertoire actuel.

Copie du nouveau référentiel de clés dans LISA_HOME

Procédez comme suit:

1. Copiez le nouveau fichier de référentiel de clés dans le répertoire **LISA_HOME**.
2. Remplacez le nom du fichier de référentiel de clés par **webserver.ks**.

Remarque : webserver.ks est le fichier par défaut spécifié dans lisa.properties. Si vous voulez utiliser un nom de fichier différent, ouvrez lisa.properties et modifiez la propriété **lisa.webserver.ssl.keystore.location** pour indiquer le chemin et le nom de fichier approprié. Pour plus d'informations, consultez la section [Mise à jour des propriétés Webserver](#) (page 83).

Mise à jour des propriétés Webserver

Procédez comme suit:

1. Ouvrez le fichier `local.properties` dans le répertoire `LISA_HOME`.
2. Ajoutez les propriétés suivantes au fichier.

```
# enable https and setup the webserver ssl keystore
lisa.webserver.https.enabled=true
lisa.webserver.ssl.keystore.location={{LISA_HOME}}webserver.ks
lisa.webserver.ssl.keystore.password=yourpassword
lisa.webserver.ssl.keymanager.password=yourpassword
lisa.webserver.port=8443
# should lisa workstation use https when launching the portals?
lisa.portal.use_https=true
lisa.portal.url.prefix=http://
```
3. Modifiez chaque propriété de sorte à spécifier la valeur appropriée.

`lisa.webserver.https.enabled`

Définissez cette propriété sur **true** pour utiliser le protocole HTTPS avec la console DevTest.

`lisa.webserver.ssl.keystore.location`

La valeur par défaut de cette propriété est `{{LISA_HOME}}webserver.ks`. Modifiez cette valeur si vous voulez utiliser un fichier de référentiel de clés avec un nom différent ou dans un répertoire différent.

`lisa.webserver.ssl.keystore.password`

Définissez cette propriété sur le mot de passe que vous avez défini lors de la génération du fichier de référentiel de clés.

`lisa.webserver.ssl.keymanager.password`

Définissez cette propriété sur le mot de passe du gestionnaire de clés que vous avez défini lors de la génération du fichier de référentiel de clés. Ce mot de passe est identique au mot de passe du référentiel de clés, sauf si vous avez spécifié un mot de passe différent.

`lisa.webserver.port`

Cette propriété est facultative ; le port par défaut pour les communications HTTPS est 8443.

`lisa.portal.url.prefix`

Remplacez la valeur `http://` de cette propriété par `https://`.

Remarque : La première fois que le système lit les mots de passe dans le fichier `local.properties`, le mot de passe est converti en une propriété chiffrée.

4. Enregistrez vos modifications et fermez le fichier `local.properties`.
5. Redémarrez le registre.

Utilisation de l'authentification Kerberos

La prise en charge de Kerberos est similaire à la prise en charge de l'authentification de base et de NTLM dans DevTest. DevTest prend en charge Kerberos lorsqu'une application ou une ressource à laquelle DevTest accède via certaines étapes est protégée par l'authentification Kerberos. Par exemple : HTTP/HTTPS, XML de service Web ; étapes identiques pour NTLM et l'authentification de base. La prise en charge de Kerberos utilise les propriétés suivantes dans le fichier local.properties :

`lisa.java.security.auth.login.config`

Indique l'emplacement du fichier de configuration de connexion.

`lisa.java.security.krb5.conf`

Emplacement du fichier de configuration Kerberos utilisé pour remplacer tous les emplacements prédéfinis.

`lisa.http.kerberos.principal`

Nom du principal utilisé pour la connexion lorsque DevTest est utilisé pour l'authentification par principal et mot de passe. Lorsque DevTest Workstation démarre, le principal est chiffré.

`lisa.http.kerberos.pass`

Mot de passe utilisé pour la connexion lorsque DevTest est utilisé pour l'authentification par principal et mot de passe. Lorsque DevTest Workstation démarre, le principal est chiffré.

Vous pouvez vous authentifier uniquement avec les paramètres

`lisa.java.security.auth.login.config` et **`lisa.java.security.krb5.conf`**. Ces fichiers et leurs paramètres varient selon le système d'exploitation sur lequel DevTest est exécuté. Consultez la documentation appropriée sur la procédure de configuration de ces deux fichiers pour l'authentification qui n'utilise pas la prise en charge DevTest pour l'authentification par principal et mot de passe.

Prise en charge de DevTest pour l'authentification par mot de passe principal +

Pour prendre en charge la connexion d'un utilisateur à DevTest à l'aide d'informations d'identification, l'utilisateur doit configurer son fichier de configuration de connexion de sorte à utiliser celui de DevTest. L'exemple suivant illustre le contenu du fichier :

```
com.sun.security.jgss.initiate {  
  
    com.itko.lisa.http.LisaKrb5LoginModule required  
    doNotPrompt=false;  
  
};
```

La propriété personnalisée **LisaKrb5LoginModule** est une extension de la propriété standard **com.sun.security.auth.module.Krb5LoginModule** avec une modification. Cette extension soumet les informations d'identification fournies dans **lisa.http.kerberos.principal** et **lisa.http.kerberos.pass** au lieu d'inviter l'utilisateur à indiquer ses informations d'identification.

Exemple de fichier krb5.conf

```
[libdefaults]

    default_realm = EXAMPLE.COM

    allow_weak_crypto = true


[realms]

    EXAMPLE.COM = {
        kdc = kdc.fakedomain.com:60088
    }


[domain_realm]

    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM


[login]

    krb4_convert = true
```

Exemple de fichier krb5.conf avec Active Directory comme service KDC

```
[libdefaults]

    default_realm = FAKEDOMAIN.COM

    allow_weak_crypto = false

    default_tkt_enctypes = arcfour-hmac-md5

    default_tgs_enctypes = arcfour-hmac-md5

    permitted_enctypes = RC4-HMAC arcfour-hmac-md5


[realms]

    FAKEDOMAIN.COM = {
```

```
kdc = kdc.fakedomain.com
master_kdc = kdc.fakedomain.com
admin_server = kdc.fakedomain.com
default_domain = FAKEDOMAIN.COM
}
[domain_realm]
    fakedomain.com = FAKEDOMAIN.COM
[login]
    krb4_convert = true
```

Sample login.config file

```
com.sun.security.jgss.initiate {
    com.itko.lisa.http.LisaKrb5LoginModule required
    doNotPrompt=false;
};
```

(Liste de contrôle d'accès

La liste de contrôle d'accès est le mécanisme utilisé par DevTest pour authentifier des utilisateurs et appliquer des rôles. La liste de contrôle d'accès est activée par défaut.

Cette section comprend les rubriques suivantes :

[Présentation de ACL](#) (page 87)

[Outils ou API de liste de contrôle d'accès et de ligne de commande.](#) (page 91)

[Types de droits](#) (page 92)

[Types d'utilisateur standard et rôles standard](#) (page 93)

[Autorisations standard](#) (page 107)

[Utilisateurs standard](#) (page 120)

[Affichage des informations d'utilisateur à partir de DevTest Workstation](#) (page 124)

[Gestion des utilisateurs et des rôles](#) (page 125)

[Configuration de la liste de contrôle d'accès pour l'utilisation de l'authentification LDAP](#) (page 133)

[Autorisation des utilisateurs authentifiés par LDAP](#) (page 135)

[groupes de ressources](#) (page 137)

Présentation de ACL

Les listes de contrôle d'accès (ACL) constituent un mécanisme de sécurité largement utilisé. La liste de contrôle d'accès octroie aux utilisateurs l'accès uniquement aux fonctionnalités des applications qu'ils requièrent pour effectuer leurs activités basées sur des rôles. La liste de contrôle d'accès est requise pour DevTest Solutions de sorte à surveiller et à maintenir la conformité au contrat de licence. Les contrats de licence reposent sur le nombre maximum de sessions d'utilisateur autorisées simultanément.

Cette présentation introduit les rubriques relatives aux listes de contrôle d'accès suivantes :

- Planification du déploiement des listes de contrôle d'accès
- Authentification
- Authorization (Autorisation)
- Sessions utilisateur
- Scénarios de test automatisés
- Base de données ACL

Planification du déploiement des listes de contrôle d'accès

Lors du démarrage DevTest Solutions 8.0, le contrôle d'accès via le système de listes de contrôle d'accès est requis. Il n'est pas possible d'accéder à la station de travail DevTest Workstation ni au portail DevTest sans authentification au niveau du système de liste de contrôle d'accès.

Avant de configurer la liste de contrôle d'accès, prenez attentivement en compte l'utilisation de DevTest Solutions par chaque utilisateur et l'accès correspondant requis pour chaque type d'utilisateur.

Par défaut, seuls le superutilisateur et l'administrateur système peuvent avoir accès à la console de serveur, qui fournit l'accès administratif au système de liste de contrôle d'accès.

Administration des listes de contrôle d'accès

L'Administrateur ACL est responsable des activités suivantes :

- Création des utilisateurs dans le système ACL
- Affectation des rôles aux utilisateurs, en fonction de leurs responsabilités et de l'accès requis par chacun d'eux

- Restriction de l'accès à plusieurs parties de DevTest Solutions en assignant des composants à des groupes de ressources
- Affectation de l'accès utilisateur à des groupes de ressources définis.

L'administrateur doit parfaitement connaître les différents rôles ACL et leurs droits associés pour affecter les rôles appropriés à chaque utilisateur.

Important : N'utilisez pas le superutilisateur par défaut ou les administrateurs système pour gérer le système de liste de contrôle d'accès. Utilisez le superutilisateur par défaut pour créer des utilisateurs avec des rôles identiques au superutilisateur par défaut et administrateur système. Utilisez les nouveaux utilisateurs pour gérer le système de liste de contrôle d'accès et changez les mots de passe du superutilisateur par défaut et des administrateurs système pour éviter les accès non autorisés.

Utilisation du protocole LDAP avec DevTest Solutions

Vous pouvez également gérer les mots de passe pour DevTest Solutions via LDAP, particulièrement si un système LDAP ou Active Directory est déjà disponible. Lorsque vous utilisez LDAP, les modifications apportées aux mots de passe d'utilisateur sont effectuées par l'administrateur LDAP. L'administrateur de liste de contrôle d'accès n'est plus en mesure d'effectuer des modifications de mot de passe.

Important : La responsabilité de l'implémentation du système de liste de contrôle d'accès et de toute intégration à un service LDAP incombe au client. Si vous avez besoin d'une assistance pour ces activités d'implémentation, contactez CA Services. La responsabilité de l'administration d'utilisateurs via une liste de contrôle d'accès incombe à l'administrateur LDAP. Le service de support de CA n'est pas en mesure d'améliorer des situations où l'accès de vue à la table des rôles n'est pas disponible.

Par exemple, un client qui signale un problème de simulation d'un test en raison de problèmes d'autorisation doit vérifier que l'administrateur de liste de contrôle d'accès/LDAP est disponible lorsqu'il contacte le service de support de CA. Les administrateurs ACL doivent tenir compte de ces facteurs lors de l'affectation des rôles à leurs utilisateurs et leurs groupes.

Authentication

Vous pouvez déterminer le mode d'authentification des utilisateurs par DevTest. Vous pouvez [ajouter manuellement des utilisateurs](#) (page 126) à la base de données de listes de contrôle d'accès et spécifier les informations d'identification. Les informations d'identification incluent l'ID d'utilisateur et le mot de passe avec lequel l'utilisateur peut se connecter à l'interface utilisateur de DevTest Solutions ou l'interface de ligne de commande. Si vos utilisateurs sont déjà définis avec des informations d'identification dans une base de données LDAP, vous pouvez également utiliser le serveur LDAP pour l'authentification. Dans ce cas, vous effectuez les étapes décrites dans la section [Configuration de la liste de contrôle d'accès pour l'utilisation de l'authentification LDAP](#). (page 133)

Authorization (Autorisation)

DevTest limite l'accès aux fonctionnalités DevTest auxquelles chaque utilisateur peut accéder en fonction de leur rôle dans l'entreprise. DevTest Solutions est installé avec plus d'une dizaine de rôles standard. Vous pouvez mettre en pratique l'utilisation de DevTest par les utilisateurs disposant de différents rôles en vous connectant comme utilisateur standard. Des [rôles standard](#) (page 93) uniques sont affectés à des [utilisateurs standard](#) (page 120).

Important : A des fins de sécurité, l'administrateur ACL doit modifier le mot de passe par défaut (admin, guest) dès que possible et le remplacer par un mot de passe qu'ils n'oublieront pas.

Lorsque vous ajoutez manuellement des utilisateurs à la base de données ACL, vous affectez un rôle à chaque utilisateur. Chaque rôle dispose d'un ensemble d'autorisations. Il est possible d'affecter plusieurs rôles, mais cela est rarement nécessaire, car les rôles avec davantage de responsabilité incluent des autorisations des rôles inférieurs. Lorsque vous utilisez LDAP, la liste de contrôle d'accès est automatiquement remplie avec une ligne par utilisateur. Dans ce cas, vous affectez uniquement des rôles tel que décrit dans la section [Autorisation d'utilisateurs authentifiés par LDAP](#) (page 135).

Les exemples suivants sont des activités que vous pouvez contrôler avec des autorisations :

- Créer un scénario de test
- Créer un document de simulation
- Simuler un scénario de test

Sessions utilisateur

Lorsqu'un utilisateur autorisé se connecte à une interface utilisateur ou interface de ligne de commande DevTest, une session d'utilisateur est créée. Les sessions d'utilisateur sont auditées et forment la base des rapports d'audit d'utilisation. Ces rapports incluent des mesures et des statistiques sur les sessions d'utilisateur simultanées maximum par type d'utilisateur, les [types d'utilisateur](#) (page 68) étant des catégories qui incluent plusieurs rôles. Consultez la section Liste de contrôle d'accès et sessions d'utilisateur

Liste de contrôle d'accès et rétrocompatibilité pour les interfaces de ligne de commande et API exécutées sans informations d'identification

Pour accéder à une interface utilisateur ou une interface de ligne de commande DevTest, les utilisateurs doivent se connecter avec un nom d'utilisateur et le mot de passe valides. La condition d'informations d'identification s'applique également à l'exécution de tests et au démarrage de services virtuels. Si les scénarios de test automatisés dans une version antérieure sont exécutés sans informations d'identification, vous pouvez temporairement remplacer la liste de contrôle d'accès de sorte à continuer à les exécuter comme prévu. Consultez la section [Outils ou API de liste de contrôle d'accès](#) (page 91) et de ligne de commande.

Base de données ACL

Les données de liste de contrôle d'accès sont stockées dans la base de données Derby interne par défaut après l'installation. Comme l'indique la rubrique *Installation*, la base de données Derby doit être remplacée par une base de données de l'entreprise. Pour en savoir plus, reportez-vous à la section [Administration des bases de données](#) (page 41).

Outils ou API de liste de contrôle d'accès et de ligne de commande.

LISA 7.5.2 et version antérieure n'appliquent pas de liste de contrôle d'accès. Par défaut, DevTest Solutions applique la liste de contrôle d'accès. CA Technologies reconnaît la nécessité d'une période de transition pour mettre à jour les outils de ligne de commande et API existants qui ont été exécutés sans nom d'utilisateur et mot de passe spécifiques. Pendant la mise à jour de vos tests automatisés, vos services virtuels et vos programmes tels que TestRunner (Exécuteur de tests) avec des informations d'identification, vous pouvez définir un paramètre indiquant à votre programme de s'exécuter avec un nom d'utilisateur d'exécution interne. Dans ce cas, l'identité de l'utilisateur connecté au système d'exploitation est stocké dans l'objet de session.

Pour remplacer la liste de contrôle d'accès temporairement, procédez comme suit :

1. Connectez-vous au serveur DevTest contenant le registre in-use (en cours d'utilisation).
2. Accédez au répertoire d'installation.
3. Ouvrez le fichier local.properties pour le modifier.
4. Ajoutez le paramètre `lisa.acl.use.runtime` et définissez-le sur `true`, comme suit :
`lisa.acl.use.runtime=true`
5. Enregistrez le fichier local.properties.

Votre programme de ligne de commande est exécuté comme
`_runtime_<username>`, où `<username>` est issu de la propriété système
`user.name`.

Pour appliquer la liste de contrôle d'accès sans exceptions, procédez comme suit :

1. Connectez-vous au serveur DevTest contenant le registre in-use (en cours d'utilisation).
2. Accédez au répertoire d'installation.
3. Ouvrez le fichier local.properties pour le modifier.
4. Commentez le paramètre suivant ou définissez-le sur `false`.
`lisa.acl.use.runtime=`
5. Enregistrez le fichier local.properties.

Toutes les interfaces utilisateur et les interfaces de ligne de commande seront exécutées en utilisant des informations d'identification valides.

Types de droits

Les autorisations peuvent être classées selon les types suivants :

- Booléen
- Limite numérique
- Liste
- Personnalisé

Booléen

La plupart des autorisations sont de type booléen. Ces autorisations indiquent si une activité est autorisée ou non.

Par exemple, l'autorisation Stop Registry (Arrêter le registre) indique si un utilisateur peut arrêter le registre.

Limite numérique

Une autorisation peut représenter une limite numérique.

Par exemple, l'autorisation Stage Test (Simuler le test) permet à un utilisateur de simuler un scénario de test avec le nombre maximum spécifié d'utilisateurs virtuels.

La valeur d'une autorisation de limite numérique doit être -1, 0, ou un nombre entier positif.

Si la valeur est -1, l'autorisation est octroyée et il n'y a aucune limite numérique.

Si la valeur est 0, l'autorisation est refusée.

Liste

Vous pouvez associer une autorisation à une liste de chaînes. Les chaînes peuvent être des expressions régulières.

Personnalisé

Le provisionnement cloud d'environnements de développement et de test utilise des propriétés personnalisées. DevTest crée des propriétés personnalisées pour spécifier le nom d'utilisateur et le mot de passe requis pour accéder au fournisseur de gestionnaire virtuel de laboratoires (VLM).

Pour plus d'informations, consultez la section Configuration des propriétés DCM de la rubrique *Utilisation de CA Application Test*.

Types d'utilisateur standard et rôles standard

DevTest Solutions crée des types d'utilisateur standard avec des rôles associés. Chaque onglet est associé à un ensemble unique d'[autorisations](#) (page 107). Vous pouvez [changer](#) (page 128) les autorisations affectées à un rôle standard par DevTest. Vous pouvez également [supprimer](#) (page 128) un rôle standard.

[PF Power User \(Utilisateur avancé PF\) et SV Power User \(Utilisateur avancé SV\)](#) (page 94)

La combinaison de types d'utilisateur avancé PF et SV inclue les rôles suivants :

- Super User (Superutilisateur)
- DevTest Administrator (Administrateur de DevTest)

[PF Power User \(Utilisateur avancé PF\)](#) (page 96)

Le type PF Power User (Utilisateur avancé PF) inclut le rôle suivant :

- PF Power (Avancé PF)

[SV Power User \(Utilisateur avancé SV\)](#) (page 98)

Le type SV Power User (Utilisateur avancé SV) inclut les rôles suivants :

- Test Administrator (Administrateur de test)
- SV Power (Avancé SV)
- Utilitaire Test Runner (Exécuteur de tests)

[Test Power User \(Utilisateur avancé de test\)](#) (page 101)

Le type Test Power User (Utilisateur avancé de test) inclut les rôles suivants :

- Test Power (Avancé Test)
- Test Observer (Observateur de tests)
- Load Tester (Testeur de charge)
- User (Utilisateur)

[Runtime User \(Utilisateur d'exécution\)](#) (page 105)

Le type Runtime User (Utilisateur d'exécution) inclut les rôles suivants :

- Administrateur système
- Exécution
- Guest (Invité)

Combinaison de types d'utilisateur avancé PF et SV

Le type d'utilisateur de la combinaison d'utilisateur avancé PF/SV possèdent les rôles suivants :

- Super User (Superutilisateur)
- DevTest Administrator (Administrateur de DevTest)

Les superutilisateurs et les administrateurs système peuvent réaffecter des autorisations de rôle. Consultez la section [Ajout et mise à jour de rôles](#) (page 128).

Super User (Superutilisateur)

Le rôle Super User (Superutilisateur) dispose de toutes les autorisations standard.

- [Administration de la console LISA](#) (page 108)
- [Administration des utilisateurs et des rôles](#) (page 108)
- [Administration des ressources](#) (page 109)
- [Administration des tests et des suites](#) (page 109)
- [Administration des services virtuels](#) (page 110)
- [Administration du DevTest Server](#) (page 112)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)
- [Administration des mesures et des événements](#) (page 115)
- [Administration de Pathfinder](#) (page 116)
- [DevTest Workstation](#) (page 117)
- [Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Accès à toutes les cibles

DevTest Administrator (Administrateur de DevTest)

Le rôle d'administrateur de DevTest dispose des autorisations standard complètes, excepté l'administration de la console LISA, l'administration des utilisateurs et des rôles et l'administration des ressources. A savoir :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Administration des tests et des suites](#) (page 109)
- [Administration des services virtuels](#) (page 110)
- [Administration du DevTest Server](#) (page 112)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)
- [Administration des mesures et des événements](#) (page 115)
- [Administration de Pathfinder](#) (page 116)
- [DevTest Workstation](#) (page 117)
- [Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Accès à toutes les cibles

Type d'utilisateur PF Power User (Utilisateur avancé PF)

Le type d'utilisateur PF Power User (Utilisateur avancé PF) a le rôle PF Power (Avancé PF).

Les superutilisateurs et les administrateurs système peuvent réaffecter des autorisations de rôle. Consultez la section [Ajout et mise à jour de rôles](#) (page 128).

PF Power (Avancé PF)

Le rôle PF Power (Avancé PF) dispose des autorisations suivantes :

- Autorisation partielle de l'[administration de la console DevTest](#) (page 108)
 - Accès à la console Pathfinder (PFP)
 - View VSEasy Console (Afficher la console VSEasy)
- [Administration des tests et des suites](#) (page 109)
- Autorisation partiel de l'administration des [services virtuels](#) (page 110)
 - Affichage du tableau de bord du VSE
 - Déploiement du service du VSE
 - Récupération d'archive de service du VSE
 - Démarrage du service du VSE
 - Arrêt du service du VSE
 - Update Virtual Service Capacity (Mettre à jour la capacité du service virtuel)
 - Update Virtual Service Think Scale (Mettre à jour le pourcentage de délai de réflexion du service virtuel)
 - Update Virtual Service Auto-Restart (Mettre à jour la valeur du redémarrage automatique du service virtuel)
 - Set Virtual Service Execution Mode (Définir le mode d'exécution du service virtuel)
 - Reset Virtual Service Transaction Counts (Réinitialiser les nombres de transactions du service virtuel)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)
- [Administration des mesures et des événements](#) (page 115)
- [CAI Administration \(Administration de CAI\)](#) (page 116)
- Autorisation partielle de l'administration de la station de travail [DevTest Workstation](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)

- Création modification et affichage d'une configuration
- Création modification et affichage d'un document de simulation
- Création modification et affichage d'une suite
- Création modification et affichage d'un scénario de test
- Création modification et affichage d'un document d'audit
- View Virtual Service Model (Afficher un modèle de service virtuel)
- View Virtual Service Image (Afficher une image de service virtuel)
- Execute ITR (Exécuter un test interactif)
- Execute Instant Replay (Exécuter une relecture instantanée)
- View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
- View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
- List Available Labs (Liste des laboratoires disponibles)
- Démarrage/arrêt des laboratoires
- Expand Labs (Développer les laboratoires)
- Suppression de laboratoires d'autres utilisateurs
- Accès à toutes les cibles

Type d'utilisateur SV Power User (Utilisateur avancé SV)

Le type d'utilisateur SV Power User (Utilisateur avancé SV) a les rôles suivants :

- Test Administrator (Administrateur de test)
- SV Power (Avancé SV)
- Utilitaire Test Runner (Exécuteur de tests)

Les superutilisateurs et les administrateurs système peuvent réaffecter des autorisations de rôle. Consultez la section [Ajout et mise à jour de rôles](#) (page 128).

Test Administrator (Administrateur de test)

Le rôle Test Administrator (Administrateur de test) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation d'administration des tests et des suites](#) (page 109)
- [Autorisation Virtual Services Administration \(Administration des services virtuels\)](#) (page 110)
- [Autorisation DevTest Workstation](#) (page 117)
- [Autorisation Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Accès à toutes les cibles

SV Power (Avancé SV)

Le rôle SV Power (Avancé SV) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation d'administration des tests et des suites](#) (page 109)
- Autorisation partiel de l'administration des [services virtuels](#) (page 110)
 - Affichage du tableau de bord du VSE
 - Déploiement du service du VSE
 - Récupération d'archive de service du VSE
 - Démarrage du service du VSE
 - Arrêt du service du VSE
 - Update Virtual Service Capacity (Mettre à jour la capacité du service virtuel)
 - Update Virtual Service Think Scale (Mettre à jour le pourcentage de délai de réflexion du service virtuel)
 - Update Virtual Service Auto-Restart (Mettre à jour la valeur du redémarrage automatique du service virtuel)
 - Update Virtual Service Group Tag (Mettre à jour la balise d'un groupe de service virtuel)
 - Set Virtual Service Execution Mode (Définir le mode d'exécution du service virtuel)
 - Reset Virtual Service Transaction Counts (Réinitialiser les nombres de transactions du service virtuel)
 - Heal Virtual Service Image (Réparer une image de service virtuel)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)
- [Administration des mesures et des événements](#) (page 115)
- Autorisation partielle d'administration de la [station de travail de LISA](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)
 - Création modification et affichage d'une configuration
 - Création modification et affichage d'un document de simulation
 - Création modification et affichage d'une suite
 - Création modification et affichage d'un scénario de test
 - Création modification et affichage d'un document d'audit

- Création modification et affichage d'un modèle de service virtuel
- Création modification et affichage d'une image de modèle de service virtuel
- Execute ITR (Exécuter un test interactif)
- Execute Instant Replay (Exécuter une relecture instantanée)
- View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
- View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
- List Available Labs (Liste des laboratoires disponibles)
- Démarrage/arrêt des laboratoires
- Expand Labs (Développer les laboratoires)
- Suppression de laboratoires d'autres utilisateurs
- Accès à toutes les cibles

Utilitaire Test Runner (Exécuteur de tests)

Le rôle Test Runner (Exécuteur de tests) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation d'administration des tests et des suites](#) (page 109)
- [Autorisation DevTest Workstation](#) (page 117)
- [Autorisation Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Accès à toutes les cibles

Type d'utilisateur Test Power User (Utilisateur avancé Test)

Le type Test Power User (Utilisateur avancé de test) inclut les rôles suivants :

- Test Power (Avancé Test)
- Test Observer (Observateur de tests)
- Load Tester (Testeur de charge)
- User (Utilisateur)

Les superutilisateurs et les administrateurs système peuvent réaffecter des autorisations de rôle. Consultez la section [Ajout et mise à jour de rôles](#) (page 128).

Test Power (Avancé Test)

Le rôle Test Power (Avancé Test) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Administration des tests et des suites](#) (page 109)
- Autorisation partiel de l'administration des [services virtuels](#) (page 110)
 - Affichage du tableau de bord du VSE
 - Déploiement du service du VSE
 - Récupération d'archive de service du VSE
 - Démarrage du service du VSE
 - Arrêt du service du VSE
 - Update Virtual Service Capacity (Mettre à jour la capacité du service virtuel)
 - Update Virtual Service Think Scale (Mettre à jour le pourcentage de délai de réflexion du service virtuel)
 - Update Virtual Service Auto-Restart (Mettre à jour la valeur du redémarrage automatique du service virtuel)
 - Update Virtual Service Group Tag (Mettre à jour la balise d'un groupe de service virtuel)
 - Set Virtual Service Execution Mode (Définir le mode d'exécution du service virtuel)
 - Reset Virtual Service Transaction Counts (Réinitialiser les nombres de transactions du service virtuel)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)

- [Metric/Event Administration \(Administration des mesures/événements\)](#) (page 115)
- Toutes les [autorisations de la station de travail DevTest Workstation](#) (page 117), excepté :
 - Création ou modification d'un modèle de service virtuel
 - Création ou modification d'une image de modèle de service virtuel
- [Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Accès à toutes les cibles
- Accès à une liste spécifique de cibles uniquement

Test Observer (Observateur de tests)

Le rôle Test Observer (Observateur de tests) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation Test/Suite Administration \(Administration des tests/suites\)](#) (page 109)
- Autorisation partielle d'administration de la [station de travail de LISA](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)
 - View a Configuration (Afficher une configuration)
 - View a Staging Document (Afficher un document de simulation)
 - View a Suite (Afficher une suite)
 - View a Test Case (Afficher un scénario de test)
 - View an Audit Document (Afficher un document d'audit)
 - View Virtual Service Model (Afficher un modèle de service virtuel)
 - View Virtual Service Image (Afficher une image de service virtuel)
 - View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
 - View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
- [Autorisation Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Can only access a given list of targets (Peut accéder uniquement à certaines cibles)

Load Tester (Testeur de charge)

Le rôle Test Load Tester (Testeur de charge) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation Test/Suite Administration \(Administration des tests/suites\)](#) (page 109)
- [Autorisation CVS Administration \(Administration des tests/suites\)](#) (page 113)
- Autorisation partielle d'administration de la [station de travail de LISA](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)
 - View a Configuration (Afficher une configuration)
 - View a Staging Document (Afficher un document de simulation)
 - View a Suite (Afficher une suite)
 - View a Test Case (Afficher un scénario de test)
 - View an Audit Document (Afficher un document d'audit)
 - View Virtual Service Model (Afficher un modèle de service virtuel)
 - View Virtual Service Image (Afficher une image de service virtuel)
 - View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
 - View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
- [Autorisation Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)
- Can only access a given list of targets (Peut accéder uniquement à certaines cibles)

User (Utilisateur)

Le rôle User (Utilisateur) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [LISA](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Autorisation Test/Suite Administration \(Administration des tests/suites\)](#) (page 109)
- Autorisation partielle d'administration de la [station de travail de LISA](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)
 - View a Configuration (Afficher une configuration)
 - View a Staging Document (Afficher un document de simulation)
 - View a Suite (Afficher une suite)
 - View a Test Case (Afficher un scénario de test)
 - View an Audit Document (Afficher un document d'audit)
 - View Virtual Service Model (Afficher un modèle de service virtuel)
 - View Virtual Service Image (Afficher une image de service virtuel)
 - View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
 - View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
 - List Available Labs (Liste des laboratoires disponibles)
 - Démarrage/arrêt des laboratoires
 - Expand Labs (Développer les laboratoires)
- Accès à toutes les cibles

Type d'utilisateur Runtime User (Utilisateur d'exécution)

Le type d'utilisateur Runtime User (Utilisateur d'exécution) a les rôles suivants :

- Administrateur système
- Exécution
- Guest (Invité)

Les superutilisateurs et les administrateurs système peuvent réaffecter des autorisations de rôle. Consultez la section [Ajout et mise à jour de rôles](#) (page 128).

Administrateur système

Le rôle d'administrateur système dispose des autorisations par défaut suivantes :

- Autorisation partielle de l'administration de la console [DevTest](#) (page 108)
 - Accès à la console DevTest
 - Access Server Console (Accès à la console de serveur)
- [Administration des utilisateurs et des rôles](#) (page 108)
- [Administration des ressources](#) (page 109)
- Autorisation partiel de l'administration des [services virtuels](#) (page 110)
 - Configuration du nettoyage de données de suivi du SVE
 - Arrêt du serveur VSE
 - Réinitialisation du serveur VSE
 - Surveillance du serveur VSE
- [Administration du DevTest Server](#) (page 112)

Exécution

Le rôle Runtime (Exécution) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la console [DevTest](#) (page 108)
 - View VSEasy Console (Afficher la console VSEasy)
- [Administration des tests et des suites](#) (page 109)
- Autorisation partiel de l'[administration des services virtuels](#) (page 110)
 - Affichage du tableau de bord du VSE
 - Déploiement du service du VSE (R)
 - Récupération d'archive de service du VSE (R)
 - Démarrage du service du VSE (R)
 - Arrêt du service du VSE (R)
 - Update Virtual Service Capacity (Mettre à jour la capacité du service virtuel)
 - Update Virtual Service Think Scale (Mettre à jour le pourcentage de délai de réflexion du service virtuel)
 - Update Virtual Service Auto-Restart (Mettre à jour la valeur du redémarrage automatique du service virtuel)
 - Update Virtual Service Group Tag (Mettre à jour la balise d'un groupe de service virtuel)
 - Définition du mode d'exécution du service virtuel (R)
 - Réinitialisation des nombres de transactions du service virtuel (R)
- [CVS Administration \(Administration des mesures/événements\)](#) (page 113)
- [Administration des rapports](#) (page 114)
- Autorisation partielle de l'administration de la station de travail [DevTest Workstation](#) (page 117)
 - Démarrage de la station de travail de DevTest
 - View a Configuration (Afficher une configuration)
 - View a Staging Document (Afficher un document de simulation)
 - View a Suite (Afficher une suite)
 - View a Test Case (Afficher un scénario de test)
 - View an Audit Document (Afficher un document d'audit)
 - View Virtual Service Model (Afficher un modèle de service virtuel)
 - View Virtual Service Image (Afficher une image de service virtuel)

- View ITR Properties (Afficher les propriétés de l'exécution de test interactif)
- View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)
- Autorisation partielle de l'[intégration de laboratoire cloud](#) (page 119)
 - List Available Labs (Liste des laboratoires disponibles)
 - Expand Labs (Développer les laboratoires)
- Can only access a given list of targets (Peut accéder uniquement à certaines cibles)

Guest (Invité)

Le rôle Guest (Invité) dispose des autorisations suivantes :

- Autorisation partielle de l'administration de la station de travail [DevTest Workstation](#) (page 117)
 - Start DevTest Workstation (Démarrer DevTest Workstation)
 - View a Suite (Afficher une suite)
 - View a Test Case (Afficher un scénario de test)

Autorisations standard

Une autorisation détermine si un utilisateur peut effectuer une activité spécifique.

Si une autorisation parente est octroyée, toutes ses autorisations enfants le seront également.

Les autorisations de niveau supérieur suivantes sont automatiquement créées.

Autorisations

[Autorisation d'administration de la console de LISA](#) (page 108)

[Autorisation User and Role Administration \(Administration des utilisateurs et des rôles\)](#) (page 108)

[Resource Administration Permission \(Autorisation d'administration des ressources\)](#) (page 109)

[Test and Suite Administration Permission \(Autorisation d'administration de tests et de suites\)](#) (page 109)

[Virtual Services Administration Permission \(Autorisation d'administration des services virtuels\)](#) (page 110)

[DevTest Server Administration Permission \(Autorisation d'administration de DevTest Server\)](#) (page 112)

[CVS Administration Permission \(Autorisation d'administration du service de validation en continu\)](#) (page 113)

[Report Administration Permission \(Autorisation d'administration des rapports\)](#) (page 114)

[Administration des mesures et des événements](#) (page 115)

[Administration de CA Continuous Application Insight](#) (page 116)

[Autorisation DevTest Workstation](#) (page 117)

[Cloud Lab Integration \(Intégration du laboratoire cloud\)](#) (page 119)

[Débogage du DevTest Server](#) (page 119)

Autorisation d'administration de la console de LISA

L'autorisation d'administration de la console de LISA contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Access LISA Console (Accès à la console LISA)	Booléen	Permet à un utilisateur de se connecter à la console DevTest.
Access Server Console (Accès à la console de serveur)	Booléen	Permet à un utilisateur de se connecter à la console de serveur.
Accès à la console Pathfinder (Accès à la console Pathfinder)	Booléen	Permet à un utilisateur de se connecter à la console Pathfinder.
View VSEasy Console (Afficher la console VSEasy)	Booléen	Permet à un utilisateur d'afficher la console VSEasy.

Autorisation User and Role Administration (Administration des utilisateurs et des rôles)

L'autorisation User and Role Administration (Administration des utilisateurs et des rôles) est une autorisation de type booléen qui permet à un utilisateur de gérer la liste de contrôle d'accès à partir de la console de serveur.

Resource Administration Permission (Autorisation d'administration des ressources)

La Resource Administration Permission (Autorisation d'administration des ressources) est une autorisation de type booléen qui permet à un utilisateur de gérer des [groupes de ressources](#) (page 137).

Test and Suite Administration Permission (Autorisation d'administration de tests et de suites)

L'autorisation Test/Suite Administration (Administration des mesures/événements) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Stage Test (Simuler le test)	Limite numérique	Permet à un utilisateur de simuler un scénario de test avec le nombre maximum spécifié d'utilisateurs virtuels.
Stage Suite (Simuler la suite)	Limite numérique	Permet à un utilisateur de simuler une suite avec le nombre maximum spécifié d'utilisateurs virtuels.
Stop Test (Arrêter le test)	Booléen	Permet à un utilisateur d'arrêter un test dans le moniteur de registre.
Kill Test (Éliminer le test)	Booléen	Permet à un utilisateur de supprimer un test du moniteur de registre.
Optimize Test (Optimiser le test)	Booléen	Permet à un utilisateur d'optimiser un test du moniteur de registre.
View Test (Afficher le test)	Booléen	Permet à un utilisateur d'afficher un test dans le moniteur de registre.
Quick Stage Test (Simulation rapide du test)	Booléen	Permet à un utilisateur de simuler un test rapide.
Stage Local Suite (Simuler une suite locale)	Booléen	Permet à un utilisateur d'exécuter une suite locale.

Virtual Services Administration Permission (Autorisation d'administration des services virtuels)

La Virtual Services Administration Permission (Autorisation d'administration des services virtuels) contient les autorisations enfants suivantes.

Niveau d'autorisation enfant 1	Niveau d'autorisation enfant 2	Niveau d'autorisation enfant 3	Type	Description
View VSE Dashboard (Afficher le tableau de bord du VSE)			Booléen	Permet à un utilisateur d'afficher le tableau de bord du VSE dans la console du serveur.
VSE Server Administration (Administration des serveurs du VSE)			Booléen	
	Configure VSE Tracking Data Cleanup (Configurer le nettoyage de données de suivi de VSE)		Booléen	Permet à un utilisateur de configurer le processus qui supprime des données de suivi antérieures à une durée spécifique.
	Stop VSE Server (Arrêter le serveur du VSE)		Booléen	Permet à un utilisateur d'arrêter un environnement de service virtuel.
	Reset VSE Server (Réinitialiser le serveur de VSE)		Booléen	Permet à un utilisateur de réinitialiser un environnement de service virtuel.
	Monitor VSE Server (Surveiller le serveur de VSE)		Booléen	Permet à un utilisateur de surveiller un environnement de service virtuel.
VSE Service Administration (Administration des services de VSE)			Booléen	
	VSE Service Deployment (Déploiement de services de VSE)		Booléen	Permet à un utilisateur de déployer un service virtuel.

	VSE Service Archive Retrieval (Récupération d'archive de service de VSE)		Booléen	Permet à un utilisateur de télécharger l'archive de modèle (MAR) associée à un service virtuel.
	VSE Service Execution (Exécution de service de VSE)		Booléen	
		Start VSE Service (Démarrer un service de VSE)	Booléen	Permet à un utilisateur de démarrer un service virtuel.
		Stop VSE Service (Arrêter un service de VSE)	Booléen	Permet à un utilisateur d'arrêter un service virtuel.
	Update Deployed VSE Service (Mettre à jour le service de VSE déployé)		Booléen	
		Update Virtual Service Capacity (Mettre à jour la capacité du service virtuel)	Booléen	Permet à un utilisateur de mettre à jour la capacité simultanée d'un service virtuel déployé.
		Update Virtual Service Think Scale (Mettre à jour le pourcentage de délai de réflexion du service virtuel)	Booléen	Permet à un utilisateur de mettre à jour le pourcentage de délai de réflexion d'un service virtuel déployé.
		Update Virtual Service Auto-Restart (Mettre à jour la valeur du redémarrage automatique du service virtuel)	Booléen	Permet à un utilisateur de mettre à jour l'option de redémarrage automatique d'un service virtuel déployé.
		Update Virtual Service Group Tag (Mettre à jour la balise d'un groupe de service virtuel)	Booléen	Permet à un utilisateur de mettre à jour la balise d'un groupe dans un service virtuel déployé.

	Set Virtual Service Execution Mode (Définir le mode d'exécution du service virtuel)		Booléen	Permet à un utilisateur de sélectionner un nouveau mode d'exécution pour un service virtuel déployé.
	Reset Virtual Service Transaction Counts (Réinitialiser les nombres de transactions du service virtuel)		Booléen	Permet à un utilisateur de réinitialiser les nombres de transactions et d'erreurs d'un service virtuel déployé.
	Heal Virtual Service Image (Réparer une image de service virtuel)		Booléen	Permet à un utilisateur d'effectuer une réparation de modèle.

DevTest Server Administration Permission (Autorisation d'administration de DevTest Server)

La DevTest Server Administration Permission (Autorisation d'administration de DevTest Server) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Débogage du DevTest Server	Booléen	Permet à un utilisateur de créer des images mémoires de segment de mémoire, des fils de discussion et d'effectuer un nettoyage de la mémoire pour un composant de serveur.
Monitor Registry (Surveiller le registre)	Booléen	Permet à un utilisateur d'accéder au moniteur de registre.
Reset Registry (Réinitialiser le registre)	Booléen	Permet à un utilisateur de réinitialiser le registre.
Stop Registry (Arrêter le registre)	Booléen	Permet à un utilisateur d'arrêter le registre.
Monitor Coordinator (Surveiller le coordinateur)	Booléen	Permet à un utilisateur d'afficher un message de statut du coordinateur dans la console du serveur ou le moniteur de registre.
Reset Coordinator (Réinitialiser le coordinateur)	Booléen	Permet à un utilisateur de réinitialiser un coordinateur dans la console du serveur ou le moniteur de registre.

Stop Coordinator (Arrêter le coordinateur)	Booléen	Permet à un utilisateur d'arrêter un coordinateur dans la console du serveur ou le moniteur de registre.
Monitor Simulator (Surveiller le simulateur)	Booléen	Permet à un utilisateur d'afficher un message de statut du simulateur dans la console du serveur ou le moniteur de registre.
Reset Simulator (Réinitialiser le simulateur)	Booléen	Permet à un utilisateur de réinitialiser un simulateur dans la console du serveur ou le moniteur de registre.
Stop Simulator (Arrêter le simulateur)	Booléen	Permet à un utilisateur d'arrêter un simulateur dans la console du serveur ou le moniteur de registre.

CVS Administration Permission (Autorisation d'administration du service de validation en continu)

La CVS Administration Permission (Autorisation d'administration du service de validation en continu) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
View CVS Dashboard (Afficher le tableau de bord du service de validation en continu)	Booléen	Permet à un utilisateur d'accéder au tableau de bord du service de validation en continu.
Deploy or re-deploy monitor to CVS (Déployer ou redéployer le moniteur vers le service de validation en continu)	Booléen	Permet à un utilisateur de déployer et redéployer des moniteurs vers le service de validation en continu.
Delete monitor from CVS (Supprimer le moniteur du service de validation en continu)	Booléen	Permet à un utilisateur de supprimer des moniteurs du service de validation en continu.
Run monitor immediately on CVS (Exécuter le moniteur immédiatement sur le service de validation en continu)	Booléen	Permet à un utilisateur d'exécuter des moniteurs immédiatement sur le service de validation en continu, quelle que soit leur planification d'exécution.
Activate/Deactivate monitor on CVS (Activer/Désactiver le moniteur sur le service de validation en continu)	Booléen	Permet à un utilisateur d'activer et de désactiver des moniteurs sur le service de validation en continu.

Report Administration Permission (Autorisation d'administration des rapports)

La Report Administration Permission (Autorisation d'administration des rapports) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Access reporting console (Accéder à la console de génération de rapports)	Booléen	Permet à un utilisateur d'accéder à la console de génération de rapports.
View report data (Afficher les données du rapport)	Booléen	Permet à un utilisateur d'afficher ses propres données de rapport dans la console de génération de rapports.
View report data of other users (Afficher les données de rapport d'autres utilisateurs)	Booléen	Permet à un utilisateur d'afficher les données de rapport d'autres utilisateurs dans la console de génération de rapports.
View PDF report data (Afficher les données du rapport au format PDF)	Booléen	Permet à un utilisateur d'afficher ses propres données de rapport au format de fichier PDF dans la console de génération de rapports.
View PDF report data of other users (Afficher les données de rapport PDF d'autres utilisateurs)	Booléen	Permet à un utilisateur d'afficher les données de rapport d'autres utilisateurs au format PDF dans la console de génération de rapports.
Import XML report data (Importer les données du rapport XML)	Booléen	Permet à un utilisateur d'importer des données XML dans la console de génération de rapports.
Export XML report data (Exporter les données du rapport XML)	Booléen	Permet à un utilisateur d'exporter ses propres données de rapport au format de fichier XML dans la console de génération de rapports.
Export XML report data of other users (Exporter les données de rapport XML d'autres utilisateurs)	Booléen	Permet à un utilisateur d'exporter les données de rapport d'autres utilisateurs au format de fichier XML dans la console de génération de rapports.
Export Excel report data (Exporter les données du rapport Excel)	Booléen	Permet à un utilisateur d'exporter ses propres données de rapport au format de fichier Excel dans la console de génération de rapports.
Export Excel report data of other users (Exporter les données de rapport Excel d'autres utilisateurs)	Booléen	Permet à un utilisateur d'exporter les données de rapport d'autres utilisateurs au format de fichier Excel dans la console de génération de rapports.
Delete report data (Supprimer les données de rapport)	Booléen	Permet à un utilisateur de supprimer ses propres données de rapport de la console de génération de rapports.

Delete report data of other users (Supprimer les données de rapport d'autres utilisateurs)	Booléen	Permet à un utilisateur de supprimer les données de rapport d'autres utilisateurs de la console de génération de rapports.
Create report filter (Créer un filtre de rapport)	Booléen	Permet à un utilisateur de créer un filtre dans la console de génération de rapports.
Delete report filter (Supprimer un filtre de rapport)	Booléen	Permet à un utilisateur de supprimer ses propres filtres de la console de génération de rapports.
Delete report filter of other users (Supprimer un filtre de rapport d'autres utilisateurs)	Booléen	Permet à un utilisateur de supprimer des filtres d'autres utilisateurs de la console de génération de rapports.
View all filters (Afficher tous les filtres)	Booléen	Permet à un utilisateur d'afficher tous les filtres des utilisateurs dans la console de génération de rapports.

Administration des mesures et des événements

L'autorisation Metric/Event Administration (Administration des mesures/événements) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Add metric at runtime (Ajouter une mesure à l'exécution)	Booléen	Permet à un utilisateur d'ajouter une mesure à l'exécution.
Remove metric at runtime (Supprimer une mesure à l'exécution)	Booléen	Permet à un utilisateur de supprimer une mesure à l'exécution.
Pause metrics collection (Interrompre la collecte de mesures)	Booléen	Permet à un utilisateur d'interrompre la collecte de mesures.
Save interval data (Enregistrer les données d'intervalle)	Booléen	Permet à un utilisateur d'enregistrer des données d'intervalle.
Save metric data (Enregistrer les données de mesure)	Booléen	Permet à un utilisateur d'enregistrer des données de mesure.
Save event data (Enregistrer les données de l'événement)	Booléen	Permet à un utilisateur d'enregistrer des données d'événement.

Administration de CA Continuous Application Insight

L'autorisation CA Continuous Application Insight (CAI) Administration (Autorisation d'administration de CA Continuous Application Insight CAI) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
View Paths (Afficher les chemins d'accès)	Booléen	Permet à un utilisateur d'afficher les chemins d'accès au portail DevTest.
Create Baselines (Créer des références)	Booléen	Permet à un utilisateur de créer des scénarios de test et des suites de référence dans le portail DevTest.
Create Virtual Service Models (Créer des modèles de service virtuel)	Booléen	Permet à un utilisateur de créer des modèles de service virtuel et des fichiers de trafic brut dans le portail DevTest.
Extract Data (Extraire les données)	Booléen	Permet à un utilisateur d'extraire des données de test de demandes ou de réponses XML dans le portail DevTest.
View Tickets (Afficher des tickets)	Booléen	Permet à un utilisateur d'afficher des tickets dans le portail DevTest.
Edit Tickets (Modifier des tickets)	Booléen	Permet à un utilisateur de modifier des tickets dans le portail DevTest.
View Agents (Afficher les agents)	Booléen	Permet à un utilisateur d'afficher les informations d'agent dans le portail DevTest.
Agent Administration (Administrateur de l'agent)	Booléen	Permet à un utilisateur d'arrêter et de démarrer la répartition d'un agent dans le portail <dt>.
Import Paths (Importer les chemins d'accès)	Booléen	Permet à un utilisateur d'importer un ou plusieurs chemins d'accès dans le portail DevTest.
Export Paths (Exporter les chemins d'accès)	Booléen	Permet à un utilisateur d'exporter un ou plusieurs chemins d'accès à partir du portail DevTest.
Create Document (Créer un document)	Booléen	Permet à un utilisateur de créer un document à partir de transactions dans le portail DevTest.
View Manual Cases (Afficher des scénarios manuels)	Booléen	Permet à un utilisateur d'afficher des scénarios manuels dans le portail DevTest.

Create Manual Cases (Créer des scénarios manuels)	Booléen	Permet à un utilisateur de créer des scénarios manuels dans le portail DevTest.
Edit Point of Interest (Modifier un point d'intérêt)	Booléen	Permet à un utilisateur de modifier des transactions de point d'intérêt dans le portail DevTest.
View Point of Interest (Afficher un point d'intérêt)	Booléen	Permet à un utilisateur d'afficher des transactions de point d'intérêt dans le portail DevTest.
View Defects (Afficher des défauts)	Booléen	Permet à un utilisateur d'afficher des transactions présentant des défauts dans le portail DevTest.

Autorisation DevTest Workstation

L'autorisation DevTest Workstation contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
Start DevTest Workstation (Démarrer DevTest Workstation)	Booléen	Permet à un utilisateur de démarrer DevTest Workstation.
View a Configuration (Afficher une configuration)	Booléen	Permet à un utilisateur d'afficher des configurations.
Modification d'une configuration	Booléen	Permet à un utilisateur de modifier des configurations.
Create a New Configuration (Créer une configuration)	Booléen	Permet à un utilisateur de créer des configurations.
View a Staging Document (Afficher un document de simulation)	Booléen	Permet à un utilisateur d'afficher des documents de simulation.
Edit a Staging Document (Modifier un document de simulation)	Booléen	Permet à un utilisateur de modifier des documents de simulation.
Create a New Staging Document (Créer un document de simulation)	Booléen	Permet à un utilisateur de créer des documents de simulation.
View a Suite (Afficher une suite)	Booléen	Permet à un utilisateur d'afficher des suites.
Edit a Suite (Modifier une suite)	Booléen	Permet à un utilisateur de modifier des suites.
Create a New Suite (Créer une suite)	Booléen	Permet à un utilisateur de créer des suites.
View a Test Case (Afficher un scénario de test)	Booléen	Permet à un utilisateur d'afficher des scénarios de test.
Edit a Test Case (Modifier un scénario de test)	Booléen	Permet à un utilisateur de modifier des scénarios de test.

Create a New Test Case (Créer un scénario de test)	Booléen	Permet à un utilisateur de créer des scénarios de test.
View an Audit Document (Afficher un document d'audit)	Booléen	Permet à un utilisateur d'afficher des documents d'audit.
Edit an Audit Document (Modifier un document d'audit)	Booléen	Permet à un utilisateur de modifier des documents d'audit.
Create a New Audit Document (Créer un document d'audit)	Booléen	Permet à un utilisateur de créer des documents d'audit.
View Virtual Service Model (Afficher un modèle de service virtuel)	Booléen	Permet à un utilisateur d'afficher des modèles de service virtuel.
Edit Virtual Service Model (Modifier un modèle de service virtuel)	Booléen	Permet à un utilisateur de modifier des modèles de service virtuel.
Create a New Virtual Service Model (Créer un modèle de service virtuel)	Booléen	Permet à un utilisateur de créer des modèles de service virtuel.
View Virtual Service Image (Afficher une image de service virtuel)	Booléen	Permet à un utilisateur d'afficher des images de service virtuel.
Edit Virtual Service Image (Modifier une image de service virtuel)	Booléen	Permet à un utilisateur de modifier des images de service virtuel.
Create a New Virtual Service Image (Créer une image de service virtuel)	Booléen	Permet à un utilisateur de créer des images de service virtuel.
Execute ITR (Exécuter un test interactif)	Booléen	Permet à un utilisateur de démarrer l'utilitaire d'exécution de test interactif.
Execute Instant Replay (Exécuter une relecture instantanée)	Booléen	Permet à un utilisateur de relire un scénario de test à un point spécifique dans l'utilitaire d'exécution de test interactif.
View ITR Properties (Afficher les propriétés de l'exécution de test interactif)	Booléen	Permet à un utilisateur d'afficher l'onglet Properties (Propriétés) dans l'utilitaire d'exécution de test interactif.
View ITR Test Events (Afficher les événements de test de l'exécution d'un test interactif)	Booléen	Permet à un utilisateur d'afficher l'onglet Test Events (Evénements de test) dans l'utilitaire d'exécution de test interactif.

Cloud Lab Integration (Intégration du laboratoire cloud)

L'autorisation Cloud Lab Integration (Intégration du laboratoire cloud) contient les autorisations enfants suivantes.

Autorisation enfant	Type	Description
List Available Labs (Liste des laboratoires disponibles)	Booléen	Permet à un utilisateur d'afficher la liste des laboratoires disponibles.
Start / Stop Labs (Démarrer/Arrêter les laboratoires)	Booléen	Permet à un utilisateur de démarrer et d'arrêter des laboratoires.
Expand Labs (Développer les laboratoires)	Booléen	Permet à un utilisateur de développer de façon dynamique un laboratoire de test.
Kill Other User's Labs (Arrêter des laboratoires d'un autre utilisateur)	Booléen	Permet à un utilisateur d'arrêter un laboratoire qu'un autre utilisateur a démarré.

Débogage du DevTest Server

Cette autorisation permet à un utilisateur de créer des images mémoires de segment de mémoire et de fils de discussion, et de lancer le nettoyage de la mémoire. Elle s'applique aux menus contextuels de la console de serveur et aux commandes émises à partir de l'utilitaire de ligne de commande [ServiceManager](#). (page 149)

Utilisateurs standard

Les utilisateurs standard sont créés lors du premier démarrage du registre. Un rôle dans un type d'utilisateur et un mot de passe par défaut sont affectés à chaque utilisateur standard. Pour connaître les autorisations associées à chaque rôle, consultez la section [Types d'utilisateur standard et rôles standard](#) (page 93).

Important : Pour empêcher l'accès non autorisé, il est recommandé de [modifier les mots de passe](#) (page 123) par défaut pour ces utilisateurs dès que possible.

admin

L'administrateur dispose du rôle Super User (Superutilisateur), un type de combinaison d'utilisateur avancé PF et SV. Le mot de passe par défaut est **admin**.

pfpower

L'utilisateur pfpower dispose du rôle PF Power (Avancé PF), un type d'utilisateur PF Power (Avancé PF). Le mot de passe par défaut est **pfpower**.

svpower

L'utilisateur svpower dispose du rôle SV Power (Avancé SV), un type d'utilisateur SV Power (Avancé SV). Le mot de passe par défaut est **svpower**.

tpower

L'utilisateur tpower dispose du rôle Test Power (Avancé Test), un type d'utilisateur Test Power (Avancé Test). Le mot de passe par défaut est **tpower**.

devtest

L'utilisateur devtest dispose du rôle Runtime (Exécution), un type d'utilisateur Runtime (Exécution). Le mot de passe par défaut est **devtest**.

sysadmin

L'utilisateur sysadmin dispose du rôle d'administrateur système, un type d'utilisateur Runtime (Exécution). Le mot de passe par défaut est **sysadmin**.

guest (invité)

L'utilisateur guest (invité) dispose du rôle Guest (Invité). Le mot de passe par défaut est **guest**.

Utilisation des rôles d'utilisateurs standard

DevTest Solutions est installé avec des utilisateurs standard ; chacun d'eux dispose d'informations d'identification uniques et d'un rôle différent. Pour préparer l'affectation de rôles à des utilisateurs nouveaux, utilisez les utilisateurs standard pour acquérir une expérience pratique des rôles. Vous pouvez vous connecter à l'aide des informations d'identification de chaque utilisateur standard pour mettre en pratique l'utilisation des autorisations associées aux différents rôles des utilisateurs.

Procédez comme suit:

1. Accédez à la console de serveur et connectez-vous en tant qu'utilisateur disposant du rôle de superutilisateur.

`http://nom-hôte:1505`

2. Développez le volet Administration dans la barre de navigation gauche. Dans la zone Security, le superutilisateur fournit des informations d'identification pour authentifier les utilisateurs et accorde des autorisations d'accès à des fonctionnalités via des affectations de rôle.
3. Cliquez sur Users (Utilisateurs).

Les utilisateurs standard apparaissent.

DevTest Users								
<input type="checkbox"/>	User Id	Roles						
		Super User	System Administration	PF Power	SV Power	Test Power	Runtime	Guest
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	sysadmin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	pfpower	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	svpower	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	tpower	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	devtest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Le mot de passe par défaut est identique à l'ID d'utilisateur de chaque utilisateur standard.

- Superutilisateur : admin, admin
- PF Power (Avancé PF) : pfpower, pfpower
- SV Power (Avancé SV) : svpower, svpower
- Test Power (Avancé Test) : tpower, tpower
- Runtime (Exécution) : devtest, devtest
- Administrateur système : sysadmin, sysadmin
- Guest (Invité) : guest, guest

4. Connectez-vous à chaque interface utilisateur et interface de ligne de commande à l'aide des informations d'identification d'un superutilisateur.
5. Examinez les fonctionnalités auxquelles les utilisateurs disposant de ce rôle peuvent accéder.
6. Répétez les deux dernières étapes avec d'autres utilisateurs standard.

Ce processus vous permet de préparer la configuration du contrôle d'accès (liste de contrôle d'accès). Configurez le contrôle d'accès en ajoutant des utilisateurs et en assignant des rôles qui accordent uniquement les autorisations nécessaires aux tâches qu'ils effectuent.

Important : Dans le cadre du contrôle d'accès, il est recommandé de [modifier les mots de passe des utilisateurs standard](#) (page 123). La modification des mots de passe est une manière d'éviter que des utilisateurs non autorisés accèdent à votre système.

Modification des mots de passe des utilisateurs standard

Lors du premier démarrage le registre, sept utilisateurs standard sont créés. Un rôle, type d'utilisateur et un mot de passe par défaut sont affectés à chaque utilisateur standard. Pour empêcher l'accès non autorisé, il est recommandé de modifier les mots de passe par défaut pour ces utilisateurs dès que possible.

Procédez comme suit:

1. Vérifiez que DevTest Solutions est en cours d'exécution. Consultez la section Démarrage des composants de serveur.
2. Accédez à la console DevTest.
`http://localhost:1505`
3. Connectez-vous à la console DevTest. Si vous ne disposez pas d'informations d'identification, appliquez l'une des approches suivantes :
 - Si vous prévoyez d'utiliser LDAP pour l'authentification, connectez-vous en tant que superutilisateur standard.
 - Si vous prévoyez de définir les informations d'identification des utilisateurs et que vous n'êtes pas encore défini comme utilisateur, créez un utilisateur avec le rôle de superutilisateur.
4. Cliquez sur Server Console (Console du serveur).
5. Cliquez sur l'onglet de navigation Administration.
6. Cliquez sur Users (Utilisateurs).
Les utilisateurs standard apparaissent.
7. Pour chaque utilisateur standard, procédez comme suit :
 - a. Cliquez sur Show User Details (Afficher les détails de l'utilisateur) pour l'un des utilisateurs standard.



- b. Saisissez un nouveau mot de passe dans le champ Password (Mot de passe).
 - c. Saisissez le nouveau mot de passe dans le champ Re-type Password (Confirmer le mot de passe).
 - d. Cliquez sur Save (Enregistrer).
8. Cliquez sur Logout (Déconnexion).

Affichage des informations d'utilisateur à partir de DevTest Workstation

Lorsque vous êtes connecté à la station de travail DevTest Workstation, vous pouvez ouvrir une boîte de dialogue qui fournit les informations suivantes :

- L'ID unique de votre nom d'utilisateur
- Les rôles qui vous sont affectés
- Autorisations disponibles

Procédez comme suit:

1. Dans le menu principal, sélectionnez System (Système), View Security Permissions (Afficher les autorisations de sécurité).

La boîte de dialogue User Security Permissions (Autorisations de sécurité d'utilisateur) s'ouvre.

2. Lorsque vous avez terminé, fermez la boîte de dialogue.

Gestion des utilisateurs et des rôles

Les administrateurs disposant de l'accès de superutilisateur gèrent les utilisateurs et les rôles dans le panneau Administration de la console de serveur. Tenez compte de l'approche suivante :

1. Examinez les rôles et les types d'utilisateur.
 - a. Sélectionnez des rôles.
 - b. Dans l'onglet Permissions (Autorisations), notez que les rôles disponibles sont répertoriés avec les types d'utilisateur associés. Par exemple, le rôle Test Administrator (Administrateur de tests) est associé au type d'utilisateur SV Power User (Utilisateur avancé SV).
 - c. Votre contrat de licence spécifie le nombre maximum d'utilisateurs simultanés autorisé pour chaque type d'utilisateur. Rappelez-vous de ce chiffre lors de l'affectation de rôles aux utilisateurs. Notez que de nombreux rôles sont mappés vers le même type d'utilisateur.
 - d. Examinez les autorisations associées à chaque rôle ; vous pouvez également personnaliser les autorisations.
 - e. De même, vous pouvez ajouter un nouveau rôle basé un rôle standard. Le nouveau rôle hérite du type d'utilisateur du rôle sur lequel il est basé.
2. Ajoutez tous les utilisateurs de DevTest.
 - a. Sélectionnez des utilisateurs.
 - b. DevTest utilise l'ID d'utilisateur et le mot de passe que vous spécifiez pour authentifier l'utilisateur nommé.
 - c. DevTest utilise le rôle que vous spécifiez pour autoriser l'utilisateur à effectuer différentes activités en fonction des autorisations accordées.
3. Vérifiez que tous vos utilisateurs sont convenablement configurés avec les rôles appropriés. Si vous avez personnalisé des rôles existants ou en avez ajouté de nouveaux, vérifiez la configuration.
4. **Sauvegardez votre base de données** de manière stratégique conformément à vos stratégies de maintenance internes. Cette précaution permet de récupérer rapidement la configuration d'utilisateurs et de rôles en cas d'endommagement de la base de données. La solution à un endommagement de base de données de listes de contrôle d'accès consiste à effectuer une restauration qui doit être gérée par l'administrateur de base de données.

Ajout, mise à jour et suppression d'utilisateurs

Utilisez la [console du serveur](#) (page 153) pour ajouter des utilisateurs, changer les détails d'un utilisateur et supprimer des utilisateurs. Les détails que vous pouvez changer incluent le mot de passe.

Le comportement relatif à la casse des ID d'utilisateur et des mots de passe diffère.

- Les ID d'utilisateur ne respectent pas la casse. Par exemple, les ID d'utilisateur **AAAA1** et **aaaa1** sont considérés comme la même valeur.
- Les mots de passe respectent la casse.

Vous ne pouvez pas supprimer l'utilisateur avec lequel vous êtes actuellement connecté.

Vous pouvez afficher ou masquer l'une des colonnes de la fenêtre Users (Utilisateurs). Cliquez sur la flèche déroulante dans une colonne. Sélectionnez Show/Hide Columns (Afficher/Masquer des colonnes). Sélectionnez ou désélectionnez les cases à cocher appropriées.

Pour ajouter un utilisateur :

1. Dans la console du serveur, affichez le panneau Administration.
2. Cliquez sur le noeud Users (Utilisateurs).
3. Au bas du panneau de droite, cliquez sur Add User (Ajouter un utilisateur).
La boîte de dialogue Add User (Ajouter un utilisateur) s'affiche.
4. Dans le champ User ID (ID d'utilisateur), entrez un ID unique pour l'utilisateur.
Vous pouvez entrer une combinaison de caractères alphanumériques, de trait d'union (-), de trait de soulignement (_), de point (.) et d'esperluette (&). Le nombre maximum de caractères autorisés est de 100.
5. Dans le champ Password (Mot de passe), entrez un mot de passe pour l'utilisateur.
Vous pouvez entrer une combinaison de caractères alphanumériques, de trait d'union (-), de trait de soulignement (_) et d'esperluette (&).
6. Dans le champ Re-type Password (Confirmer le mot de passe), entrez à nouveau le mot de passe.
7. Dans le champ Name (Nom), entrez le nom d'utilisateur.
Vous pouvez entrer une combinaison de caractères alphanumériques, de trait d'union (-), de trait de soulignement (_) et d'espaces. Le nombre maximum de caractères autorisés est de 100.
8. Dans le champ Misc Info (Informations diverses), entrez toutes informations supplémentaires.
Le nombre maximum de caractères autorisés est de 600.
9. Dans la zone Roles for the User (Rôles de l'utilisateur), sélectionnez un ou plusieurs rôles à affecter à l'utilisateur.

10. Cliquez sur Add User (Ajouter un utilisateur).
Le message User Added (Utilisateur ajouté) s'affiche.
11. Cliquez sur OK (Redéployer/déployer).

Pour mettre à jour un utilisateur :

1. Cliquez sur l'icône Show User Details (Afficher les détails d'utilisateur) à droite de l'ID d'utilisateur.
La boîte de dialogue Add Details (Détails de l'utilisateur) s'affiche.
2. Apportez les modifications nécessaires.
Vous pouvez afficher les autorisations pour un rôle en cliquant sur le nom du rôle.
3. Cliquez sur Save (Enregistrer).

Pour supprimer un utilisateur :

















1. Cochez la case à gauche de l'ID d'utilisateur.
2. Cliquez sur Delete User(s) (Supprimer les utilisateurs).
3. Cliquez sur Yes (Oui).

Ajout, mise à jour et suppression de rôles

Utilisez la [console du serveur](#) (page 153) pour ajouter des rôles, changer les détails d'un rôle et supprimer des rôles.

La console de serveur affiche les rôles et les autorisations sous forme de grille.

- Les autorisations s'affichent à gauche sous forme de lignes.
- Les rôles s'affichent dans la partie supérieure sous forme de colonnes. Le rôle à gauche a la priorité la plus élevée. Le rôle à droite a la priorité la plus faible. L'ordre prend son importance lorsqu'un utilisateur dispose de plusieurs rôles. La console de serveur permet de [changer l'ordre de priorité](#) (page 130).

Permissions		Roles							
Permissions		Super User	LISA Administrator	Test Administrator	Test Runner	Test Observer	Load Tester	User	Guest
🔑	LISA Console Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	User and Role Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Resource Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
🔑	Test/Suite Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Stage Test	 -1	 -1	 -1	 -1	 -1	 -1	 -1	 0
	Stage Suite	 -1	 -1	 -1	 -1	 -1	 -1	 -1	 0
	Stop Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Kill Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Optimize Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	View Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Quick Stage Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Stage Local Suite	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
🔑	Virtual Services Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	View VSE Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
🔑	VSE Server Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Configure VSE Tracking Data Cleanup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Stop VSE Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Reset VSE Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Monitor VSE Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
🔑	VSE Service Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	VSE Service Deployment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	VSE Service Archive Retrieval	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
🔑	VSE Service Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Start VSE Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si vous sélectionnez une autorisation parente, les autorisations enfants seront automatiquement sélectionnées. Si vous désélectionnez une autorisation parente, les autorisations enfants ne seront *pas* automatiquement désélectionnées. Si vous désélectionnez une autorisation enfant, les autorisations parentes seront automatiquement désélectionnées.

Vous pouvez afficher ou masquer l'une des colonnes de la fenêtre Roles. Cliquez sur la flèche déroulante dans la colonne Permissions (Autorisations). La flèche déroulante dans la colonne Permissions (Autorisations) s'affiche quand vous placez le pointeur de souris sur la colonne. Sélectionnez Show/Hide Columns (Afficher/Masquer des colonnes). Sélectionnez ou désélectionnez les cases à cocher appropriées.

Pour ajouter un rôle :

1. Dans la console du serveur, affichez le panneau Administration.
2. Cliquez sur le noeud Roles.

3. Au bas du panneau de droite, cliquez sur Add Role (Ajouter un rôle).
La boîte de dialogue Add Role (Ajouter un rôle) s'affiche.
4. Dans le champ Name (Nom), entrez le nom du rôle.
Vous pouvez entrer une combinaison de caractères alphanumériques, de trait d'union (-), de trait de soulignement (_) et d'espaces. Le nombre maximum de caractères autorisés est de 50.
5. Dans le champ Description, entrez la description du rôle.
Le nombre maximum de caractères autorisés est de 200.
6. Dans la zone Permissions for new Role (Autorisations du nouveau rôle), affectez des autorisations au rôle.
Vous pouvez utiliser la liste déroulante pour sélectionner un rôle existant sur lequel baser le nouveau rôle.
7. Cliquez sur Add role (Ajouter un rôle).
Une colonne est ajoutée pour le nouveau rôle. La colonne s'affiche à droite des rôles existants.

Pour mettre à jour un rôle :

1. Recherchez la colonne du rôle dans la grille des rôles et des autorisations.
2. Pour mettre à jour une autorisation de type [Boolean](#) (page 92) (Booléenne), sélectionnez ou désélectionnez la case à cocher.
3. Pour mettre à jour une autorisation de [limite numérique](#) (page 92) :
 - a. Cliquez sur l'icône de Numeric Limits (Limites numérique).
 - b. Pour le champ Maximum number of... (Nombre maximum de), sélectionnez Unlimited (Illimité), None (Aucun) ou entrez une valeur dans la limite numérique.
 - c. Cliquez sur Save (Enregistrer).
4. Pour mettre à jour une autorisation d'[élément de liste](#) (page 92):
 - a. Cliquez sur l'icône List items (Éléments de liste).
 - b. Ajoutez, modifiez, et supprimez des éléments de liste comme requis.
 - c. Cliquez sur Save (Enregistrer).
5. Cliquez sur Save (Enregistrer).

Pour supprimer un rôle :

1. Dans la grille de rôles et autorisations, sélectionnez le nom du rôle et cliquez sur la flèche déroulante.
2. Cliquez sur Delete Role (Supprimer un rôle).
3. Cliquez sur Yes (Oui).

Modification de l'ordre de priorité des rôles

La console de serveur affiche les rôles dans l'ordre de priorité. L'ordre prend son importance lorsqu'un utilisateur dispose de plusieurs rôles.

Procédez comme suit:

1. Dans la console du serveur, affichez le panneau Administration.
2. Effectuez l'une des actions suivantes :
 - Cliquez sur le noeud Roles.
 - Cliquez sur Display Roles (Afficher les rôles).
3. Cliquez sur Reorder Priority (Réorganiser la priorité).

La boîte de dialogue Reset Role Priority Order (Réinitialiser l'ordre de priorité des rôles) s'affiche.

4. Pour modifier l'ordre des rôles, sélectionnez les rôles et faites-les glisser vers la destination cible.
5. Cliquez sur Save Order (Enregistrer l'ordre).

Affichage du journal d'audit

Le journal d'audit contient une série d'entrées pour des activités contrôlées par la liste de contrôle d'accès (ACL). Chaque entrée inclut les informations suivantes :

Timestamp (Horodatage)

Date et heure de la création de l'entrée

User ID (ID de l'utilisateur)

ID unique de l'utilisateur

Rôle

Rôle affecté à l'utilisateur

Permission ID (ID d'autorisation)

Identificateur numérique de l'autorisation

Permission Name (Nom de l'autorisation)

Autorisation qui contrôle l'activité.

Status (Statut)

Activité autorisée ou refusée

Acted On (Action effectuée)

Nom du composant de serveur, du scénario de test ou du modèle de service virtuel
(le cas échéant)

Other Details (Informations complémentaires)

Autres informations (le cas échéant)

Procédez comme suit:

1. Dans la console du serveur, affichez le panneau Administration.
2. Effectuez l'une des actions suivantes :
 - Cliquez sur le noeud Audit Log (Journal d'audit).
 - Cliquez sur Display Audit Log (Afficher le journal d'audit).
3. Cliquez sur Refresh (Actualiser).

Utilitaire de ligne de commande **adduser**

Vous pouvez utiliser l'utilitaire de ligne de commande **adduser** pour ajouter un utilisateur. L'utilitaire est disponible dans le répertoire **LISA_HOME\bin** d'une installation de DevTest Server. Pour utiliser l'utilitaire, vous devez disposer de l'autorisation User and Role Administration (Administration des utilisateurs et des rôles).

L'utilitaire est au format suivant :

```
adduser -d userid -w password [-r role] -u userid -p password [-m registry_url]
```

Les options suivantes permettent d'affecter des informations de base au nouvel utilisateur :

- Utilisez l'option **-d** ou **--adduser** pour affecter un ID d'utilisateur au nouvel utilisateur.
- Utilisez l'option **-w** ou **--addpassword** pour affecter un mot de passe au nouvel utilisateur.
- (Facultatif) Utilisez l'option **-r** ou **--rolename** pour affecter un rôle au nouvel utilisateur. Si vous n'affectez pas de rôle, l'utilisateur ne disposera d'aucune autorisation jusqu'à ce qu'un rôle soit affecté à partir de la console du serveur.

Les options suivantes permettent de spécifier vos informations d'identification :

- Utilisez l'option **-u** ou **--username** pour spécifier votre ID d'utilisateur.
- Utilisez l'option **-p** ou **--password** pour spécifier votre mot de passe.

Si le registre est exécuté sur un ordinateur distant, utilisez l'option **-m** ou **--registry** pour spécifier l'URL du registre.

Exemple

Dans cet exemple, un utilisateur appelé **user1** est ajouté. Etant donné que le nom du rôle contient plusieurs termes, les guillemets sont utilisés.

```
adduser -d user1 -w password1 -r "Load Tester" -u admin -p myadminpassword
```

Configuration de la liste de contrôle d'accès pour l'utilisation de l'authentification LDAP

Vous pouvez configurer la liste de contrôle d'accès pour baser l'authentification d'utilisateur sur les informations d'un serveur LDAP, au lieu de la base de données de DevTest. Le processus d'autorisation continue d'utiliser la base de données de DevTest. L'administrateur de liste de contrôle d'accès doit consulter l'administrateur LDAP pour la configuration et l'implémentation basée sur les éléments de propriété décrits ci-après.

Remarque : Lorsque vous configurez une liste de contrôle d'accès pour utiliser le serveur LDAP, les utilisateurs peuvent se connecter uniquement avec des comptes qui figurent dans leur base de données LDAP. Les utilisateurs ne pourront pas utiliser des informations d'identification d'[utilisateur standard](#) (page 120) pour se connecter à une interface utilisateur ou une interface de ligne de commande DevTest.

Si l'utilisateur est authentifié via LDAP, mais qu'il n'existe pas dans la base de données de DevTest, il sera automatiquement ajouté à la base de données.

Pendant le processus de configuration, ajoutez les propriétés suivantes :

`lisa.acl.ldap.ldapUrl`

URL du serveur LDAP

`lisa.acl.ldap.securityPrincipal`

Nom unique de l'entité de sécurité

`lisa.acl.ldap.securityCredential`

Mot de passe de l'entité de sécurité. Lorsque le registre démarre, la chaîne **_enc** est ajoutée au nom de la propriété et la valeur est chiffrée.

`lisa.acl.ldap.securityAuthentication`

Niveau de sécurité à utiliser. Les valeurs valides sont **none (aucun)** et **simple**. Si vous ne définissez la valeur sur **none (aucun)**, l'appel d'authentification LDAP ignorera le mot de passe fourni par l'utilisateur et valide simplement le nom d'utilisateur. De plus, il n'est pas nécessaire d'inclure les propriétés **`lisa.acl.ldap.securityPrincipal`** et **`lisa.acl.ldap.securityCredential`**. Si vous définissez la valeur sur **simple**, le nom d'utilisateur et le mot de passe (transmis sous forme de texte clair) seront validés.

`lisa.acl.ldap.baseContext`

Nom unique du noeud dans lequel la recherche d'utilisateur commence.

`lisa.acl.ldap.userSearchFilter`

Filtre de recherche qui spécifie la classe d'objets pour des entrées d'utilisateur ; par exemple : **(objectClass=user)**.

`lisa.acl.ldap.usernameAttribute`

Attribut qui spécifie le nom d'utilisateur ; par exemple : **sAMAccountName**.

`lisa.acl.ldap.userSearchAllDepths`

Indique si la recherche doit être effectuée dans tous les sous-noeuds. Les valeurs valides sont **true** et **false**.

`lisa.acl.ldap.lisaDefaultRole`

Rôle par défaut affecté à un utilisateur ajouté à la base de données de DevTest après son authentification. Si vous n'incluez pas cette propriété, le rôle par défaut est Guest (Invité).

`lisa.acl.ldap.referralSupport`

Si le serveur LDAP utilise des références, vous pouvez utiliser cette propriété pour spécifier le type de référence. Les valeurs valides sont **follow** (suivre), **ignore** (ignorer) et **throw** (renvoyer). Si vous n'incluez pas cette propriété, la valeur par défaut sera **follow** (suivre).

Remarque : Si le fichier de propriétés inclut également la propriété **`lisa.acl.auth.enabled`** et que sa valeur est définie sur **true**, l'authentification LDAP ne fonctionnera pas correctement. Supprimez ou commentez la propriété **`lisa.acl.auth.enabled`**.

L'authentification LDAP utilise les mêmes boîtes de dialogue de connexion fournies pour le module de liste de contrôle d'accès par défaut.

Procédez comme suit:

1. Ouvrez le fichier **`local.properties`** ou **`site.properties`** sur l'ordinateur sur lequel se trouve le registre.
2. Ajoutez la ligne suivante :
`lisa.acl.auth.module.impl=com.itko.lisa.acl.custom.BaseLDAPAuthenticationModule`
3. Ajoutez les propriétés **`lisa.acl.ldap.*`** décrites précédemment dans cette rubrique. Par exemple :

```
lisa.acl.ldap.ldapUrl=ldap://172.24.255.255:389
lisa.acl.ldap.securityPrincipal=CN=admin,OU=users,DC=example,DC=com
lisa.acl.ldap.securityCredential=adminpwd
lisa.acl.ldap.securityAuthentication=simple
lisa.acl.ldap.baseContext=OU=users,DC=example,DC=com
lisa.acl.ldap.userSearchFilter=(objectClass=user)
lisa.acl.ldap.usernameAttribute=sAMAccountName
lisa.acl.ldap.userSearchAllDepths=true
```

```
lisa.acl.ldap.lisaDefaultRole=DevTest Administrator
```

4. Enregistrez le fichier **local.properties** ou **site.properties**.
5. Démarrez le registre.

Autorisation des utilisateurs authentifiés par LDAP

Lorsque vous configurez la liste de contrôle d'accès avec authentification LDAP des utilisateurs, spécifiez un rôle par défaut avec le paramètre suivant :

```
lisa.acl.ldap.lisaDefaultRole
```

Rôle par défaut affecté à un utilisateur ajouté à la base de données de DevTest après son authentification. Si vous n'incluez pas cette propriété, le rôle par défaut est Guest (Invité).

Lorsqu'un utilisateur se connecte avec des informations d'identification LDAP valides, LDAP authentifie l'utilisateur ; s'il n'existe pas dans la base de données de DevTest, une ligne est automatiquement ajoutée à la base de données. La ligne inclut l'ID d'utilisateur et le rôle actuellement spécifié pour **lisa.acl.ldap.lisaDefaultRole**.

Il existe treize rôles. Par exemple, vous pouvez définir le rôle par défaut sur Runtime (Exécution). Lorsque chaque utilisateur se connecte à une interface utilisateur ou une interface de ligne de commande DevTest la première fois, une ligne est ajoutée à la table devTest Users (Utilisateurs DevTest) avec leur ID d'utilisateur et leur rôle par défaut.

User Id	Name	Super User	DevTest Admini...	Test Administrator	System Adminis...	PF Power	SV Power	Test Power	Runtime	Test Runner	Test Observer	Load Tester	User	Guest
<input type="checkbox"/> ldapuser1		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ldapuser2		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ldapuser3		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ldapuser4		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pour mettre à jour la table devTest Users (Utilisateurs DevTest) via l'affectation de rôles spécifiques :

1. Demandez à tous les utilisateurs de DevTest de se connecter à DevTest Solutions, puis de se déconnecter.
2. Accédez à la console DevTest et connectez-vous.
`http://nom-hôte:1505`
3. Cliquez sur Server Console (Console de serveur), puis sur l'onglet Administratif dans le volet de navigation gauche.
4. Cliquez sur Users (Utilisateurs).
La table devTest Users (Utilisateurs DevTest) s'ouvre.
5. Pour chaque utilisateur, supprimez le rôle par défaut et sélectionnez le rôle approprié.
6. (Facultatif) pour afficher les autorisations d'un rôle dans le volet droit de la boîte de dialogue User Detail (Détails de l'utilisateur), cliquez sur l'icône Show User Details (Afficher les détails de l'utilisateur), puis sur le nom du rôle.
7. Cliquez sur Save (Enregistrer).

Pour mettre à jour la table devTest Users (Utilisateurs DevTest) automatiquement :

1. Définissez la valeur par défaut sur un rôle donné.
2. Demandez à tous les utilisateurs auxquels vous voulez affecter ce rôle de se connecter à DevTest Solutions, puis de se déconnecter.
3. Modifiez le rôle par défaut par un autre rôle.
4. Demandez à tous les utilisateurs auxquels vous voulez affecter ce rôle de se connecter à DevTest Solutions, puis de se déconnecter.
5. Répétez les étapes 3 et 4 pour chaque rôle.

groupes de ressources

Les groupes de ressources sont composés d'un ou plusieurs DevTest Servers ou VSE. Définissez des groupes de ressources pour déterminer les ressources auxquelles un utilisateur ou un projet peuvent accéder.

Lors de l'utilisation d'une liste de contrôle d'accès (ACL), associez des rôles à des groupes de ressources pour déterminer les rôles pouvant agir sur des ressources.

Cette section comprend les rubriques suivantes :

[Gestion des groupes de ressources](#) (page 138)

[Affection de rôles à des groupes de ressources](#) (page 139)

[Utilisation de groupes de ressources pour le contrôle d'accès](#) (page 140)

Gestion des groupes de ressources

Utilisez la console du serveur pour ajouter des groupes de ressources, changer les détails d'un groupe de ressources, supprimer des groupes de ressources et supprimer une ressource d'un groupe de ressources.

Vous pouvez afficher ou masquer l'une des colonnes de la fenêtre Resource Groups (Groupes de ressources). Cliquez sur la flèche déroulante dans une colonne. Sélectionnez Show/Hide Columns (Afficher/Masquer des colonnes). Sélectionnez ou désélectionnez les cases à cocher appropriées.

Pour ajouter un groupe de ressources :

1. Dans la console du serveur, affichez le panneau Administration.
2. Cliquez sur le noeud Resource Groups (Groupes de ressources).
3. Au bas du panneau de droite, cliquez sur Add Resource Group (Ajouter un groupe de ressources). La boîte de dialogue Add Resource Group (Ajouter un groupe de ressources) s'affiche.
4. Dans le champ Name (Nom), entrez le nom du groupe de ressources. Le nom doit contenir uniquement des caractères alphanumériques, des espaces, des traits d'union ou des traits de soulignement.
5. Dans le champ Description, entrez une description du groupe de ressources.
6. Sélectionnez un ou plusieurs groupes de ressources en cochant la case située à côté de ces groupes.
7. Cliquez sur Add (Ajouter).

Le panneau Resource Groups (Groupes de ressources) affiche la ressource et le groupe de ressources associé dans la colonne Resource Groups (Groupes de ressources).

Pour afficher des groupes de ressources :

1. Pour actualiser l'affichage, cliquez sur Refresh (Actualiser) dans le coin supérieur droit de la fenêtre.
2. Les étiquettes des ressources inactives, mais toujours associées à un groupe, apparaissent avec le texte barré.

Pour supprimer un groupe de ressources :

1. Sélectionnez le triangle noir situé à côté du nom du groupe de ressources.
2. Dans la liste déroulante, sélectionnez Delete Resource Group (Supprimer le groupe de ressources).
3. Cliquez sur Yes (Oui) dans la boîte de dialogue Delete Resource Group (Supprimer le groupe de ressources).

Pour supprimer une ressource d'un groupe de ressources :

Remarque : Vous ne pouvez pas supprimer de ressource d'un groupe de ressources si elle est active.

Désélectionnez la case à cocher située à côté du groupe de ressources et cliquez sur Save (Enregistrer).

Affectation de rôles à des groupes de ressources

Pour accorder des rôles à des groupes de ressources, utilisez la console du serveur.

Procédez comme suit:

1. Sélectionnez Administration, Security (Sécurité), Resource Groups (Groupes de ressources).
2. Sélectionnez les cases à cocher pour les rôles à associer à chaque groupe de ressources.
3. Cliquez sur Save (Enregistrer).

Utilisation de groupes de ressources pour le contrôle d'accès

Vous pouvez utiliser des groupes de ressources pour contrôler l'accès aux ressources en plus des listes de contrôle d'accès.

Procédez comme suit:

1. Ajoutez les groupes de ressources appropriés pour votre organisation. Pour obtenir des instructions, consultez la section [Gestion des groupes de ressources](#) (page 138).
2. Pour ouvrir un fichier de configuration dans DevTest Workstation, double-cliquez dessus dans le panneau Project (Projet).
3. Cliquez sur l'icône Add (Ajouter) au bas du panneau.
4. Cliquez sur la colonne Key (Clé) dans l'éditeur Properties Editor (Editeur de propriétés).
5. Dans la liste de propriétés, sélectionnez RESOURCE_GROUP.
6. Cliquez sur la colonne Value (Valeur).
7. Entrez le groupe de ressource que vous souhaitez associer à cette configuration.
Vous pouvez uniquement sélectionner un groupe de ressources dans la liste déroulante, mais vous pouvez modifier la colonne Value (Valeur) pour entrer une liste de groupes de ressources, séparés par des virgules.
8. Pour enregistrer la configuration, cliquez sur Save (Enregistrer).

Un scénario de test, une suite de tests ou un module de service virtuel simulé à l'aide de cette configuration peut uniquement utiliser les ressources définies dans le groupe de ressources.

Remarque : L'association de groupe de ressources s'applique uniquement lorsque la configuration constitue la configuration active.

Chapitre 5: Logging (Journalisation)

Ce chapitre traite des sujets suivants :

[Présentation des fichiers journaux](#) (page 141)

[Fichier de propriétés de journalisation](#) (page 144)

[Messages relatifs au statut pour les composants de serveur](#) (page 145)

[Fils de discussion automatiques](#) (page 146)

[Enregistreur d'étape de test](#) (page 147)

Présentation des fichiers journaux

Cette section présente les fichiers journaux suivants et leur emplacement.

- [Fichiers journaux principaux](#) (page 142)
- [Fichiers journaux du serveur de démonstration](#) (page 143)

Fichiers journaux principaux

Les fichiers journaux principaux incluent les suivants :

- **coordinator.log** : sortie de journalisation pour le coordinateur
- **cvsmgr.log** : sortie de journalisation pour le service de validation en continu (CVS)
- **devtest_broker_pid.log** : sortie de journalisation pour le composant intermédiaire de l'agent Java pour DevTest
- **devtest_console_pid.log** : sortie de journalisation pour le composant console de l'agent Java pour DevTest
- **marmaker.log** : sortie de journalisation pour l'utilitaire de ligne de commande Make Mar
- **pfbroker.log** : sortie de journalisation cumulée pour le composant intermédiaire de l'agent Java pour DevTest
- **portal.log** : sortie de journalisation pour le portail DevTest
- **registry.log** : sortie de journalisation pour le registre
- **simulator.log** : sortie de journalisation pour le simulateur
- **svcmgrmgr.log** : sortie de journalisation pour l'utilitaire de ligne de commande du gestionnaire d'images de service
- **svcmgr.log** : sortie de journalisation pour l'utilitaire de ligne de commande du gestionnaire de services
- **trunner.log** : sortie de journalisation pour l'utilitaire de ligne de commande Test Runner (Exécuteur de tests)
- **vse.log** : sortie de journalisation pour le serveur du VSE
- **vsemgr.log** : sortie de journalisation pour l'utilitaire de ligne de commande du gestionnaire de VSE
- **vse_xxx.log** : sortie de journalisation pour les conversations du VSE et la navigation d'images de service, xxx étant le nom de l'image de service
- **workstation.log** : sortie de journalisation pour DevTest Workstation

La propriété **lisa.tmpdir** contrôle l'emplacement de ces fichiers journaux. Pour afficher la valeur de la propriété **lisa.tmpdir** dans la station de travail DevTest Workstation :

1. Dans le menu principal, cliquez sur Help (Aide), puis sur DevTest Runtime Info (Informations d'exécution DevTest).
2. Cliquez sur l'onglet System Properties (Propriétés système) et recherchez **lisa.tmpdir**.

Si le registre, le coordinateur, le simulateur ou le VSE est [exécuté en tant que service Windows](#) (page 19), les fichiers journaux seront présents dans le répertoire **LISA_HOME\lisatmp**.

Remarque : Même si **lisa.tmpdir** permet de changer l'emplacement de stockage de vos fichiers temporaires, CA Technologies recommande de ne pas modifier cette propriété pour enregistrer les fichiers temporaires à un emplacement de point de montage externe ou de partage externe. Si le produit présente des problèmes d'instabilité et que vous utilisez un partage externe pour le stockage de fichiers temporaires, le service de support peut vous indiquer de revenir à l'utilisation d'un disque local pour le stockage de fichiers temporaires pour obtenir une prise en charge continue de votre environnement.

Fichiers journaux du serveur de démonstration

Le serveur de démonstration contient ses propres fichiers journaux, disponibles dans le répertoire **lisa-demo-server/jboss/server/default/log**.

La propriété **lisa.tmpdir** ne contrôle pas cet emplacement.

Les fichiers journaux du serveur de démonstration sont les suivants :

- boot.log
- server.log

Fichier de propriétés de journalisation

DevTest utilise la structure de journalisation log4j d'Apache. Le fichier **logging.properties** dans le répertoire de **LISA_HOME** permet de configurer le comportement de la journalisation.

Pour obtenir plus d'informations sur la journalisation à partir de DevTest Workstation, vous pouvez changer le niveau de journalisation dans le fichier **log4j.rootCategory**.

```
log4j.rootCategory=INFO,A1
```

Ce fichier contient un ensemble d'enregistreurs pour des composants tiers fournis avec DevTest. Les niveaux de journalisation par défaut pour ces enregistreurs ont pour but d'empêcher les composants tiers de submerger les fichiers journaux avec un nombre excessif messages. Il n'est en général pas nécessaire de changer les niveaux de journalisation.

```
log4j.logger.com.teamdev=WARN
log4j.logger.EventLogger=WARN
log4j.logger.org.apache=ERROR
log4j.logger.com.smardec=ERROR
log4j.logger.org.apache.http=ERROR
log4j.logger.org.apache.http.header=ERROR
log4j.logger.org.apache.http.wire=ERROR
log4j.logger.com.mchange.v2=ERROR
log4j.logger.org.hibernate=WARN
log4j.logger.org.jfree=ERROR
log4j.logger.com.jniwrapper=ERROR
log4j.logger.sun.rmi=INFO
```

L'annexe par défaut est **com.itko.util.log4j.TimedRollingFileAppender**. Les instructions de journal pour un composant sont ajoutées à un fichier sauvegardé lorsqu'il atteint une certaine taille. La taille de fichier maximum par défaut est de 10 Mo. Le nombre par défaut de fichiers sauvegardés est 5.

```
log4j.appender.A1=com.itko.util.log4j.TimedRollingFileAppender
log4j.appender.A1.File=${lisa.tmpdir}/${LISA_LOG}
log4j.appender.A1.MaxFileSize=10MB
log4j.appender.A1.MaxBackupIndex=5
log4j.appender.A1.layout=org.apache.log4j.EnhancedPatternLayout
log4j.appender.A1.layout.ConversionPattern=%d{ISO8601}{UTC}Z (%d{HH:mm}) [%t]
%-5p %-30c - %m%n
```

Les fichiers de sauvegarde sont placés dans le même répertoire que le fichier journal. Par exemple, si le fichier journal pour le registre a été sauvegardé trois fois, le répertoire contient les fichiers suivants :

- registry.log
- registry.log.1

- registry.log.2
- registry.log.3

Les dispositions contrôlent le format des instructions de journal. La disposition par défaut est **org.apache.log4j.EnhancedPatternLayout**. Le modèle de conversion par défaut est **%d{ISO8601}{UTC}Z (%d{HH:mm}) [%t] %-5p %-30c - %m%n**. Ce modèle de conversion spécifie qu'une instruction de journal inclut la date, le thread, la priorité, la catégorie et le message. Par exemple :

```
2014-11-20 14:09:08,152Z (07:09) [main] INFO com.itko.lisa.net.ActiveMQFactory
- Starting amq broker
```

La date utilise l'UTC (Temps universel coordonné). Cette convention facilite le suivi des événements de journaux lorsque le registre est exécuté dans un fuseau horaire différent de celui de DevTest Workstation.

Pour plus d'informations sur les propriétés de fil de discussion, reportez-vous à la section [Fils de discussion automatiques](#) (page 146).

Messages relatifs au statut pour les composants de serveur

Les composants de serveur suivants écrivent des messages relatifs au statut dans leurs fichiers journaux à un intervalle spécifique :

- Registre
- Coordinateur
- Simulateur
- VSE

L'exemple suivant a été écrit dans un fichier journal par le registre.

```
2012-03-05 12:48:01,136 [Event Sink Thread Pool Thread 1] INFO
com.itko.lisa.coordinator.TestRegistryImpl -
Coordinator Servers: 0 Simulator Servers: 0 VSEs: 0 Running vusers: 0 Labs: 1
Memory used 83mb, allocated 158mb, max 227mb (36%) labSims: 0 labVSEs: 0 labCoords:
0
Our cpu usage 0%, system cpu used 16%
```

L'intervalle par défaut des messages de statut est de 30 secondes. Vous pouvez changer l'intervalle en modifiant les propriétés suivantes dans le fichier **lisa.properties** :

- lisa.defaultRegistry.pulseInterval
- lisa.coordinator.pulseInterval
- lisa.simulator.pulseInterval
- lisa.vse.pulseInterval

Fils de discussion automatiques

Vous pouvez utiliser le fichier **logging.properties** pour activer des fils de discussion automatiques, qui sont utiles en cas de problèmes de performances de débogage.

Recherchez la propriété suivante et remplacez **WARN (avertir)** par **INFO**.

```
log4j.logger.threadDumpLogger=warn, THREAD_DUMPS
```

Pour désactiver les fils de discussion, remplacez **INFO** par **WARN (avertir)**.

L'intervalle par défaut des fils de discussion est de 30 secondes. Vous pouvez changer l'intervalle en modifiant la propriété **lisa.threadDump.interval** dans le fichier **lisa.properties**.

Enregistreur d'étape de test

Comme l'indique la section *Eléments d'une étape de test* de la rubrique *Utilisation de CA Application Test*, chaque étape de test inclut un élément du message de journal.

Pour envoyer le message de journal à un fichier spécifique lors de l'exécution, ajoutez les propriétés suivantes au fichier **logging.properties** dans le répertoire **LISA_HOME**.

```
log4j.logger.com.itko.lisa.test.StepLogger=DEBUG, A2
log4j.additivity.com.itko.lisa.test.StepLogger=false
log4j.appender.A2=org.apache.log4j.RollingFileAppender
log4j.appender.A2.File=${lisa.tmpdir}/log.log
log4j.appender.A2.MaxFileSize=10MB
log4j.appender.A2.MaxBackupIndex=5
log4j.appender.A2.layout=org.apache.log4j.PatternLayout
log4j.appender.A2.layout.ConversionPattern=%d [%t] %-5p %-30c - %m%n
```

Les valeurs des propriétés **File** (Fichier), **MaxFileSize** (Taille maximum de fichier) et **MaxBackupIndex** (Index maximum de sauvegarde) peuvent être différentes des valeurs indiquées dans l'exemple précédent.

Remarque : Après avoir ajouté les propriétés, redémarrez DevTest Workstation (s'il est déjà en cours d'exécution).

Le message obtenu dans le fichier journal est similaire à l'exemple suivant :

```
2012-07-11 17:32:59,390 [basic-test/basic-test [QuickStageRun]/0] DEBUG
com.itko.lisa.test.StepLogger -
LOG basic-test,basic-test [QuickStageRun],local,0,3,my log message
```

La partie du message qui suit **LOG** comprend six composants :

- Nom du scénario de test
- Nom du document de simulation.
- Nom du simulateur
- Nombre d'instances/utilisateurs virtuels. Dans un test comptant dix utilisateurs virtuels, ce nombre varie de 1 à 10.
- Nombre de cycles. Ce nombre s'applique à des situations dans lesquelles le document de simulation est configuré pour exécuter le test en boucle jusqu'à ce qu'une certaine condition se produise. La valeur correspond au nombre d'exécutions du test par cet utilisateur virtuel particulier.
- Message de journal défini dans l'étape de test

Chapitre 6: surveillance

Vous pouvez surveiller DevTest Solution à l'aide de l'utilitaire de ligne de commande du gestionnaire de services, de la console de serveur Web, du moniteur de registre ou du tableau de bord Enterprise Dashboard.

Ce chapitre traite des sujets suivants :

[Service Manager \(Gestionnaire de services\)](#) (page 149)

[Ouverture de la console du serveur](#) (page 153)

[Affichage du récapitulatif d'intégrité des composants](#) (page 154)

[Affichage du détail des performances des composants](#) (page 155)

[Création d'images mémoires de segment de mémoire et de fils de discussion](#) (page 156)

[Nettoyage de la mémoire forcé](#) (page 157)

[Utilisation du moniteur de registre](#) (page 158)

[Utilisation du tableau de bord Enterprise Dashboard](#) (page 160)

Service Manager (Gestionnaire de services)

L'utilitaire de ligne de commande du ServiceManager (Gestionnaire de services) permet d'effectuer diverses actions avec un registre, un coordinateur, un simulateur, ou le serveur de VSE.

```
ServiceManager [- - command]=service-name
```

service-name correspond au nom du service à affecter.

Vous pouvez répéter la paire commande-nom.

Pour rechercher le nom, placez une clé lisa.properties entre accolades doubles. Par exemple :

```
{{lisa.registryName}}
```

Exemple de noms de service :

- tcp://localhost:2010/Registry
- Simulator (resolves to tcp://localhost:2014/Simulator)

Options du gestionnaire de services

-h, --help

Affiche le texte d'aide.

-s service-name, --status=service-name

Affiche un message de statut du service. Pour que service-name renvoie des messages de statut pour tous les services enregistrés, saisissez *all*.

-r service-name, --reset=service-name

Conserve le service en mémoire, mais actualise son état.

-o service-name, --stop=service-name

Indique au service de se finaliser.

-i valid-remote-init-service-name, --initialize=valid-remote-init-service-name

Initialise un service à distance.

-t service-name, --threaddump=service-name

Indique au service de générer un fil de discussion (trace de pile) pour les diagnostics.

-b simulator-name, --attached=simulator-name

Indique au simulateur de renvoyer une liste des appareils mobiles connectés.

-e service-name, --heapdump=service-name

Indique au service de créer un fichier .hprof pour les diagnostics de mémoire.

-g service-name, --gc=service-name

Indique au service de forcer le nettoyage de la mémoire Java.

-d service-name, --diagnostic=service-name

Crée un fichier .zip qui contient des fichiers de diagnostic pour le service. Si le service est un registre, le fichier .zip contiendra également des fichiers de diagnostic pour tous les coordinateurs, simulateurs et serveurs de VSE connectés. En règle générale, vous utilisez cette option lorsque vous y êtes invité par le service de support.

loglevel

Cette option inclut également un paramètre facultatif, secondaire, appelé **loglevel**, suivi par l'un des mots clés loglevel suivants : error (erreur), warn (avertissement), info, debug (débogage), trace.

Par exemple, **ServiceManager -d tcp://10.1.1.23:2010/Registry loglevel debug** définit le niveau de journalisation de tous les composants, y compris des agents, sur le niveau debug (débogage). Le gestionnaire de services écrit alors le message suivant :

Log levels set to debug (Niveaux de journalisation définis sur débogage).
Run your repro steps, then press return to restore log levels and capture diagnostic (Exécutez vos étapes de reproduction, puis appuyez sur Retour pour restaurer des niveaux de journalisation et capturer le diagnostic).

Le fichier .zip généré contient des journaux de niveau de journalisation debug pour tous les composants connectés, les fils de discussion, les informations de licence et les propriétés. Ce fichier .zip contient également les journaux pour chaque agent connecté à l'intermédiaire du registre.

Remarque : Si la commande -d est envoyée vers un VSE, un coordinateur ou un serveur de simulation, seuls les journaux et le diagnostic pour ce composant seront inclus dans le fichier .zip.

Les agents n'ont pas de niveau de journal de trace, mais le niveau de journalisation dev (développement) est similaire et traité comme tel.

-u username, --username=username

Utilisez cette commande pour spécifier votre nom d'utilisateur.

-p password, --password=password

Utilisez cette commande pour spécifier votre mot de passe.

--version

Imprime le numéro de version.

-m registry-name, --registry-name=registry-name

Utilisée avec la commande *initialize* pour spécifier un registre auquel se connecter

-n component-name, --component-name=registry-name

Utilisée avec la commande *initialize* pour spécifier un nom du composant

-l lab-name, --lab-name=lab-name

Utilisée avec *initialize* pour spécifier un nom de laboratoire à créer.

-a app-name, --app=app-name

Utilisée avec la commande *initialize* pour spécifier une ID d'application de serveur

Exemple :

Si vous voulez nommer un simulateur *MySim*, puis le connecter au registre *MyRegistry* et démarrer un nouveau laboratoire nommé *MyDevLab*, saisissez :

```
./SimulatorService -n MySim -m tcp://1.2.3.4:2010/MyRegistry -l MyDevLab
```

Pour ajouter un deuxième simulateur à ce laboratoire :

```
./SimulatorService -component-name=MySecondSim  
-registry-name=tc;"/1.2.3.4:2010/MyRegistry -lab-name=MyDevLab
```

Pour ajouter un VSE à ce registre, mais dans un laboratoire différent :

```
./VirtualServiceEnvironment -n CoreServices -m  
tcp://1.2.3.4:2010/MyRegistry -l QA
```

Exemples du gestionnaire de services

Dans l'exemple suivant, le statut du registre est vérifié.

```
ServiceManager -s Registry  
Coordinator Servers: 1 Simulator Servers: 2 VSEs: 1 Running vusers: 0  
Labs: 1 Memory used 76mb, allocated 155mb, max 253mb (30%)  
labSims: 2 labVSEs: 1 labCoords: 1
```

Dans l'exemple suivant, le statut de l'ensemble des services enregistrés est vérifié.

```
Coordinator Server: tcp://bdert-mbp.local:2011/Coordinator  
OK: 1 Coordinators running. Memory used 223mb, allocated 461mb, max 910mb (24%)  
Our cpu usage 0%, system cpu used 8%  
Simulator Server: tcp://bdert-mbp.local:2014/Simulator  
OK: 1 Simulators running. Memory used 301mb, allocated 437mb, max 910mb (33%) Our  
cpu usage 0%, system cpu used 8%
```

Dans l'exemple suivant, le registre s'arrête.

```
ServiceManager -o Registry  
Sending stop request to Registry.
```

Dans l'exemple suivant, un fil de discussion pour le serveur de VSE est généré.

```
ServiceManager --threaddump=tcp://remote.host.com:2013/VSE  
< a bunch of stack traces >
```

Dans l'exemple suivant, un nettoyage de la mémoire Java du serveur de VSE est forcé.

```
ServiceManager --gc=VSE  
After GC: Memory used 55mb, allocated 225mb, max 246mb (22%)
```

Dans l'exemple suivant, un fichier .zip contenant des journaux de niveau trace pour tous les composants connectés au registre est généré.

```
ServiceManager --diagnostic=Registry loglevel TRACE
```

Dans l'exemple suivant, un fichier .zip contenant des journaux de niveau debug (débogage) pour le simulateur est généré.

```
ServiceManager -d Simulator loglevel debug
```


Ouverture de la console du serveur

Vous pouvez ouvrir la console du serveur à partir de DevTest Workstation ou d'un navigateur Web.

Pour ouvrir la console du serveur à partir de DevTest Workstation :

Sélectionnez View (Afficher), Server Console (Console du serveur) dans le menu principal.

Pour ouvrir la console du serveur à partir d'un navigateur Web :

1. Vérifiez que le registre est exécuté.
2. Dans un navigateur Web, entrez **http://localhost:1505/**.
Si le registre se trouve sur un ordinateur distant, remplacez **localhost** par le nom ou l'adresse IP de l'ordinateur.
La console DevTest s'affiche.
3. Cliquez sur Server Console (Console du serveur).

Affichage du récapitulatif d'intégrité des composants

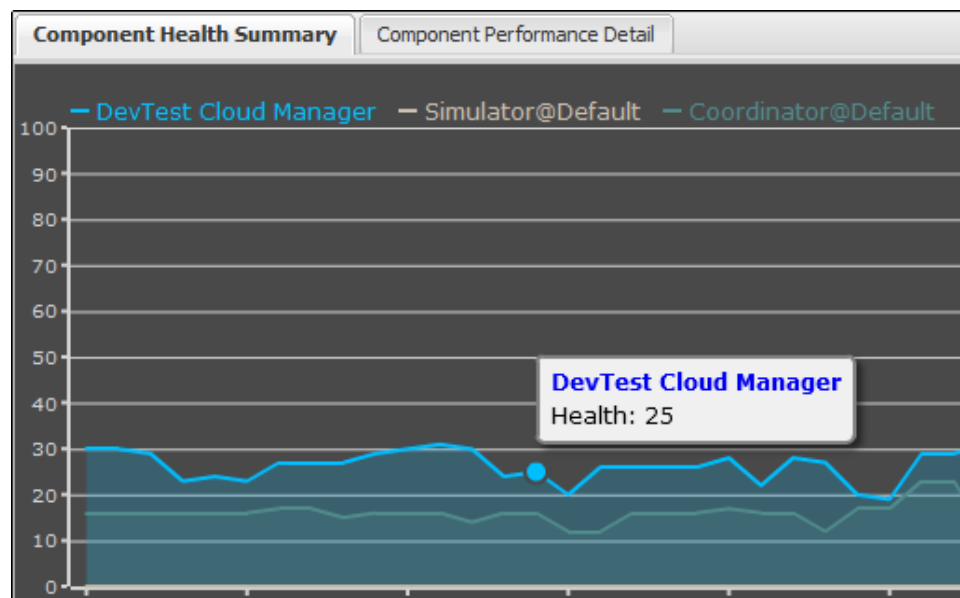
L'onglet Component Health Summary (Récapitulatif de l'intégrité des composants) dans la console du serveur fournit un indicateur de l'intégrité globale des composants en cours d'exécution.

L'indicateur d'intégrité s'affiche sur une échelle de 0 à 100. La valeur est issue des statistiques suivantes :

- Charge d'UC globale
- Quantité d'UC utilisée par le serveur
- Quantité du segment de mémoire utilisé par le serveur même

La valeur 0 représente un système inactif. La valeur 100 représente un système ayant atteint le maximum.

L'image suivante illustre l'onglet Component Health Summary (Récapitulatif de l'intégrité des composants). L'Axe X représente le temps. L'axe Y représente la valeur de l'indicateur d'intégrité.



Pour afficher le récapitulatif d'intégrité des composants :

1. Accédez à la console du serveur.
2. Dans le panneau Network DevTest (Réseau DevTest), cliquez sur le noeud DevTest Cloud Manager.

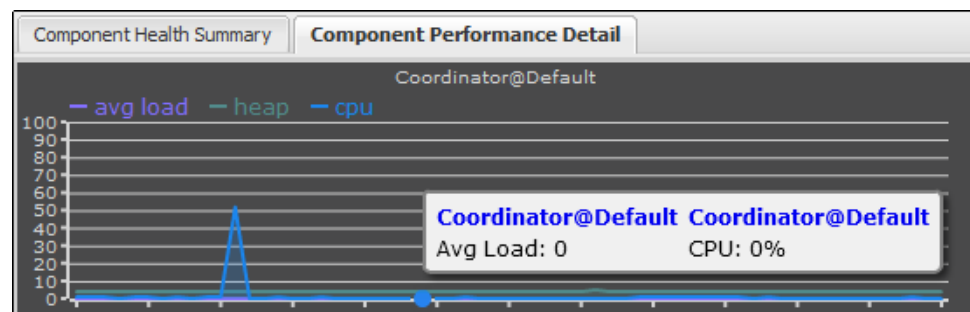
Les données s'affichent dans l'onglet Component Health Summary (Récapitulatif de l'intégrité des composants).

Affichage du détail des performances des composants

L'onglet Component Performance Detail (Détail des performances des composants) dans la console du serveur permet d'afficher les statistiques de performances suivantes sur des membres de laboratoire en cours d'exécution :

- **Average load (Charge moyenne)** : la valeur s'affiche sous forme de nombre entier.
- **Heap (Segment de mémoire)** : la valeur est exprimée sous forme de pourcentage.
- **CPU (UC)** : la valeur est exprimée sous forme de pourcentage.

L'image suivante contient les données de performances pour un coordinateur dans le laboratoire Default (Par défaut). Les info-bulles pour les mesures de charge moyenne et d'UC s'affichent.



Pour afficher les détails des performances des composants :

1. Accédez à la console du serveur.
2. Dans le panneau Network DevTest (Réseau DevTest), cliquez sur le noeud DevTest Cloud Manager.
3. Cliquez sur l'onglet Component Performance Detail (Détail des performances des composants).
4. Cliquez avec le bouton droit de la souris sur un membre de laboratoire dans le graphique de réseau et sélectionnez View Performance (Afficher les données de performance).

Le membre de laboratoire est ajouté à l'onglet Component Performance Detail (Détail des performances des composants). Les mesures s'affichent avec des couleurs différentes. Chaque mesure fournit une info-bulle.

Création d'images mémoires de segment de mémoire et de fils de discussion

La console du serveur permet de créer des images mémoires de segment de mémoire et des fils de discussion pour un composant de serveur.

Généralement, vous effectuez ces procédures uniquement lorsque vous y êtes invité par le service de support clientèle.

Vous pouvez également créer une image mémoire de segment de mémoire à l'aide de l'utilitaire de ligne de commande du gestionnaire de services.

Pour créer une image mémoire de segment de mémoire :

1. Accédez à la console du serveur.
2. Cliquez avec le bouton droit de la souris sur un composant de serveur dans le graphique de réseau et sélectionnez Dump Heap (Image mémoire de segment de mémoire).
3. Lorsque vous y êtes invité, enregistrez le fichier.
4. Ouvrez le fichier.

Le fichier contient le chemin d'accès complet du fichier .hprof ; par exemple :

C:\Users\myusername\lisatmp_6.0.7\Coordinator_Server_HeapDump_2012-02-28_08-36-55.hprof.

Remarque : Cette fonctionnalité est disponible uniquement dans des environnements d'exécution Sun Java 6. Cet outil de diagnostic peut aider le service de support à déterminer les causes de conditions OutOfMemory. Le segment de mémoire est automatiquement vidé si une condition OutOfMemory se produit ; ce bouton permet de déclencher manuellement une image mémoire de segment de mémoire.

Pour créer un fil de discussion :

1. Accédez à la console du serveur.
2. Cliquez avec le bouton droit de la souris sur un composant de serveur dans le graphique de réseau et sélectionnez Dump Threads (Fil de discussion).
3. Lorsque vous y êtes invité, enregistrez le fichier de fil de discussion.
4. Ouvrez le fichier de fil de discussion et affichez le contenu.

Nettoyage de la mémoire forcé

La console du serveur permet de forcer un composant de serveur à effectuer nettoyage de la mémoire.

En plus du nettoyage de la mémoire, cette procédure crée un fichier qui contient des statistiques de mémoire. Par exemple :

Before: Memory used 35mb, allocated 97mb, max 227mb (15%) ;
After: Memory used 19mb, allocated 95mb, max 227mb (8%)

Généralement, vous effectuez cette procédure uniquement lorsque vous y êtes invité par le service de support clientèle.

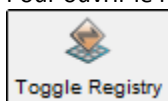
Pour forcer le nettoyage de la mémoire :

1. Accédez à la console du serveur.
2. Cliquez avec le bouton droit de la souris sur un composant de serveur dans le graphique de réseau et sélectionnez Force GC (Forcer le nettoyage de la mémoire).
3. Lorsque vous y êtes invité, enregistrez le fichier de statistiques.
4. Ouvrez le fichier de statistiques et affichez le contenu.

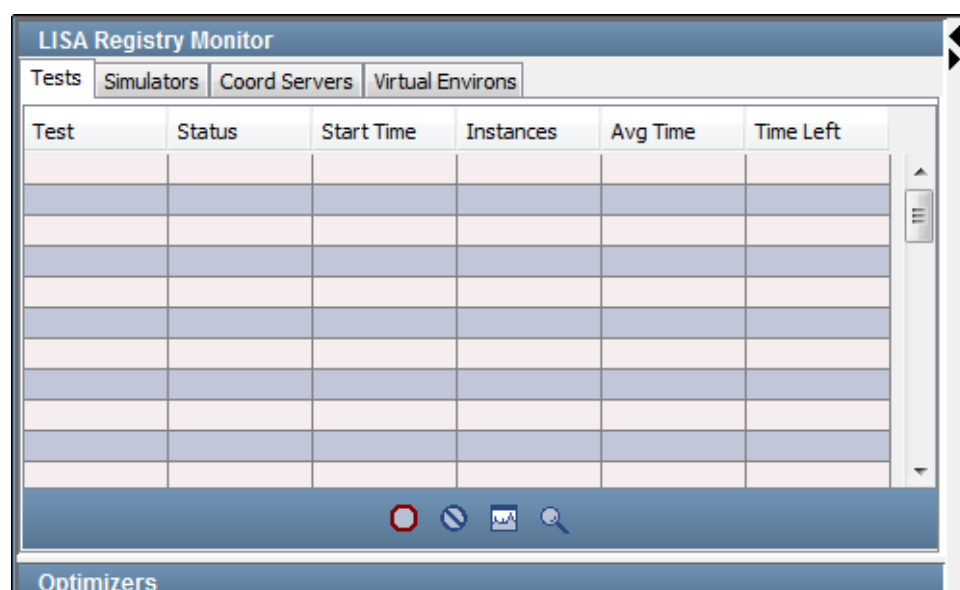
Utilisation du moniteur de registre

Le moniteur de registre permet de surveiller les scénarios de test, les simulateurs, les coordinateurs et les environnements virtuels pour une suite de tests.

Pour ouvrir le moniteur de registre, cliquez sur Toggle Registry (Basculer vers le registre)



dans la barre d'outils principale de la station de travail DevTest Workstation.



Le moniteur de registre comporte les onglets suivants :





- [Onglet Tests](#) (page 159)
- [Onglet Simulators \(Simulateurs\)](#) (page 159)
- [Onglet Coordinator Servers \(Serveurs de coordination\)](#) (page 160)
- [Onglet Virtual Environments \(Environnements virtuels\)](#) (page 160)

Moniteur de registre - Onglet Test

L'onglet Tests répertorie des informations sur tous les scénarios de test en cours d'exécution dans cette suite de tests.

Pour chaque scénario de test, vous pouvez afficher le nom de test, le statut, l'heure de début, les instances, la durée moyenne et le temps restant.

Vous pouvez effectuer les actions suivantes avec un test de votre choix :

- Pour arrêter un test, cliquez sur Stop (Arrêter) .
- Pour arrêter immédiatement un test, cliquez sur Kill (Arrêter immédiatement) .
- Pour optimiser un test, cliquez sur Optimize Test (Optimiser un test) 
Pour plus d'informations, consultez la section Utilisation de l'optimiseur de test de charge de la rubrique *Utilisation de CA Application Test*.
- Pour afficher un test, cliquez sur View Test (Afficher le test) 
Les informations de test sont affichées dans le moniteur de test.

Moniteur de registre - Onglet Simulators (Simulateurs)




L'onglet Simulators (Simulateurs) permet d'ajouter des utilisateurs virtuels en temps réel au serveur de simulation de votre choix.

Cet onglet répertorie le serveur de simulation et ses instances disponibles.

Moniteur de registre - Onglet Coordinator Servers (Serveurs de coordination)

L'onglet Coordinator Servers (Serveurs de coordination) répertories des informations sur les serveurs de coordination en cours d'exécution.

Vous pouvez effectuer les actions suivantes sur un serveur de coordination sélectionné :

- Pour arrêter ce service, cliquez sur Stop (Arrêter) .
- Pour réinitialiser ce service (arrêter et effacer les activités actuelles), cliquez sur Reset (Réinitialiser) .
- Pour afficher un message de statut, cliquez sur View Status Message (Afficher le message de statut) .

Moniteur de registre - Onglet Virtual Environments (Environnements virtuels)

L'onglet Virtual Environments (Environnements virtuels) répertorie des informations sur les environnements virtuels (le cas échéant) en cours d'exécution.

Utilisation du tableau de bord Enterprise Dashboard

Cette section comprend les rubriques suivantes :

[Ouverture du tableau de bord d'entreprise](#) (page 161)

[Réactivation d'un registre ou du tableau de bord Enterprise Dashboard](#) (page 167)

[Maintenance des registres](#) (page 168)

[Exportation des données du tableau de bord](#) (page 170)

[Exportation des données d'audit d'utilisation](#) (page 172)

[Purge des données de tableau de bord](#) (page 173)

Ouverture du tableau de bord d'entreprise

Pour ouvrir le tableau de bord Enterprise Dashboard à partir d'un navigateur Web :

1. Vérifiez que le registre est en cours d'exécution.
2. Accédez au répertoire dans lequel vous avez installé le tableau de bord Enterprise Dashboard.
3. Accédez au répertoire **bin** et exécutez le fichier **EnterpriseDashboard.exe** ou cliquez sur Enterprise Dashboard (Tableau de bord d'entreprise) dans le menu Démarrer, Programmes.
4. Entrez **http://localhost:1506/** dans un navigateur Web.

Si le tableau de bord d'entreprise est exécuté sur un ordinateur distant, remplacez **localhost** par le nom ou l'adresse IP de cet ordinateur.

Le tableau de bord Enterprise Dashboard s'ouvre.

Fenêtre principale du tableau de bord d'entreprise

La fenêtre principale dans le tableau de bord d'entreprise permet d'afficher les statistiques de performances suivantes relatives aux registres en cours d'exécution :

Nom d'affichage

Le nom d'affichage (également appelé nom de registre dans la fenêtre de configuration) est le nom que vous affectez lors de la configuration du registre.

nom

URL du registre.

Statut

Les valeurs peuvent être *Running* (En cours d'exécution) ou *Stopped* (Arrêté).

Version

Version de DevTest pour ce registre.

Coordinators (Coordinateurs), Simulators (Simulateurs), VSEs (Environnements de service virtuel), Workstations (Stations de travail), Agents et Labs (Laboratoires)

Nombre de ressources associées au registre.

Remarque : Pour afficher des agents, vous devez démarrer broker.exe.

DevTest Console URL (URL de la console de DevTest)

Adresse de la console de DevTest.

Pour afficher une fenêtre Registry Summary (Récapitulatif du registre) contenant plus d'informations, placez votre souris sur le champ Display Name (Nom d'affichage) d'un registre.

Nom d'affichage

Le nom d'affichage (également appelé nom de registre dans la fenêtre de configuration) est le nom que vous affectez lors de la configuration du registre.

URL (Propriété/URL)

URL du registre.

DevTest Solutions Version

Version de DevTest exécutée sur l'ordinateur sur lequel le registre est exécuté.

Version de Java

Version de Java en cours d'exécution sur l'ordinateur sur lequel le registre est exécuté.

Système d'exploitation

Version du système d'exploitation exécuté sur l'ordinateur sur lequel le registre est exécuté.

Security (Sécurité)

Enabled (activée) ou Disabled (désactivée), selon si la liste de contrôle d'accès est définie pour le registre.

Statut

Les valeurs peuvent être *Running* (En cours d'exécution) ou *Stopped* (Arrêté).

Uptime (Durée de disponibilité)

Nombre de jours, heures, minutes et secondes depuis le démarrage du registre

Last Start Time (Date/heure du dernier démarrage)

Indique la date et l'heure du dernier démarrage du registre.

Pour afficher des informations sur la base de données utilisée par le tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise), cliquez sur l'icône de base de



données dans le coin supérieur droit du panneau. La fenêtre contextuelle affiche l'URL, le type et la version de la base de données, le nom et la version du pilote, ainsi que l'utilisateur.

Remarque : Toutes les informations ne sont pas disponibles pour des versions antérieures à 7.1. La table suivante indique les informations des fonctionnalités affichées pour les versions antérieures.

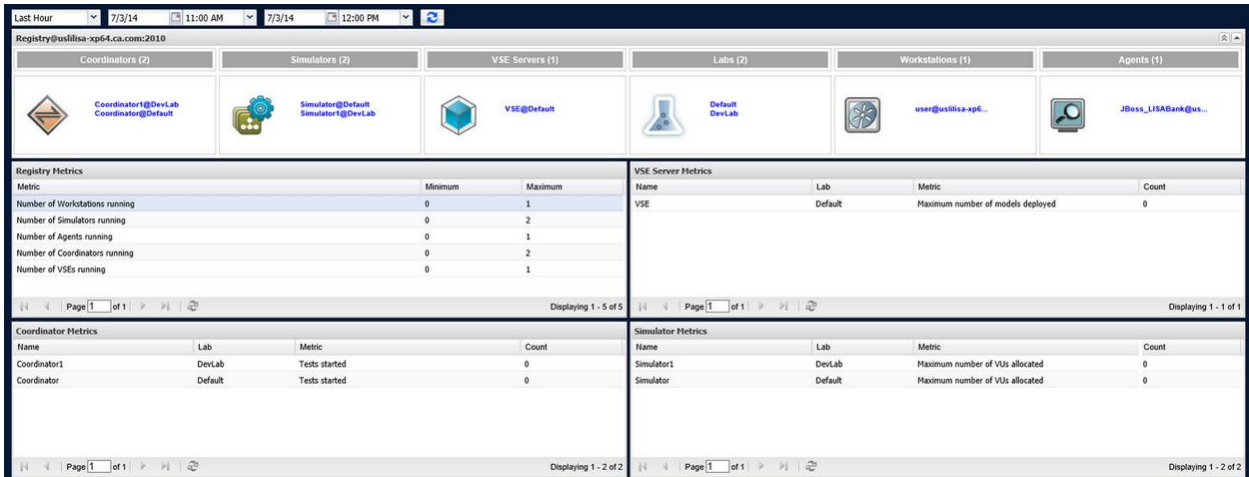
Fonction	Disponible pour les registres antérieurs à la version 7.1	Disponible pour les registres de la version 7.1	Nouveauté pour les registres de la version 7.5
Nom d'affichage du registre		x	
URL	x		
Statut	x		
Durée de disponibilité		x	
Sécurité	x		
DevTest version		x	
Version de Java		x	
Durée de disponibilité		x	
Système d'exploitation		x	
URL de la console DevTest		x	
Noms des coordinateurs	x		
Noms des simulateurs	x		
Noms de serveurs de VSE	x		
Noms de laboratoires	x		

Fonction	Disponible pour les registres antérieurs à la version 7.1	Disponible pour les registres de la version 7.1	Nouveauté pour les registres de la version 7.5
Mesures			x
Données historiques			x

Fenêtre Enterprise Dashboard Registry Details (Détails des registres du tableau de bord d'entreprise)


La fenêtre de détails de registre du tableau de bord d'entreprise permet d'afficher des détails sur les registres.

Remarque : Cette fenêtre affiche uniquement les données pour les registres exécutant la version 7.5 (ou version ultérieure).



La partie supérieure de la fenêtre répertorie tous les coordinateurs, les simulateurs, les serveurs de VSE, les laboratoires, les stations de travail et les agents actifs pour le registre.

Pour définir la période à utiliser pour l'affichage des mesures, utilisez les champs déroulants dans la partie supérieure gauche du panneau. Le premier champ déroulant fournit une liste des périodes standard. Pour plus de détails, spécifiez une date et heure de début, et une date et heure de fin dans les autres champs déroulants. Cliquez sur l'icône Refresh (Actualiser) pour actualiser l'affichage.

Si le tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise) était inactif pendant un certain temps, cliquez sur Refresh (Actualiser)  pour actualiser les données de chaque panneau.

La partie inférieure de la fenêtre indique des mesures pour des registres, des serveurs de VSE, des coordinateurs et des simulateurs.


La zone Registry Metrics (Mesures de registre) du panneau indique le plus grand nombre et le plus petit nombre de stations de travail, de simulateurs, de coordinateurs et de VSE en cours d'exécution dans la période définie.

La zone VSE Server Metrics (Mesures de serveur de VSE) du panneau indique le nombre de transactions et le nombre de laboratoires déployés pour chaque VSE actif dans la période définie.

La zone Coordinators Metrics (Mesures de coordinateur) du panneau indique le nombre de tests démarrés pour chaque coordinateur dans la période définie.

Si vous exécutez une suite de tests et le nombre de tests démarrés indiqués dans le tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise) est différent du nombre attendu, reportez-vous à la section de résultats de suite de DevTest Workstation. Vérifiez les résultats de chaque test ayant échoué. Si un échec de simulation se produit pour un test, le nombre de tests démarrés ne le comptabilise pas.

La zone Simulator Metrics (Mesures de simulateur) du panneau indique le nombre maximum d'utilisateurs virtuels actifs dans la période définie.

Pour retourner à la fenêtre principale, cliquez sur Go Back to registry view (Revenir à la vue de registre)  ou sur Overview (Présentation) dans les chemins de navigation du coin supérieur gauche de la page.

Réactivation d'un registre ou du tableau de bord Enterprise Dashboard

L'assistant de configuration de l'installation de DevTest 8.0 version ultérieure permet de configurer les nouveaux registres. Lorsque vous démarrez le tableau de bord Enterprise Dashboard et les registres, les registres sont automatiquement activés. Toutefois, en cas de modification ultérieure à l'un des éléments suivants, une réactivation sera nécessaire.

- Nom d'hôte du serveur sur lequel le registre est installé
- Nom du registre
- Port du registre
- URL du tableau de bord Enterprise Dashboard

Procédez comme suit:

1. En cas de modification du nom d'hôte ou du port du tableau de bord Enterprise Dashboard :
 - a. Connectez-vous à l'ordinateur sur lequel le tableau de bord Enterprise Dashboard est installé.
 - b. Accédez à LISA_HOME et ouvrez local.properties.
 - c. Si le nom d'hôte ou le port du tableau de bord Enterprise Dashboard a été modifié, mettez à jour la ligne suivante :

```
lisa.enterprisedashboard.service.url=tcp://somehost:2003/EnterpriseDashboard
```
 - d. Enregistrez le fichier.
 - e. Redémarrez le tableau de bord Enterprise Dashboard.
2. Vérifiez que le tableau de bord Enterprise Dashboard est en cours d'exécution.
3. Si le nom d'hôte du serveur sur lequel le registre est installé est modifié, redémarrez le registre pour le réactiver.
4. En cas de modification du nom ou du port d'un registre :
 - a. Connectez-vous à l'ordinateur sur lequel la modification apportée au registre a eu lieu.
 - b. Ouvrez une invite de commande ou une fenêtre de terminal et accédez à LISA_HOME.
 - c. Démarrez le registre dont le nom ou le port a été modifié. Par exemple :

```
./bin/Registry.exe -n "tcp://localhost:2093/MyRegistry"
```
5. Vérifiez la reconfiguration du registre.

Maintenance des registres

La maintenance des registres implique les procédures suivantes :

- Ajout du registre d'un DevTest Server, puis validation du registre
Remarque : Pour plus d'informations sur l'ajout d'un registre à partir d'une version antérieure à DevTest 7.5, consultez la section Configuration des registres existants. Pour les versions à partir de 8.0, le processus d'installation configure automatiquement les nouveaux registres.
- Mise à jour et validation d'un registre existant
- Suppression d'un registre d'un DevTest Server qui n'est plus inclus dans le service
- Validez régulièrement chaque registre répertorié dans le tableau de bord Enterprise Dashboard.

Pour ajouter un registre (DevTest 7.5.x) :

1. Accédez au répertoire LISA_HOME d'un DevTest Server nouvellement installé.
2. Copiez _local.properties et remplacez le nom de la copie par local.properties.
3. Ouvrez le fichier local.properties pour le modifier. Recherchez la Section 1 - Enterprise Dashboard.
4. Supprimez les commentaires de la ligne suivante et remplacez localhost ou le nom d'hôte valide par somehost.

`lisa.enterprisedashboard.service.url=tcp://localhost:2003/EnterpriseDashboard`
5. Enregistrez local.properties et fermez-le.

Pour supprimer un registre :

1. [Ouvrez le tableau de bord Enterprise Dashboard](#) (page 161).
2. Sélectionnez Configure (Configurer) dans le menu Options.
3. Cliquez sur le registre que vous voulez supprimer de la liste des registres dans la colonne Registry (Registre).
4. Cliquez sur Delete (Supprimer).

Remarque : Si vous supprimez un registre exécuté sur la version 7.5 (ou version ultérieure), vous devez également mettre à jour la propriété **`lisa.enterprise.dashboard.url`** dans le fichier **`local.properties`** pour ce registre.

Remarque : Supprimer un registre à partir de la page Registry Configuration (Configuration de registre) supprime le registre du tableau de bord. Toutefois, les données historiques pour ce registre ne sont pas automatiquement purgées de la base de données. Pour plus d'informations sur la purge des données historiques, consultez la rubrique [Purge des données de tableau de bord](#) (page 173).

Pour mettre à jour un registre :

1. [Ouvrez le tableau de bord Enterprise Dashboard](#) (page 161).
2. Sélectionnez Configure (Configurer) dans le menu Options.
3. Cliquez sur le registre que vous voulez mettre à jour dans la liste des registres de la colonne Registry (Registre).
4. Modifiez les champs Registry Name (Nom du registre) et Display Registry (Afficher le registre).
5. Cliquez sur Save (Enregistrer).

Pour valider un registre :

1. [Ouvrez le tableau de bord Enterprise Dashboard](#) (page 161).
2. Sélectionnez Configure (Configurer) dans le menu Options.
3. Cliquez sur le registre que vous voulez valider dans la liste des registres de la colonne Registry (Registre).
4. Cliquez sur Validate (Valider).

Le serveur de tableau de bord interroge le registre sélectionné et affiche le statut ; par exemple : Is running (En cours d'exécution).

5. Cliquez sur OK.

Exportation des données du tableau de bord

Le tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise) vous permet d'exporter des données de tableau de bord actuelles et historiques au format Excel. Vous pouvez exporter des données à partir de la [fenêtre principale](#) (page 162) ou à partir de la fenêtre Registry Details (Détails du registre).

Les mesures suivantes sont exportées :

- **Mesures de registre**
 - Nombre de stations de travail en cours d'exécution (minimum/maximum)
 - Nombre de simulateurs en cours d'exécution (minimum/maximum)
 - Nombre d'agents en cours d'exécution (minimum/maximum)
 - Nombre de coordinateurs en cours d'exécution (minimum/maximum)
 - Nombre d'environnements de service virtuel en cours d'exécution (minimum/maximum)
- **Mesures VSE Metrics (Mesures SNMP)**
 - Nombre maximum de modèles déployés
- **Mesures de coordinateur**
 - Nombre de tests démarrés
- **Mesures de simulateur**
 - Nombre maximum d'utilisateurs virtuels alloué

Procédez comme suit:

1. Cliquez sur Options dans le coin supérieur droit de la fenêtre et sélectionnez Export To Excel (Exporter dans un fichier Excel).

Si vous exportez à partir de la fenêtre Registry Details (Détails du registre), passez à l'étape 4.

Si vous exportez à partir de la fenêtre principale, la fenêtre Export Registry Data (Exporter les données de registre) s'ouvre.

2. Renseignez les champs suivants :

Export live data only (Exporter des données actives uniquement)

Cocher cette case limite l'exportation aux données actives.

Décocher la case permet d'exporter les données historiques.

Ping registries (Exécuter une commande ping sur les registres)

Lorsque cette case est cochée, une commande ping est exécutée pour chaque registre afin de déterminer son statut et de l'afficher dans le fichier exporté.

Lorsque cette case est désactivée, chaque registre du fichier exporté a un statut Unknown (Inconnu).

Remarque : Cette option s'applique uniquement aux données historiques. Pour une exportation de données actives, le statut de chaque registre est automatiquement déterminé.

3. Cliquez sur OK (Redéployer/déployer).

Vous êtes invité à enregistrer ou ouvrir le fichier Excel exporté.

4. Cliquez sur l'une des options suivantes :
 - Cliquez sur Save (Enregistrer) pour enregistrer le fichier exporté dans un répertoire spécifique.
 - Cliquez sur Open (Ouvrir) pour afficher le fichier exporté.

Exportation des données d'audit d'utilisation

Le rapport d'audit d'utilisation de DevTest Solutions fournit des détails sur la conformité à votre contrat de licence, en fonction de l'utilisation simultanée maximum des types d'utilisateur suivants :

- PF Power User (Utilisateur avancé PF)
- SV Power User (Utilisateur avancé SV)
- Test Power User (Utilisateur avancé de test)
- Runtime User (Utilisateur d'exécution)

Le rapport peut inclure l'administrateur, qui apparaît dans la grille Roles de la console de service comme combinaison des utilisateurs PF Power User (Utilisateur avancé PF) et SV Power User (Utilisateur avancé SV). Les licences ignorent cette combinaison de types d'utilisateur.

Vous pouvez générer le rapport d'audit d'utilisation à la demande. Par défaut, le rapport est généré tous les trois mois.

Procédez comme suit:

1. Accédez au tableau de bord Enterprise Dashboard.
`http://hostname:1506`
2. Cliquez sur la liste déroulante Options et sélectionnez Export Usage Audit Data (Exporter des données d'audit d'utilisation).
La boîte de dialogue Export Usage Audit Data (Exporter des données d'audit d'utilisation) s'ouvre.
3. Pour sélectionner une date de début et une date de fin pour la plage de dates du rapport, cliquez sur les icônes de calendrier, puis cliquez sur OK.
Le rapport généré pour la plage de dates spécifiée est téléchargé dans la partie inférieure gauche de la fenêtre.
4. Cliquez sur DevTestSolutionsUsageAuditReport.xlsx pour ouvrir le classeur Excel contenant votre rapport.
Pour plus d'informations sur chaque onglet, consultez la section [Rapport d'audit d'utilisation de DevTest Solutions](#) (page 64).

Purge des données de tableau de bord

Le tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise) vous permet de purger les journaux d'événements historiques et les mesures antérieures à la date et heure spécifiée. Vous pouvez également purger des registres de la base de données supprimée à partir de la page Registry Configuration (Configuration de registre). Pour plus d'informations, reportez-vous à la rubrique Configuration des registres.

Procédez comme suit:

1. Cliquez sur Options dans le coin supérieur droit de la fenêtre et sélectionnez Purge Data (Purger les données).

La boîte de dialogue Purge Data s'affiche.

2. Sélectionnez une date et heure pour les données à purger.

La fonctionnalité de purge supprime de façon permanente tous les journaux d'événements et les mesures de la base de données antérieurs à la date et heure spécifiée.

Les valeurs par défaut suppriment les journaux d'événements et les mesures antérieurs de 100 jours à la date et heure actuelle.

3. Cochez la case **Purge registries marked for deletion** (Purger les registres marqués pour suppression) permet de supprimer de façon permanente tous les registres supprimés de la base de données à partir de la page Registry Configuration (Configuration de registre).

Remarque : Supprimer un registre à partir de la page Registry Configuration (Configuration de registre) supprime le registre du tableau de bord. Toutefois, les données historiques pour ce registre ne sont pas automatiquement purgées de la base de données. Cochez cette case permet de supprimer de façon permanente les registres supprimés de la base de données et tous les journaux d'événements, les mesures et les composants associés au registre.

4. Cliquez sur OK (Redéployer/déployer).

Une boîte de dialogue de confirmation s'ouvre.

5. Cliquez sur Yes (Oui).

Les données sélectionnées sont purgées du tableau de bord Enterprise Dashboard (Tableau de bord d'entreprise).

Glossaire

Archive de modèle (MAR)

Une *archive de modèle (MAR)* est le principal artefact de déploiement dans DevTest. Les fichiers MAR contiennent un actif principal, tous les fichiers secondaires qui sont requis pour exécuter l'actif principal, un fichier d'informations et un fichier d'audit. Pour plus d'informations, consultez la section Utilisation des archives de modèle (MAR) de la rubrique *Utilisation de CA Application Test*.

assertion

Une *assertion* est un élément qui s'exécute après l'exécution d'une étape et de tous ses filtres. Les assertions vérifient que les résultats de l'étape sont conformes aux prévisions. Une assertion est généralement utilisée pour modifier le flux d'un scénario de test ou le modèle de service virtuel. Les assertions globales s'appliquent à chaque étape d'un scénario de test ou d'un modèle de service virtuel. Pour plus d'informations, consultez la section Assertions de la rubrique *Utilisation de CA Application Test*.

Audit document (Document d'audit)

Un *document d'audit* permet de définir des critères de réussite d'un test, ou d'un ensemble de tests dans une suite. Pour plus d'informations, consultez la section Génération de documents d'audit dans la rubrique *Utilisation de CA Application Test*.

companion (compagnon)

Un *Companion (Compagnon)* est un élément exécuté avant et après chaque exécution de scénario de test. Les compagnons sont comparables à des filtres applicables à l'ensemble du scénario de test, par opposition à des étapes de test spécifiques. Les compagnons sont utilisés pour configurer le comportement global dans le scénario de test. Pour plus d'informations, consultez la section Compagnons de la rubrique *Utilisation de CA Application Test*.

Configuration

Une *configuration* est une collection nommée de propriétés qui spécifient en général des valeurs propres à un environnement pour le système testé. La suppression de données d'environnement codées de manière irréversible permet d'exécuter un scénario de test ou un modèle de service virtuel au niveau d'environnements différents en modifiant simplement des configurations. La configuration par défaut dans un projet est appelée *project.config*. Un projet peut contenir de nombreuses configurations, mais une seule configuration peut être active à la fois. Pour plus d'informations, consultez la section Configurations de la rubrique *Utilisation de CA Application Test*.

Conversation tree (Arborescence des conversations)

Une *arborescence des conversations* est un ensemble de noeuds liés qui représentent des chemins de conversation pour les transactions avec état dans une image de service virtuel. Chaque noeud porte une étiquette de nom d'opération ; par exemple : `withdrawMoney`. Exemple de chemin de conversation pour un système d'opérations bancaires : `getNewToken`, `getAccount`, `withdrawMoney`, `deleteToken`. Pour plus d'informations, reportez-vous à la rubrique *Utilisation de CA Service Virtualization*.

coordinator (coordinateur)

Le *coordinateur* reçoit les informations d'exécution de test sous forme de document et coordonne les tests exécutés sur un ou plusieurs serveurs de simulation. Pour plus d'informations, consultez la section *Coordinator Server (Serveur de coordination)* de la rubrique *Utilisation de CA Application Test*.

data protocol (protocole de données)

Un *protocole de données* est également appelé gestionnaire de données. Dans *CA Service Virtualization*, un protocole de données est responsable de la gestion de l'analyse des demandes. Certains protocoles de transport autorisent (ou requièrent) un protocole de données auquel le job de création de demandes est délégué. C'est pourquoi le protocole doit connaître la charge utile de la demande. Pour plus d'informations, consultez la section *Utilisation de protocoles de données* dans la rubrique *Utilisation de CA Service Virtualization*.

Data set (Ensemble de données)

Un *Data set (Ensemble de données)* est une collection de valeurs que vous pouvez utiliser pour définir des propriétés dans un scénario de test ou un modèle de service virtuel lors de l'exécution. Les ensembles de données fournissent un mécanisme permettant d'introduire des données de test externes dans un scénario de test ou un modèle de service virtuel. Vous pouvez créer des ensembles de données internes à DevTest, ou de manière externe ; par exemple, dans un fichier ou une table de base de données. Pour plus d'informations, consultez la section *Ensembles de données* de la rubrique *Utilisation de CA Application Test*.

desensitize (désensibiliser)

La *désensibilisation* consiste à convertir des données sensibles par des valeurs de substitution définies par l'utilisateur. Par exemple, les numéros de carte de crédit et les numéros de sécurité sociale sont des données sensibles. Pour plus d'informations, consultez la section *Désensibilisation de données* de la rubrique *Utilisation de CA Service Virtualization*.

Event (Événement)

Un *Event (Événement)* est un message sur une action qui s'est produite. Vous pouvez configurer des événements au niveau d'un scénario de test ou d'un modèle de service virtuel. Pour plus d'informations, consultez la section *Introduction aux événements* de la rubrique *Utilisation de CA Application Test*.

Filter (Filtre)

Un *filtre* est un élément exécuté avant et après une étape. Les filtres permettent de traiter les données des résultats ou de stocker des valeurs dans des propriétés. Les filtres globaux s'appliquent à chaque étape d'un scénario de test ou d'un modèle de service virtuel. Pour plus d'informations, consultez la section Filtres de la rubrique *Utilisation de CA Application Test*.

Groupe

Un *groupe* ou un *groupe de services virtuels* est une collection de services virtuels portant la même balise de groupe. Cela permet de les surveiller ensemble dans la console VSE.

Interactive Test Run (ITR) (Exécuter un test interactif)

L'utilitaire *Interactive Test Run (ITR)* (Exécuter un test interactif) permet d'exécuter un scénario de test ou un modèle de service virtuel étape par étape. Vous pouvez changer le scénario de test ou le modèle de service virtuel lors de l'exécution et le réexécuter pour vérifier les résultats. Pour plus d'informations, consultez la section Utilisation de l'utilitaire Interactive Test Run (ITR) (Exécuter un test interactif) de la rubrique *Utilisation de CA Application Test*.

Lab (Laboratoire)

Un *laboratoire* est un conteneur logique pour un ou plusieurs membres de laboratoire. Pour plus d'informations, consultez la section Laboratoires et membres de Laboratoire dans la rubrique *Utilisation de CA Application Test*.

magic date (date magique)

Pendant un enregistrement, un analyseur de dates analyse les demandes et les réponses. Une valeur correspondant à une définition étendue de formats de la date est convertie en *date magique*. Les dates magiques permettent de vérifier que le modèle de service virtuel fournit des valeurs de date explicites dans des réponses. Exemple e date magique : `{{=doDateDeltaFromCurrent("yyyy-MM-dd","10");/*2012-08-14*/}}`. Pour plus d'informations, consultez la section Chaînes et dates magiques de la rubrique *Utilisation de CA Service Virtualization*.

Magic string (Chaîne magique)

Une *chaîne magique* est une chaîne générée pendant la création d'une image de service. Une chaîne magique est utilisée pour vérifier que les réponses fournies par le modèle de service virtuel contiennent des valeurs de chaîne explicites. Exemple de chaîne magique : `{{=request_fname;/chris/}}`. Pour plus d'informations, consultez la section Chaînes et dates magiques de la rubrique *Utilisation de CA Service Virtualization*.

Match tolerance (Tolérance de correspondance)

La *tolérance de correspondance* est un paramètre qui permet de contrôler la méthode utilisée par CA Service Virtualization pour comparer une demande entrante avec les demandes dans une image de service. Les options disponibles sont EXACT, SIGNATURE et OPERATION. Pour plus d'informations, consultez la section Tolérance de correspondance de la rubrique *Utilisation de CA Service Virtualization*.

Metrics (Mesures)

*Les mesures permettent d'appliquer des méthodes et des mesures quantitatives aux performances et aux aspects fonctionnels de vos tests, ainsi qu'au système testé. Pour plus d'informations, consultez la section Génération de mesures de la rubrique *Utilisation de CA Application Test*.*

Model Archive (MAR) Info (Fichier d'informations d'archive de modèle (MAR))

*Un Model Archive (MAR) Info (Fichier d'informations d'archive de modèle (MAR)) est un fichier qui contient des informations requises pour la création d'une archive de modèle MAR. Pour plus d'informations, consultez la section Utilisation des archives de modèle (MAR) de la rubrique *Utilisation de CA Application Test*.*

navigation tolerance (tolérance de navigation)

*La tolérance de navigation est un paramètre qui permet de contrôler le méthode utilisée par CA Service Virtualization pour rechercher la transaction suivante dans une arborescence des conversations. Les options disponibles sont CLOSE, WIDE et LOOSE. Pour plus d'informations, consultez la section Tolérance de navigation de la rubrique *Utilisation de CA Service Virtualization*.*

Network graph (Graphique du réseau)

*Le graphique de réseau est une zone de la console de serveur qui contient une représentation graphique du composant DevTest Cloud Manager et des laboratoires associés. Pour plus d'informations, consultez la section Démarrage d'un laboratoire de la rubrique *Utilisation de CA Application Test*.*

Node (Noeud)

*Une étape de test interne à DevTest peut également être appelée *node* (noeud), ce qui explique l'intégration du terme node dans l'ID de certains événements.*

Path (Chemin)

*Un *chemin* contient des informations sur une transaction capturée par l'agent Java. Pour plus d'informations, reportez-vous à la rubrique *Utilisation de CA Continuous Application Insight*.*

Path graph (Graphique de chemin)

*Un *graphique de chemin* contient une représentation graphique d'un chemin et ses trames. Pour plus d'informations, consultez la section Graphique de chemin de la rubrique *Utilisation de CA Continuous Application Insight*.*

Project (Projet)

*Un *projet* est une collection de fichiers DevTest liés. Les fichiers peuvent inclure des scénarios de test, des suites, des modèles de service virtuel, des images de service, des configurations, des documents d'audit, des documents de simulation, des ensembles de données, des moniteurs et des fichiers d'informations MAR. Pour plus d'informations, consultez la section Panneau Project (Projet) de la rubrique *Utilisation de CA Application Test*.*

Property (Propriété)

Une *propriété* est une paire clé-valeur que vous pouvez utiliser comme variable d'exécution. Les propriétés peuvent stocker plusieurs types de données différents. Exemple de propriétés communes : LISA_HOME, LISA_PROJ_ROOT et LISA_PROJ_NAME. Une configuration est une collection nommée de propriétés. Pour plus d'informations, consultez la section Propriétés de la rubrique *Utilisation de CA Application Test*.

quick test (test rapide)

La fonctionnalité *Quick test (Test rapide)* permet d'exécuter un scénario de test avec une installation minimale. Pour plus d'informations, consultez la section Simulation d'un test rapide du *Utilisation de CA Application Test*.

Registry (Registre)

Le *registre* fournit un emplacement central pour l'enregistrement de tous les composants de DevTest Server et de DevTest Workstation. Pour plus d'informations, consultez la section Registre de la rubrique *Utilisation de CA Application Test*.

ressource

Un *actif* est un ensemble de propriétés de configuration groupées dans une unité logique. Pour plus d'informations, consultez la section Actifs de la rubrique *Utilisation de CA Application Test*.

service image (image de service)

Une *image de service* est une version normalisée de transactions enregistrées dans CA Service Virtualization. Chaque transaction peut être avec état (conversationnel) ou sans état. Une image de service peut être créée à l'aide de l'enregistreur d'image de service virtuel. Les images de service sont stockées dans un projet. Une image de service est également appelée *virtual service image (image de service virtuel, VSI)*. Pour plus d'informations, consultez la section Images de service de la rubrique *Utilisation de CA Service Virtualization*.

Simulator (Simulateur)

Un *simulateur* exécute les tests sous la surveillance du serveur de coordination. Pour plus d'informations, consultez la section Simulator Server (Serveur de simulation) de la rubrique *Utilisation de CA Application Test*.

Staging document (Document de simulation)

Un *document de simulation* contient les informations sur l'exécution d'un scénario de test. Pour plus d'informations, consultez la section Génération de documents de simulation dans la rubrique *Utilisation de CA Application Test*.

Subprocess (Sous-processus)

Un *sous-processus* est un scénario de test appelé par un autre scénario de test. Pour plus d'informations, consultez la section Génération de sous-processus de la rubrique *Utilisation de CA Application Test*.

Tableau de bord Continuous Service Validation (CVS) (Service de validation en continu)

Le *Continuous Service Validation (CVS) Dashboard (Tableau de bord du service de validation en continu)* permet de planifier l'exécution régulière de scénarios de test et des suites de test, sur une période étendue. Pour plus d'informations, consultez la section Service de validation en continu dans la rubrique *Utilisation de CA Application Test*.

test case (scénario de test)

Un *scénario de test* est une spécification de la procédure de test d'un composant métier dans le système testé. Chaque scénario de test contient une ou plusieurs étapes de test. Pour plus d'informations, consultez la section Génération de scénarios de test dans la rubrique *Utilisation de CA Application Test*.

test step (étape de test)

Une *étape de test* est un élément du flux de travaux de scénario de test qui représente une action de test unique à réaliser. Exemples d'étapes : Services Web, JavaBeans, JDBC et messagerie JMS. Une étape de test peut contenir des éléments de DevTest, tels que des filtres, des assertions et des ensembles de données liés. Pour plus d'informations, consultez la section Génération d'étapes de test de la rubrique *Utilisation de CA Application Test*.

Test suite (Suite de tests)

Une *suite de tests* est un groupe de scénarios de test, d'autres suites de tests, ou les deux, planifiés pour être exécutés l'un après l'autre. Un document de suite de tests spécifie le contenu de la suite, les rapports à générer et les mesures à collecter. Pour plus d'informations, consultez la section Génération de suites de tests de la rubrique *Utilisation de CA Application Test*.

Think time (Délai de réflexion)

Le *temps de réflexion* est la durée d'attente d'un scénario de test patiente avant d'exécuter une étape de test. Pour plus d'informations, consultez les sections Exemple d'ajout d'étape de test et Editeur de documents de simulation - Onglet Base de la rubrique *Utilisation de CA Application Test*.

transaction frame (Trame de transaction)

Une *trame de transaction* contient des données sur un appel de méthode intercepté par l'agent Java de DevTest ou un agent Light de CAI. Pour plus d'informations, consultez la section Transactions organisationnelles et trames de transaction de la rubrique *Utilisation de CA Continuous Application Insight*.

Virtual Service Environment (Environnement de service virtuel, VSE)

Le *Virtual Service Environment (Environnement de service virtuel, VSE)* est une application de DevTest Server qui permet de déployer et d'exécuter des modèles de service virtuel. VSE est également appelé CA Service Virtualization. Pour plus d'informations, reportez-vous à la rubrique *Utilisation de CA Service Virtualization*.

virtual service model (VSM, modèle de service virtuel)

Un *modèle de service virtuel* reçoit des demandes de service auxquelles il répond en l'absence du fournisseur de services réel. Pour plus d'informations, consultez la section *Modèle de service virtuel* de la rubrique *Utilisation de CA Service Virtualization*.