HP Business Service Management

Für Windows und Linux-Betriebssysteme

Softwareversion: 9.20 IP 1

BSM-Plattformverwaltungshandbuch



Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212. Kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die U.S.-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

© Copyright 2005-2012 Hewlett-Packard Development Company, L.P.

Markenhinweise

Adobe® und Acrobat® sind Marken der Adobe Systems Incorporated.

AMD und das AMD Arrow-Logo sind eingetragene Marken von Advanced Micro Devices, Inc.

Google™ und Google Maps™ sind eingetragene Marken von Google Inc.

Intel®, Itanium®, Pentium® und Intel® Xeon® sind eingetragene Marken der Intel Corporation in den Vereinigten Staaten und anderen Ländern.

Java ist eine eingetragene Marke von Oracle und/oder der zugehörigen Tochtergesellschaften.

Microsoft®, Windows®, Windows NT®, Windows® XP und Windows Vista® sind in den Vereinigten Staaten eingetragene Marken der Microsoft Corporation.

Oracle ist eine eingetragene Marke der Oracle Corporation und/oder der zugehörigen Tochtergesellschaften.

UNIX® ist eine eingetragene Marke von The Open Group.

Hinweise

Dieses Produkt beinhaltet Software, die von Apache Software Foundation entwickelt wurde (www.apache.org).

Dieses Produkt beinhaltet Software, die vom JDOM-Projekt entwickelt wurde (www.jdom.org).



Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden identifizierenden Informationen:

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten:

http://h20230.www2.hp.com/selfsolve/manuals

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Hier können Sie sich für eine HP Passport-ID registrieren:

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

Alternativ können Sie auf den Link **New user registration** (Neue Benutzer registrieren) auf der HP Passport-Anmeldeseite klicken.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HP-Kundenbetreuer.

Letzte Dokumentaktualisierung: Dienstag, 20. November 2012

Support

Besuchen Sie die HP Software Support Online-Website von HP unter:

http://www.hp.com/go/hpsoftwaresupport

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Support-Leistungen von HP Software.

Der Online-Support von HP Software bietet Kunden mit Hilfe interaktiver technischer Support-Werkzeuge die Möglichkeit, ihre Probleme intern zu lösen. Als Valued Support Customer können Sie die Support-Website für folgende Aufgaben nutzen:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Support-Verträgen
- Nachschlagen von HP-Support-Kontakten
- Einsehen von Informationen über verfügbare Services
- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Für die meisten Support-Bereiche müssen Sie sich als Benutzer mit einem HP Passport registrieren und anmelden. In vielen Fällen ist zudem ein Support-Vertrag erforderlich. Hier können Sie sich für eine HP Passport-ID registrieren:

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

Weitere Informationen zu Zugriffsebenen finden Sie unter:

http://h20230.www2.hp.com/new_access_levels.jsp

Inhalt

BSM-Plattformverwaltungshandbuch	1
Inhalt	6
Übersicht über die Plattformverwaltung	15
BSM-Zugriff und -Navigation	16
BSM-Verwaltung	17
Starten und Beenden von BSM	18
Anzeigen des Status von Prozessen und Diensten	19
Startmenü unter Windows	20
Anmelden bei BSM	21
Anmelden bei BSM mit LW-SSO	22
Erweiterte Anmeldeoptionen	23
Verknüpfen mit einer bestimmten Seite	24
Verwenden der JMX-Konsole	25
BSM-Anmeldeablauf	26
Anmelden und Abmelden	27
Verwenden der erweiterten Anmeldeoptionen	28
Ändern des JMX-Kennworts	31
Erstellen eines Keystore-Zertifikats	32
Verfolgen von Anmeldeversuchen und angemeldeten Benutzern	33
Sicherheitshinweise und -maßnahmen	34
Anmelden bei der BSM-Benutzeroberfläche	35
BSM-Anmeldeseite	35
Fenster "Mit dieser Seite verknüpfen"	35
Fehlerbehebung und Einschränkungen	38
Navigieren in und Verwenden von BSM	43
Verbesserungen der Benutzeroberfläche	46
Anpassen von Mastertitel und Logo	48

Client-Anforderungen für die Anzeige von BSM	49
Menüs und Optionen	51
Setup und Verwaltung	56
Downloads	57
Aufgaben	58
Komponenten der Benutzeroberfläche	59
Lizenzverwaltung	62
Aufgaben	63
Beschreibung der Benutzeroberfläche	64
Tipps/Fehlerbehebung	66
Serverbereitstellung	67
Weitere Informationen	68
Aufgaben	70
Beschreibung der Benutzeroberfläche	72
Fehlerbehebung und Einschränkungen	75
Datenbankverwaltung	76
Partitionieren und Löschen von historischen Daten aus Datenbanken	78
Entfernen unerwünschter Daten aus der Profildatenbank	81
Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server	82
So konfigurieren Sie ein Benutzerschema auf einem Oracle-Server	83
Verwenden des Purging Manager	85
Aktivieren der Option "Nur Neuaggregierung ausführen"	87
Festlegen der Ereignisse pro Minute für das Eintreffen von Daten in BSM	88
Anpassen der Konfigurationen von Dienstprogrammen für Datenmarkierungen	89
Benutzeroberfläche der Datenbankverwaltung	90
Seite "Datenbankverwaltung"	90
Seite "Dienstprogramm für Datenmarkierung"	90
Seite "Profildatenbank-Eigenschaften - MS SQL Server"	93
Seite "Profilbenutzerschema-Eigenschaften – Oracle Server"	95
Seite "Purging Manager"	98
Fehlerbehebung und Einschränkungen	101
Infrastruktureinstellungen	103

Ändern der Infrastruktureinstellungen im Infrastructure Settings Manager	104
Ändern des Ping-Zeitintervalls	105
Ändern des Speicherorts und Ablaufs von temporären Bilddateien	106
Ändern des Verzeichnisses, in dem temporäre Bilddateien gespeichert werden	107
Zugreifen auf temporäre Verzeichnisse mit mehreren Gateway-Servercompute	rn108
Ändern der Beibehaltungsdauer temporärer Bilddateien durch BSM	111
Angeben der Verzeichnisse, aus denen temporäre Bilddateien entfernt werden	114
Beschreibung der Benutzeroberfläche - Seite "Infrastructure Settings Manager"	' 115
Audit-Protokoll	117
Weitere Informationen	118
Aufgaben	120
Beschreibung der Benutzeroberfläche	121
Zeitsynchronisierung bei BSM-Servern	123
Anzeigen der BSM-Serverzeit	124
Arbeiten in nicht englischen Gebietsschemata	125
Installations- und Bereitstellungsaspekte	126
Probleme der Datenbankumgebung	128
Verwaltungsprobleme	129
Probleme in Service Health	130
Probleme mit Service Level Management	131
Reportprobleme	132
Business Process Monitor-Probleme	133
Probleme mit SiteScope	134
Probleme mit Real User Monitor	135
Probleme bei der Endbenutzerverwaltung	136
Probleme mit der Datenflussverwaltung	137
Probleme bei mehreren Sprachen	138
Unterstützung für die mehrsprachige Benutzeroberfläche	139
Hinweise und Einschränkungen	140
BSM-Protokolle	142
Speicherorte der Protokolldateien	143
Protokolle – Schweregrade	144

Protokolldateigröße und automatische Archivierung	145
JBoss- und Tomcat-Protokolle	146
Ändern der Protokollebenen	147
Aktivieren der Debugablaufprotokollierung für ein Ereignis	148
Protokollierungsadministrator	149
Portverwendung	150
Manuelles Ändern von Ports	151
Eingehender BSM-Datenverkehr	154
Ausgehender BSM-Datenverkehr	156
Lokaler BSM-Datenverkehr	157
Empfehlungen zur Dateisicherung	161
Daten-Enrichment	163
Standortverwaltung	164
Weitere Informationen	165
Aufgaben	166
Beschreibung der Benutzeroberfläche	171
Content Packs	182
Definieren von Content Packs	187
Abhängigkeiten in Content Packs	188
Exportieren von Content Packs	191
Importieren von Content Packs	192
Erstellen und Verwalten von Content Packs	193
Prüfliste für das Veröffentlichen von Content Packs	197
Content Packs Manager-Benutzeroberfläche	202
Seite "Content Packs"	202
Assistent zum Erstellen einer neuen Content Pack-Definition	205
Seite "Allgemein"	206
Seite "Inhalt"	207
Seite "Abhängigkeiten"	211
Seite "Zusammenfassung"	212
Dialogfeld "Content Pack importieren"	213
Befehlszeilenschnittstelle für den Content Pack Manager	214

Syntax	214
Befehlszeilenschnittstelle für das automatische Hochladen von Content Packs	217
Verwendung	217
Fehlerbehebung und Einschränkungen	220
Ausfallzeitenverwaltung	221
Erstellen und Verwalten von Ausfallzeiten für CIs	223
REST-Service für Ausfallzeit	225
Beispiel eines Zeitplans für Ausfallzeit mit einem Vorkommen	228
Beispiel eines wöchentlichen Zeitplans für Ausfallzeit	228
Beispiel eines monatlichen Zeitplans für Ausfallzeit	228
Ausfallzeitverwaltung - Benutzeroberfläche	229
Seite "Ausfallzeitenverwaltung"	229
Assistent für neue Ausfallzeit	231
Seite "Eigenschaften"	232
Seite "CIs auswählen"	233
Seite "Planung"	234
Seite "Aktion"	235
Seite "Benachrichtigung"	238
Seite "Vorschau"	238
Fehlerbehebung und Einschränkungen	240
Frühling (Winterzeit zu Sommerzeit)	240
Herbst (Sommerzeit zu Winterzeit)	241
Auswirkungen von Zeitumstellungen auf geplante Ausfallzeiten – Übersicht über die Beispiele	
Benutzer, Berechtigungen und Empfänger	.245
Benutzerverwaltung	246
Berechtigungen	248
Grundlegende Informationen zu Berechtigungen für Ressourcen	249
Rollen	251
Operationen	252
Sicherheits-Officer	252
Gruppen- und Benutzerhierarchie	254

Anpassen der Benutzermenüs	256
Konfigurieren von Benutzern und Berechtigungen – Workflow	257
Konfigurieren von Benutzern und Berechtigungen – Fallspezifisches Szenario	259
Zuweisen von Berechtigungen	266
Konfigurieren der Gruppen- und Benutzerhierarchie	267
Entfernen des Status "Sicherheits-Officer" über die JMX-Konsole	270
Exportieren und Importieren von Benutzerinformationen mit der JMX-Konsole	271
Anpassen von Benutzermenüs	273
Anpassen von Benutzermenüs – Fallspezifisches Szenario	275
Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS	278
Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung	280
Superuser	280
Administrator	280
Systemmodifikation	288
Systemanzeige	293
Kunde - Superuser	296
Kunde - Administrator	302
BPM Viewer	307
BPM-Administrator	308
RUM-Administrator	308
RUM Viewer	309
Rollen in der Benutzerverwaltung für verschiedene Kontexte	310
Operationen für die Benutzerverwaltung	314
Benutzerverwaltung – Benutzeroberfläche	339
Dialogfeld "Gruppe erstellen"	339
Dialogfeld "Benutzer erstellen"	339
Registerkarte "Anpassung" (Benutzerverwaltung)	340
Registerkarte "Allgemein" (Benutzerverwaltung)	341
Registerkarte "Empfänger" (Benutzerverwaltung)	344
Registerkarte "Hierarchie" (Benutzerverwaltung)	344
Registerkarte "Berechtigungen" (Benutzerverwaltung)	346
Ausschnitt "Ressourcenstruktur"	347

Registerkarte "Rollen"	349
Registerkarte "Operationen"	350
Hauptseite der Benutzerverwaltung	351
Ausschnitt "Gruppen/Benutzer"	352
Dialogfeld "Gruppenzuordnungen"	355
Empfängerverwaltung	358
Konfigurieren und Verwalten von Empfängern	359
Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS	360
Empfängerverwaltung - Benutzeroberfläche	362
Dialogfeld "Benutzer an Empfänger anhängen"	362
Seite "Empfänger"	362
Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"	364
Registerkarte "E-Mail"	371
Registerkarte "SMS"	372
Registerkarte "Pager"	374
Persönliche Einstellungen	377
Anpassen der BSM-Menüs und -Seiten – Workflow	378
Anpassen der BSM-Menüs und -Seiten – Fallspezifisches Szenario	379
Persönliche Einstellungen – Benutzeroberfläche	382
Seite "Benutzerkonto"	382
Seite "Menüanpassung"	383
Registerkarte "Empfänger"	384
Authentifizierungsstrategien	385
Einrichten einer Strategie für die SSO-Authentizierung	386
Einrichten der LDAP-Authentifizierung	387
Authentifizierungsmodi in BSM	388
Authentifizierungsstrategie – Benutzeroberfläche	389
Seite "Authentifizierungsstrategie"	389
Assistent für die Authentifizierung	390
Seite "Single Sign-On"	391
Dialogfeld "SAML2-Konfiguration"	394
Seite "LDAP - Allgemeine Konfiguration"	396

Dialogfeld "LDAP-Anbieterattribute"	400
Seite "LDAP-Benutzersynchronisierungskonfiguration"	401
Seite "Übersicht"	402
LW-SSO-Strategie	404
LW-SSO-Konfiguration für Installationen mit mehreren und mit verschachtelten Domänen	405
Konfigurieren des Modus für die Verarbeitung unbekannter Benutzer	406
Ändern der LW-SSO-Parameter mithilfe der JMX-Konsole	407
Sicherstellen des Benutzerzugriffs auf BSM mithilfe von clientseitigen Zertifikaten	408
Sicherstellen des Benutzerzugriffs auf BSM mithilfe eines externen Authentifizierungspunkts	410
Fehlerbehebung und Einschränkungen	411
Identity Management Single Sign-On-Authentifizierung	412
Sichern von BSM-Ressourcen unter IDM-SSO	413
Fehlerbehebung und Einschränkungen	416
LDAP-Authentifizierung und Zuordnung	417
Zuordnen von Gruppen	418
Synchronisieren von Benutzern	419
Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version v BSM	
Präzises Steuern der Zuweisung von standardmäßigen Benutzerberechtigungen	422
Zuordnen der Gruppen und Synchronisieren von Benutzern	423
Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version von BSM	425
Ändern des zur Anmeldung bei BSM verwendeten Attributs	426
Sichern der Kommunikation zwischen LDAP-Server und BSM-Server über SSL	427
Löschen von veralteten Benutzern	428
Fehlerbehebung und Einschränkungen	429
LW-SSO-Authentifizierung – Allgemeine Referenz	430
LW-SSO-Systemanforderungen	431
LW-SSO-Sicherheitswarnungen	432
Fehlerbehebung und Einschränkungen	434
enorts und Warnungsverwaltung	437

Report Schedule Manager	438
Manager "Report-Planung" – Hauptseite	439
Einrichten eines Bereitstellungssystems für Warnungen	441
Warnungen und Ausfallzeiten	443
Planen von effektiven Warnungsschemata	444
Einrichten eines Bereitstellungssystems für Warnungen	445
Anpassen von Warnungen	449
Warnungsprotokolle	457
Report zu Warnungsdetails	459
Fehlerbehebung und Einschränkungen	461
Benachrichtigungsvorlagen für EUM-Warnungen	462
Benachrichtigungsvorlagen für die Aufhebung des Warnungszustands	463
Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen	464
Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands	
Benachrichtigungsvorlagen für EUM-Warnungen – Benutzeroberfläche	466
Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"	466
Seite "Benachrichtigungsvorlagen"	470
Fehlerbehebung	473
Fehlerbehebung und Einschränkungen	474

Übersicht über die Plattformverwaltung

In diesem Handbuch finden Sie Anweisungen zum Öffnen, Konfigurieren und Verwalten von HP Business Service Management (BSM).

Das Handbuch ist in folgende Teile gegliedert:

- **Zugriff auf und Navigation in BSM**. Beschreibt, wie BSM gestartet wird, wie die Anmeldung an der Applikation erfolgt und bietet eine Übersicht über die Benutzeroberfläche.
- **Setup und Verwaltung.** Beschreibt die grundlegenden Einrichtungsoptionen wie Infrastruktureinstellungen, Zeitzonen, Sprachen, Protokolle und Sicherungen.
- Daten-Enrichment. Dieser Teil umfasst die folgenden Themen:
 - Standortverwaltung Beschreibt, wie mit mehreren geografischen Standorten gearbeitet wird.
 - Content Packs Beschreibt, wie Objekte oder CIs, die in von BSM überwachten Content Packs enthalten sind, definiert werden.
 - Ausfallzeitenverwaltung Beschreibt, wie ein Systemausfall behandelt wird.
- Benutzer, Berechtigungen und Empfänger. Beschreibt, wie der Benutzerzugriff auf BSM kontrolliert wird.
- **Reports und Warnungsverwaltung.** Beschreibt, wie Reports geplant und Warnungen eingerichtet werden.
- Fehlerbehebung. Erläutert allgemeine Systemprobleme oder -beschränkungen.

Teil 1

BSM-Zugriff und -Navigation

Kapitel 1

BSM-Verwaltung

In diesem Abschnitt wird beschrieben, wie Sie BSM starten und den Status von Prozessen und Diensten sowie die Optionen im Windows-Startmenü anzeigen können.

Starten und Beenden von BSM

So starten und beenden Sie BSM unter Windows:

Wählen Sie Start > Programme > HP Business Service Management > Verwaltung > Business Service Management aktivieren | deaktivieren aus. Aktivieren Sie in einer verteilten Umgebung zuerst den Datenverarbeitungsserver und dann den Gateway-Server.

So starten und beenden Sie BSM unter Linux:

/opt/HP/BSM/scripts/run_hpbsm start | stop

So starten oder beenden Sie BSM mit einem Daemon-Skript bzw. führen einen Neustart durch:

/etc/init.d/hpbsmd {start| stop | restart}

Hinweis: Wenn Sie BSM anhalten, wird der BSM-Dienst nicht aus dem Microsoft-Fenster für Dienste entfernt. Der BSM-Dienst wird erst aus diesem Fenster entfernt, wenn Sie BSM deinstallieren.

Anzeigen des Status von Prozessen und Diensten

Sie können den Status der Prozesse und Dienste, die vom BSM-Dienst und vom Hochverfügbarkeitscontroller ausgeführt werden, auf der HTML-Seite mit dem BSM-Serverstatus anzeigen.

Führen Sie das jeweils entsprechende Verfahren aus, um den Status der Prozesse und Dienste anzuzeigen:

- Windows: Wählen Sie Start > Programme > HP Business Service Management > Verwaltung > HP Business Service Management-Status aus.
- Linux: Führen Sie "opt/HP/BSM/tools/bsmstatus/bsmstatus.sh" aus.
- Von einem Remotecomputer: Geben Sie die URL http://<servername>:8080/myStatus/myStatus.html in einen Webbrowser ein.

Einschränkungen:

- Diese Seite ist erst remote verfügbar, nachdem der JBoss-Applikationsserver hochgefahren wurde.
- Wenn Sie JMX-RMI mit Basisauthentifizierung über SSL mithilfe des SYSTEM-Benutzers konfiguriert haben, werden auf dieser Seite keine Daten angezeigt. Weitere Informationen finden Sie unter "Securing JMX-RMI Channel Used for Internal BSM Communications" im BSM Hardening Guide.

Startmenü unter Windows

Bei der Installation von BSM in einer Windows-Umgebung wird dem Startmenü des Computers, auf dem BSM installiert wird, ein Menü für BSM hinzugefügt.

Um auf das BSM-Menü zuzugreifen, wählen Sie Start > Programme > HP Business Service Management aus.

Das Menü weist die folgenden Optionen auf:

Administration

Die Menüoption **Administration** umfasst die folgenden Unteroptionen:

Unteroption	Beschreibung
Konfigurieren von BSM	Führt das Dienstprogramm für die Setup- und Datenbankkonfiguration aus. Dieses bietet Ihnen die Möglichkeit, das Management, RTSM, die RTSM-Historie und Applikationsdatenbanken/Benutzerschemata auf einem Microsoft SQL Server oder Oracle Server zu erstellen und eine Verbindung herzustellen. Weitere Informationen finden Sie unter "Server Deployment and Setting Database Parameters" im BSM-Installationshandbuch.
BSM deaktivieren	Hält BSM auf einem bestimmten Computer an und deaktiviert die automatische Ausführung beim Start des Computers.
BSM aktivieren	Startet BSM auf einem bestimmten Computer und legt die automatische Ausführung beim Start des Computers fest.
BSM Server Status	Bietet Ihnen die Möglichkeit, den Status von Diensten anzuzeigen, die vom BSM-Dienst und vom Hochverfügbarkeitscontroller ausgeführt werden. Details zu dieser HTML-Seite finden Sie unter "Nach der Bereitstellung" im BSM-Installationshandbuch.

Dokumentation

Die Menüoption **Documentation**, die nur auf dem Gateway-Server verfügbar ist, umfasst die folgende Unteroption:

Unteroption	Beschreibung
BSM Dokumentationsbibliothek	Öffnet die Startseite der BSM Dokumentationsbibliothek in Ihrem Webbrowser.

Öffnen von BSM

Wählen Sie diese Option aus, um die Anmeldeseite für die BSM-Applikation in einem Webbrowser zu öffnen.

Kapitel 2

Anmelden bei BSM

Auf BSM können Sie über einen unterstützten Webbrowser zugreifen, von einem beliebigen Computer mit Netzwerkverbindung (Intranet oder Internet) zu den BSM-Servern. Der Umfang des Zugriffs, der einem Benutzer gewährt wird, hängt von den Berechtigungen des Benutzers ab. Weitere Informationen zum Erteilen von Benutzerberechtigungen finden Sie unter "Zuweisen von Berechtigungen" auf Seite 266.

BSM ist standardmäßig mit LW-SSO (Lightweight Single Sign-On) konfiguriert. Mit LW-SSO können Sie sich bei BSM anmelden und erhalten automatisch Zugriff auf andere konfigurierte Applikationen, ohne sich bei diesen anmelden zu müssen. Weitere Informationen zu den Auswirkungen, die LW-SSO auf die Anmeldung bei BSM hat, finden Sie unter "Anmelden bei BSM mit LW-SSO" auf der nächsten Seite.

Weitere Informationen zu den Webbrowseranforderungen sowie zu den minimalen Anforderungen für die Anzeige von BSM finden Sie unter Systemanforderungen für BSM und Matrizes für die BSM-Unterstützung.

Hinweis: HP Software-as-a-Service-Kunden greifen über HP Software-as-a-Service support Web site (portal.saas.hp.com) auf BSM zu.

Anmelden bei BSM mit LW-SSO

Wenn die Unterstützung für die LW-SSO-Authentifizierung (Lightweight Single Sign-On) aktiviert ist, müssen Sie sicherstellen, dass auch für die anderen Applikationen in der Single Sign-On-Umgebung LW-SSO aktiviert ist und alle denselben initString-Parameter verwenden.

Wenn Sie Single Sign-On für BSM nicht benötigen, sollten Sie LW-SSO deaktivieren. Sie können LW-SSO mit einem der folgenden Dienstprogramme deaktivieren:

- Assistent zur Verwaltung von Authentifizierungen. Weitere Informationen zum Assistenten zur Verwaltung von Authentifizierungen finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.
- **JMX-Konsole.** Weitere Informationen zum Deaktivieren von LW-SSO mithilfe der JMX-Konsole finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 38.

Sobald LW-SSO deaktiviert ist, wird der BSM-Standardauthentifizierungsdienst automatisch aktiviert. Wenn LW-SSO deaktiviert ist oder die Authentifizierungsstrategien IDM-SSO (Identity Management Single Sign-On) oder LDAP (Lightweight Directory Access Protocol) aktiviert sind, müssen Sie die Syntax .<Domänenname> nicht in der URL für die BSM-Anmeldung (http://<Servername>.<Domänenname>/HPBSM) eingeben.

Weitere Informationen zum Implementieren der IDM-SSO- oder LDAP-Authentifizierungsstrategie finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Weitere Informationen zu den Anforderungen für die Anmeldung bei BSM finden Sie unter "Anmelden und Abmelden" auf Seite 27.

Erweiterte Anmeldeoptionen

Die erweiterten Anmeldeoptionen ermöglichen es Ihnen, die Anmeldung zu automatisieren, direkte Anmeldefunktionen zur Verfügung zu stellen, den Zugriff auf die Anmeldung zu begrenzen und Verknüpfungen auf eine bestimmte Seite in BSM herzustellen.

Zu den erweiterten Anmeldeoptionen gehören folgende Funktionen:

- Automatische Anmeldung. Sie können BSM so konfigurieren, dass Sie nach der anfänglichen Anmeldung weder Anmeldenamen noch Kennwort eingeben müssen und dass die Standardseite des Benutzers automatisch geöffnet wird. Weitere Informationen finden Sie unter "Aktivieren der automatischen Anmeldung auf der Anmeldeseite" auf Seite 28.
- **Direkte Anmeldefunktionen.** Sie können einen anderen Benutzer zu einer bestimmten Zielseite in BSM leiten. Weitere Informationen finden Sie unter "Verwenden der Option "Mit dieser Seite verknüpfen" zum Öffnen einer bestimmten Seite" auf Seite 29.
- Beschränken des Anmeldezugriffs. Sie können die Anzahl der Computer beschränken, die unter Verwendung desselben Anmeldenamens auf BSM zugreifen können. Weitere Informationen finden Sie unter "Beschränken der Computeranzahl für den Zugriff mit demselben Anmeldenamen" auf Seite 29.
- Verknüpfungen auf bestimmte Seiten. Sie haben die Möglichkeit, andere Benutzer auf eine bestimmte Seite in BSM zu leiten, indem Sie eine URL mit einem Benutzernamen, Kennwort und mit Informationen über die Zielseite erstellen. Weitere Informationen finden Sie unter "Verknüpfen mit einer bestimmten Seite" auf der nächsten Seite.

Verknüpfen mit einer bestimmten Seite

Sie haben die Möglichkeit, andere Benutzer auf eine bestimmte Seite in BSM zu leiten, indem Sie eine URL mit einem Benutzernamen, Kennwort und mit Informationen über die Zielseite erstellen.

Je nachdem, wie Sie die Option **Mit dieser Seite verknüpfen** verwenden, greift der Empfänger mithilfe einer der folgenden Methoden auf die Seite zu:

- Mit dem eigenen Benutzernamen und Kennwort.
- Mit einer URL, die mit Ihrem Benutzernamen und Kennwort verschlüsselt ist.
- Mit einer URL, die mit dem Benutzernamen und Kennwort eines anderen Benutzers verschlüsselt ist.

Bei Verwendung einer verschlüsselten URL umgeht der Empfänger die BSM-Anmeldeseite, da die URL den Benutzernamen und die Kennwortinformationen bereitstellt.

Bei dem in der URL gesendeten Benutzernamen muss es sich um ein Konto mit ausreichenden Berechtigungen für den Zugriff auf die Zielseite handeln. Falls das Konto nicht über ausreichende Berechtigungen verfügt, wird der Empfänger auf die Seite oberhalb der Zielseite gesendet.

Beispiel: Sie möchten den Empfänger auf die Seite Infrastruktureinstellungen leiten, konfigurieren aber die Option Mit dieser Seite verknüpfen, indem Sie Anmeldeinformationen verwenden für einen regulären Benutzer auswählen (der keine Berechtigungen zum Anzeigen von Infrastruktureinstellungen hat). Wenn der Empfänger die URL erhält, gelangt er auf die Seite Setup und Verwaltung und kann nicht auf die Seite Infrastruktureinstellungen zugreifen.

Die Option **Mit dieser Seite verknüpfen** führt keine Überprüfung des an die URL gesendeten Benutzernamens und Kennworts durch. Eine Überprüfung erfolgt nur, wenn der Empfänger versucht, auf die Zielseite zuzugreifen. Sind Benutzername und Kennwort falsch oder wurde das Benutzerkonto gelöscht, wird der Empfänger an die BSM-Anmeldeseite geleitet, um sich normal anzumelden. Sobald der Empfänger angemeldet ist, wird er nicht an die Zielseite weitergeleitet. Es gibt keine Meldung mit Informationen für die Ursache des Anmeldefehlers.

Zum Anzeigen der Service Health- oder MyBSM-Seiten in einem Drittanbieterportal aktivieren Sie das Kontrollkästchen **Eingebetteter Link** im Fenster **Mit dieser Seite verknüpfen**. Die generierte URL kann in einem Drittanbieterportal verwendet werden, sodass nur die jeweilige Seite angezeigt wird und nicht die gesamte BSM-Applikation mit Menüs.

Hinweis: In einem Drittanbieterportal kann jeweils nur eine Service Health- oder MyBSM-Seite in eine Portalseite eingebettet werden. Wenn Sie mehr Informationen sehen möchten, erstellen Sie eine Seite mit registerkartenbasierten Komponenten. Weitere Informationen finden Sie unter "How to Set Up the MyBSM Workspace" im BSM-Benutzerhandbuch.

Weitere Informationen zur Benutzeroberfläche der Option **Mit dieser Seite verknüpfen** finden Sie unter "Fenster "Mit dieser Seite verknüpfen" auf Seite 35.

Erstellen eines Direkt-Links in RTSM

Mithilfe der Direkt-Link-Funktion können Sie einen Link zu einer bestimmten Zielseite im Run-time Service Model (RTSM) erstellen. Weitere Informationen zu Direkt-Links finden Sie unter "Generate a Direct Link - Overview" im Modeling Guide.

Verwenden der JMX-Konsole

Die JMX-Konsole ist in BSM integriert und ermöglicht Folgendes:

- Durchführen von Verwaltungsoperationen
- Anzeigen der Leistung von Prozessen
- Beheben von Problemen in bestimmten Bereichen von BSM

Zum Zugreifen auf die JMX-Konsole müssen Sie zunächst die relevante URL (http://<Gateway-oder Datenverarbeitungsserver-Name>:8080/jmx-console/, wobei Gateway- oder Datenverarbeitungsserver-Name der Name des Computers ist, auf dem BSM ausgeführt wird) und dann die Authentifizierungsinformationen für die JMX-Konsole eingeben.

Die Anmeldeinformationen für den Zugriff auf die JMX-Konsole werden beim Installieren von BSM und Ausführen des Dienstprogramms für die Setup- und Datenbankkonfiguration konfiguriert. Sie können das Kennwort ändern, nicht jedoch den Benutzernamen. Details zur Änderung des JMX-Kennworts finden Sie unter "Ändern des JMX-Kennworts" auf Seite 31.

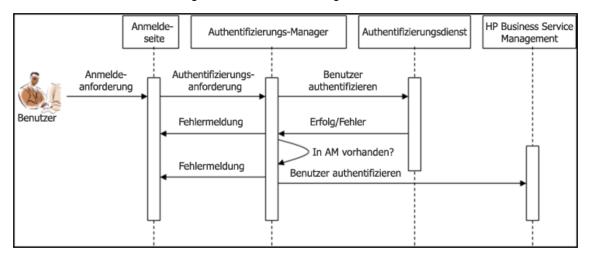
Hinweis: Der Anmeldename kann nicht geändert werden.

Sie können die Verfügbarkeit des BSM-Systems auf der HTML-Seite mit dem HP Business Service Management-Serverstatus überwachen. Weitere Informationen finden Sie unter "Anzeigen des Status von Prozessen und Diensten" auf Seite 19.

Sie können für die JMX-Konsole SSL konfigurieren, um die JMX-Daten aus Sicherheitsgründen zu verschlüsseln. Weitere Informationen finden Sie unter "Configuring the Application Server JMX Console to Work with SSL" im BSM Hardening Guide.

BSM-Anmeldeablauf

In diesem Abschnitt wird der allgemeine Authentifizierungsablauf in BSM beschrieben:



- Ein Benutzer greift auf die Anmeldeseite zu, gibt einen Prinzipal (Anmeldenamen) und Anmeldeinformationen (Kennwort) ein und schickt die Anmeldeanforderung ab (hier durch Klicken auf Anmelden).
- Die Anforderung wird zusammen mit dem Strategienamen, dem Prinzipal und den Anmeldeinformationen an den Manager für die Authentifizierung von BSM übertragen. Sie konfigurieren eine Authentifizierungsstrategie im Assistenten zur Verwaltung von Authentifizierungen. Weitere Informationen finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.
- 3. Der Authentifizierungs-Manager liest den Strategienamen und sendet die Anforderung an die relevante Authentifizierungsstrategie, um den Benutzer zu überprüfen.
- 4. Die relevante Authentifizierungsstrategie akzeptiert die Anforderung und versucht, den Benutzer in Bezug auf den jeweiligen Authentifizierungsdienst zu bestätigen.
- 5. Ist die Authentifizierung genehmigt, überprüft BSM den Benutzer gemäß der ausgewählten Strategie.

Hinweis: Überprüfen Sie beim Erstellen von Benutzern in BSM, ob die Benutzernamen den Benutzernamen in der jeweiligen Strategiedatenbank entsprechen. Eine Anmeldung bei BSM ist nicht möglich, wenn sich die Namen nicht entsprechen.

6. Wenn ein Benutzer die vorangegangenen Schritte erfolgreich durchläuft, gilt er als authentifizierter Benutzer. Die BSM-Seite **Standortübersicht** wird im Webbrowser angezeigt (bzw. die jeweils definierte Standardseite).

Schlägt einer der Schritte fehl, wird der Benutzer benachrichtigt (eine Seiten- und eine Fehlermeldung werden an den Webbrowser zurückgesendet). Der Seiteninhalt und die Fehlermeldung variieren je nach implementierter Strategie.

Anmelden und Abmelden

Sie melden sich über die Anmeldeseite bei BSM an.

Wenn Sie Ihre Sitzung abgeschlossen haben, sollten Sie sich abmelden, um den unberechtigten Zugang zu verhindern.

So greifen Sie auf die BSM-Anmeldeseite zu und melden sich an:

- Geben Sie im Webbrowser die URL http://<Servername>.<Domänenname>/HPBSM ein.
 Dabei stehen Servername und Domänenname für den vollqualifizierten Domänennamen (FQDN) des BSM-Servers. Sind mehrere Server vorhanden oder wurde BSM in einer verteilten Architektur bereitgestellt, geben Sie ggf. die Lastenausgleichs- oder Gateway-Server-URL an.
- 2. Geben Sie die Anmeldeparameter (Anmeldename und Kennwort) eines im BSM-System definierten Benutzers ein und klicken Sie auf **Anmelden**. Nach der Anmeldung wird der Benutzername oben rechts auf der Seite, unterhalb der oberen Menüleiste, angezeigt.

Der erste Zugriff kann über den im Dienstprogramm für die Setup- und Datenbankkonfiguration festgelegten Benutzernamen ("admin") und das Kennwort des Administrators erfolgen.

Achtung:

- Der Superuser des Systems sollte dieses Kennwort sofort ändern, um unberechtigten Zugang zu verhindern. Weitere Informationen zur Benutzeroberfläche zum Ändern des Kennworts finden Sie unter "Registerkarte "Allgemein" (Benutzerverwaltung)" auf Seite 341.
- Der Anmeldename kann nicht geändert werden.

Weitere Informationen zur Benutzeroberfläche zum Erstellen von Benutzern im BSM-System finden Sie unter "Dialogfeld "Benutzer erstellen" auf Seite 339.

Weitere Informationen zu Authentifizierungsmethoden für die Anmeldung, die in BSM verwendet werden können, finden Sie unter "Authentifizierungsstrategien" auf Seite 385.

Informationen zur Fehlerbehebung bei der Anmeldung finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 38.

Hinweis: Details zum sicheren Zugriff auf BSM finden Sie im BSM Hardening Guide.

So melden Sie sich bei BSM ab:

Klicken Sie oben auf der Seite auf Abmelden.

Hinweis: Wenn Sie auf **Abmelden** klicken, wir die Option für die automatischen Anmeldung deaktiviert. Wenn sich ein Benutzer abgemeldet hat, wird bei seiner nächsten Anmeldung die Anmeldeseite geöffnet und der Benutzer muss einen Anmeldenamen und ein Kennwort eingeben. Dies kann nützlich sein, wenn ein anderer Benutzer sich auf demselben Computer mit einem anderen Benutzernamen und Kennwort anmelden muss.

Verwenden der erweiterten Anmeldeoptionen

Sie haben die Möglichkeit, die erweiterten Anmeldeoptionen für BSM zu aktivieren. Weitere Informationen finden Sie unter "Erweiterte Anmeldeoptionen" auf Seite 23.

Aktivieren der automatischen Anmeldung auf der Anmeldeseite

In dieser Aufgabe wird beschrieben, wie die automatische Anmeldung bei BSM aktiviert wird.

 Wählen Sie auf der BSM-Anmeldeseite Meinen Anmeldenamen und das Kennwort 14 Tage speichern aus.

Achtung: Dieser Vorgang kann ein Sicherheitsrisiko darstellen und sollte mit Vorsicht durchgeführt werden.

2. Schließen Sie das Browserfenster nach Beendigung Ihrer Sitzung. Klicken Sie nicht oben auf der Seite auf **Abmelden**.

Durch das Klicken auf **Abmelden** wird die Option der automatischen Anmeldung deaktiviert und der Anmeldename sowie das Kennwort müssen beim nächsten Zugriff auf BSM eingegeben werden.

Hinweis: Wenn das automatische Anmelden auf der Anmeldeseite aktiviert wird und der Benutzer die URL für den Zugriff auf BSM eingibt, tritt Folgendes ein:

- Die Anmeldeseite wird nicht geöffnet.
- Der Anmeldename und das Kennwort müssen nicht eingegeben werden.
- Die Standardseite für diesen Benutzer wird automatisch geöffnet.

Ändern der Einstellungen für die automatische Anmeldung – optional

Optional haben Sie die Möglichkeit, die von Ihnen konfigurierten Einstellungen für die automatische Anmeldung zu ändern.

- Navigieren Sie zu Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen.
- 2. Wählen Sie **Foundation** und anschließend **Sicherheit** aus. Auf dieser Seite können Sie Folgendes durchführen:
 - Stellen Sie die Anzahl der Tage für die Aktivierung der Option ein, indem Sie den Wert unter Dauer der Speicherung der Anmeldeinformationen auf die gewünschte Anzahl der Tage einstellen (der Standardwert lautet 14).
 - Sie verhindern, dass die Option für die automatische Anmeldung auf der Anmeldeseite angezeigt wird, indem Sie den Wert Automatische Anmeldung aktivieren auf false einstellen (der Standardwert lautet true).
 - Konfigurieren Sie die Anzahl der Computer, die gleichzeitig mit demselben Anmeldenamen auf BSM zugreifen können, indem Sie den Wert für Max. Anzahl an Computern pro Anmeldename festlegen (der Standardwert lautet 0). Der Wert 0 bedeutet, dass die Anzahl der Anmeldungen unbegrenzt ist.

Weitere Informationen zur Verwendung der Seite **Infrastruktureinstellungen** finden Sie unter "Infrastruktureinstellungen" auf Seite 103.

Verwenden der URL-Funktion für die automatische Anmeldung

Sie können für den Zugriff auf BSM und für die automatische Anmeldung eine spezielle URL verwenden, die verschiedene Parameter enthält (Anmeldenamen und Kennwort).

Achtung: Diese Methode ist zwar praktisch, stellt allerdings ein Sicherheitsrisiko dar, da das Kennwort in der URL nicht verschlüsselt ist.

Geben Sie in einem Webbrowser folgende URL ein:

http://<Server_name>.<Domänen_name>/<HPBSM_Stammverzeichnis>/TopazSiteServlet? autologin=yes& strategyName=Topaz&requestType=login&userlogin= <Anmeldename>&userpassword=<Kennwort>&createSession=true

Hierbei gilt Folgendes:

- Server_name steht für den Namen des BSM-Servers.
- **Domänen_name** steht für den Namen der Benutzerdomäne gemäß der Netzwerkkonfiguration.
- Anmeldename und Kennwort stehen für den Anmeldenamen und das Kennwort eines in BSM definierten Benutzers.

Um den direkten Zugriff auf BSM zu aktivieren, sollten Sie ein Lesezeichen für die URL der automatischen Anmeldung verwenden.

Verwenden der Option "Mit dieser Seite verknüpfen" zum Öffnen einer bestimmten Seite

Verwenden Sie die Option **Mit dieser Seite verknüpfen**, um einen anderen Benutzer auf eine bestimmte Zielseite BSM zu leiten. Die Option **Mit dieser Seite verknüpfen** erstellt eine URL mit einem Benutzernamen, Kennwort und Informationen über die Zielseite.

Je nach Konfiguration der Parameter im Dialogfeld **Mit dieser Seite verknüpfen** greift der Empfänger mit seinem eigenen Benutzernamen und Kennwort oder über eine URL mit verschlüsseltem Benutzernamen und Kennwort des eigenen oder eines anderen Benutzers auf die Zielseite zu. Sie können diese URL per E-Mail oder SMS an einen anderen Benutzer senden. Bei dem Zugriff über eine verschlüsselte URL auf die Seite umgeht der Empfänger die BSM-Anmeldeseite, da die URL den Benutzernamen und die Kennwortinformationen bereitstellt. Weitere Informationen finden Sie unter "Fenster "Mit dieser Seite verknüpfen" auf Seite 35.

Beschränken der Computeranzahl für den Zugriff mit demselben Anmeldenamen

Auf BSM kann unter Verwendung desselben Anmeldenamens von verschiedenen Computern aus zugegriffen werden. Die Anzahl der Computer, die unter Verwendung desselben Anmeldenamens auf BSM zugreifen, kann mithilfe der Seite **Infrastruktureinstellungen** beschränkt werden.

So ändern Sie den Wert für **Max. Anzahl an Computern pro Anmeldename** auf der Seite **Infrastruktureinstellungen**:

- 1. Klicken Sie auf Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen.
- 2. Wählen Sie Foundation aus.

- 3. Wählen Sie Sicherheit aus.
- 4. Suchen Sie den Eintrag Max. Anzahl an Computern pro Anmeldename und ändern Sie den Wert für die Anzahl der Computer, denen Sie den Zugriff auf BSM unter Verwendung desselben Anmeldenamens ermöglichen möchten. Der Standardwert lautet Null (0) und ermöglicht unbegrenzte Anmeldungen.

Wurde der maximale Wert bei dem Versuch überschritten, sich an BSM anzumelden, erhält der Benutzer eine Fehlermeldung und kann sich nicht anmelden.

Informationen zu dieser Beschränkungsfunktion finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 38.

Öffnen einer Applikationsseite mithilfe einer URL

Sie können eine bestimmte BSM-Seite direkt in Ihrem Browser öffnen, indem Sie eine URL verwenden. Weitere Informationen finden Sie unter "Verknüpfen mit einer bestimmten Seite" auf Seite 24.

Ändern des JMX-Kennworts

In dieser Aufgabe wird beschrieben, wie das JMX-Kennwort geändert wird.

- 1. Beenden Sie das BSM-Gateway oder den Datenverarbeitungsserver.
- 2. Führen Sie die Datei **<HPBSM-Stammverzeichnis>\tools\jmx\changeCredentials.bat** auf dem Gateway- oder auf dem Datenverarbeitungsserver aus.

Das Dialogfeld **Kennwort ändern** wird geöffnet, in dem Sie das neue Kennwort eingeben und bestätigen können. Die Kennwortänderung wird auf dem Gateway oder Datenverarbeitungsserver registriert und verschlüsselt.

3. Starten Sie BSM erneut.

Hinweis: Der Anmeldename kann nicht geändert werden.

Erstellen eines Keystore-Zertifikats

In dieser Aufgabe wird beschrieben, wie ein Keystore-Zertifikat erstellt wird, wenn bisher noch keines vorliegt.

- 1. Führen Sie **cmd.exe** aus, um ein Eingabeaufforderungsfenster zu öffnen.
- 2. Führen Sie den folgenden Befehl aus, um die Keystore-Datei zu erzeugen.

```
keytool -genkey -dname "CN=IhrName,OU=IhreAbteilung,O=IhrFirmenname,
L=IhrOrt,S=IhrStaat, C=IhreLänderkennzahl" -alias <IhrAlias> -
keypass changeit -keystore "<Keystore-Speicherort>" -storepass
changeit -keyalg "RSA" -validity 360
```

Beispiel:

keytool -genkey -dname "CN=John Smith,OU=FND, O=HP, L=Los Angeles,
ST=Unbekannt, C=USAl" -alias john -keypass mypassword -keystore
"D:\HPBSM\JRE\lib\security\cacerts" -storepass changeit -keyalg
"RSA" -validity 360

- 3. Das Keystore-Zertifikat wird in dem Speicherort erzeugt, den Sie im Parameter keystore angegeben haben.
- Starten Sie BSM erneut.

Verfolgen von Anmeldeversuchen und angemeldeten Benutzern

So verfolgen Sie, welche Benutzer eine Systemanmeldung vorgenommen haben:

Zeigen Sie < HPBSM-Stammverzeichnis>\log\EJBContainer\UserActions.servlets.log an.

Der Appender für diese Datei befindet sich unter < HPBSM-Stammverzeichnis>\conf\core\Tools\log4j\EJB\topaz.properties

So zeigen Sie eine Liste der Benutzer an, die aktuell beim System angemeldet sind:

- 1. Öffnen Sie die JMX-Konsole auf diesem Computer. (Ausführliche Anweisungen finden Sie unter "Verwenden der JMX-Konsole" auf Seite 25.)
- 2. Wählen Sie im Abschnitt **Topaz** den Eintrag **service=Active Topaz Sessions** aus.
- 3. Rufen Sie die Operation java.lang.String showActiveSessions() auf.

Sicherheitshinweise und -maßnahmen

In diesem Abschnitt werden die Sicherheitshinweise und -maßnahmen erläutert, die bei der Verwendung von Direct Login für die Anmeldung bei BSM berücksichtigen sind:

- Benutzername und Kennwort in der URL sind verschlüsselt, damit Anmeldeinformationen nie offen gelegt werden.
- Das Senden verschlüsselter Informationen per E-Mail stellt ein Sicherheitsrisiko dar, da das Mailsystem verletzt werden kann. Falls die E-Mail abgefangen wird, erhält ein unbekannter Dritter Zugriff auf BSM.
- Verwenden Sie die URL aus Direct Login nicht als Link auf einer Webseite.
- Der Empfänger verfügt über alle Berechtigungen des Benutzernamens, den er mit der URL erhalten hat. Wenn der Empfänger auf die Zielseite zugreift, kann er in BSM alle Aktionen durchführen, die für diesen Benutzernamen zulässig sind.

Anmelden bei der BSM-Benutzeroberfläche

Dieser Abschnitt umfasst die folgenden Themen:

- "BSM-Anmeldeseite"
- "Fenster "Mit dieser Seite verknüpfen""

BSM-Anmeldeseite

Auf dieser Seite können Sie sich bei BSM anmelden.

Zugriff	Geben Sie in einem Webbrowser die folgende URL ein: http:// <server_name>.<domänenn_name>/<hpbsm-stammverzeichnis>, wobei Server_name der Name der IP-Adresse des BSM-Server ist und Domänen_name der Name der Benutzerdomäne gemäß der Netzwerkkonfiguration.</hpbsm-stammverzeichnis></domänenn_name></server_name>
Wichtiger Hinweis	Wurde LW-SSO (Lightweight Single Sign-On) deaktiviert, müssen Sie die Syntax . <domänen_name> nicht in der Anmelde-URL aufnehmen.</domänen_name>
Relevante Aufgaben	"Anmelden und Abmelden" auf Seite 27
Siehe auch	"Anmelden bei BSM mit LW-SSO" auf Seite 22

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Anmeldename	Geben Sie den jeweiligen Anmeldenamen für den Zugriff auf BSM ein.
Kennwort	Geben Sie den jeweiligen Anmeldenamen für den Zugriff auf BSM ein.
Meinen Anmeldenamen und das Kennwort 14 Tage speichern	Wählen Sie aus, dass BSM den Anmeldenamen und das Kennwort 14 Tage lang speichert. Die Anmeldeinformationen werden automatisch in zukünftigen Anmeldesitzungen eingegeben, wenn diese Option ausgewählt wird.

Fenster "Mit dieser Seite verknüpfen"

Über dieses Fenster können Sie einen anderen Benutzer zu einer bestimmten Zielseite in BSM leiten.

Hinweis: Standardmäßig verfügen nur Administratoren über Sicherheitsrechte für den Zugriff auf diese Funktion.

Zugriff	Wählen Sie Admin > Mit dieser Seite verknüpfen aus.
---------	---

Relevante Aufgaben	"Verwenden der erweiterten Anmeldeoptionen" auf Seite 28
Siehe auch	"Erweiterte Anmeldeoptionen" auf Seite 23
	"Generate a Direct Link User Interface" im Modeling Guide.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Abbrechen	Bricht den Vorgang "Mit dieser Seite verknüpfen" ab.
Link erstellen	Erstellt eine URL, die Benutzer in ihren Browser eingeben können, und zeigt die angegebene BSM-Seite an.
	Hinweis: Wenn Sie diese Option auswählen, nachdem Sie Keine Anmeldeinformationen oder Anmeldeinformationen verwenden ausgewählt haben, und die URL für die Anmeldung auf demselben lokalen Computer aufrufen wollen, auf dem Sie ihn erstellt haben, müssen Sie sich zunächst bei BSM abmelden.
Kennwort bestätigen	Geben Sie das Kennwort erneut ein, das Sie in das Feld Kennwort eingegeben haben.
In Zwischenablage	Kopiert den Inhalt des Feldes Link in die Zwischenablage.
kopieren	Hinweis: Wenn Sie den Firefox-Browser verwenden, müssen Sie Ihre Sicherheitseinstellungen ändern, damit diese Option funktioniert. Geben Sie about:config in das Suchfenster des Browsers ein, suchen Sie nach der Option signed.applets.codebase_principal_support und setzen Sie diese auf true.
Eingebetteter Link	Wird nur in Service Health und MyBSM angezeigt.
	Aktivieren Sie dieses Kontrollkästchen, um eine URL zu erstellen, die in einem Drittanbieterportal verwendet werden kann, sodass nur die jeweilige Seite angezeigt wird und nicht die gesamte BMS-Applikation mit Menüs.
HTML-Code	Generiert eine HTML-Seite für die angegebene BSM-Seite.
	Hinweis: Wenn Sie diese Option auswählen, nachdem Sie Keine Anmeldeinformationen oder Anmeldeinformationen verwenden ausgewählt haben, und sich mit der generierten HTML-Seite auf demselben lokalen Computer anmelden wollen, auf dem Sie diese erstellt haben, müssen Sie sich zunächst bei BSM abmelden.
Link	Die URL, die der Empfänger zum Zugreifen auf die angegebene BSM-Seite verwendet.

Elemente der Oberfläche	Beschreibung
Anmeldename	Der in der URL zu verschlüsselnde Anmeldename, der vom Empfänger für den Zugriff auf die angegebene Seite verwendet wird. Dabei muss es sich um den Anmeldenamen eines tatsächlichen Benutzers handeln.
Meine Anmeldeinformationen	Wählen Sie diese Option, wenn der Link mit Ihrem Anmeldenamen und Kennwort verschlüsselt werden soll.
Keine Anmeldeinformationen	Wählen Sie diese Option, wenn der Empfänger seinen eigenen Anmeldenamen und sein Kennwort für den Zugriff auf die im Link angegebenen Seite verwendet.
Kennwort	Das in der URL zu verschlüsselnde Kennwort, das vom Empfänger für den Zugriff auf die angegebene Seite verwendet wird. Dabei muss es sich um das Kennwort eines tatsächlichen Benutzers handeln.
Anmeldeinformationen verwenden	Wählen Sie diese Option, wenn der Link mit dem Anmeldenamen und Kennwort eines anderen Benutzers verschlüsselt werden soll.

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden die Fehlerbehebung bei der BSM-Anmeldung sowie Anmeldebeschränkungen behandelt.

Fehlerbehebung bei der Anmeldung

Bestimmen Sie die möglichen Ursachen für Anmeldefehler anhand der im Dialogfeld mit der Fehlerwarnung angezeigten Fehlernummer. Weitere Informationen zur Fehlerbehebung finden Sie in der HP-Wissensdatenbank zum Lösen von Softwareproblemen.

Fehlernr.	Problem/mögliche Ursache(n)	Lösung(en)
LI001	BSM konnte keine Verbindung zum JBoss-Applikationsserver herstellen, der auf dem Gateway-Server ausgeführt wird. Mögliche Ursachen: Der JBoss-Server ist heruntergefahren. Probleme mit dem BSM-Dienst Der für den Applikationsserver erforderliche Port wird von einer anderen Applikation verwendet.	Lösung 1: Schließen Sie alle Applikationen auf dem Gateway-Server-Computer und starten Sie den Computer neu. Lösung 2: Vergewissern Sie sich, dass auf dem Gateway-Server-Computer keine anderen Applikationen ausgeführt werden, die diesen Port verwenden (zum Beispiel Applikationen, die aus dem Startverzeichnis ausgeführt werden, eine andere Instanz von JBoss, eines MSDEoder Microsoft SQL Servers oder ein anderer Prozess).
L1002	Der JBoss-Applikationsserver, der auf dem Gateway-Server ausgeführt wird, reagiert nicht oder ist nicht richtig installiert.	Starten Sie die BSM-Applikation neu.
L1003	Die Management-Datenbank ist beschädigt (z. B. wenn ein Benutzerdatensatz versehentlich aus der Datenbank gelöscht wurde).	Versuchen Sie, sich als ein anderer Benutzer anzumelden, oder bitten Sie den BSM- Administrator, einen neuen Benutzer für Sie zu erstellen.
L1004	Die Verbindung zwischen der Tomcat-Servlet-Engine und dem JBoss-Applikationsserver ist wegen einer RMI-Ausnahme (Remote Method Invocation) fehlgeschlagen. Dies kann durch Probleme in RMI-Aufrufen von JBoss verursacht werden.	Vergewissern Sie sich, dass keiner der JBoss- Ports von einem anderen Prozess verwendet wird. Stellen Sie des Weiteren sicher, dass die RMI-Ports gebunden sind. Details zu Ports finden Sie unter "Portverwendung" auf Seite 150.

Fehlernr.	Problem/mögliche Ursache(n)	Lösung(en)
LI005	Die BSM-Anmeldung schlägt fehl oder hängt sich auf. Mögliche Ursachen:	Lösung 1: Vergewissern Sie sich, dass Sie oder die Benutzer eine richtige Kombination aus Anmeldenamen und Kennwort eingeben.
	 Falsche Kombination aus Anmeldename/Kennwort. Es kann keine Verbindung zur Management-Datenbank 	Lösung 2: Vergewissern Sie sich über den ordnungsgemäßen Zustand der Verbindung zur Management-Datenbank. Gehen Sie dazu folgendermaßen vor:
	hergestellt werden. • Der aktuelle Benutzer besitzt keine Zugriffsberechtigungen für Profile. • Die	Geben Sie in einem Webbrowser http:// <name datenverarbeitungsservers="" des="" gateway-servers="" oder="">:8080/jmx- console/index.html ein, um eine Verbindung mit der JMX- Verwaltungskonsole herzustellen.</name>
	Authentifizierungsstrategie wurde nicht eingerichtet/nicht richtig konfiguriert.	 Klicken Sie auf den Link System > JMX MBeans > Topaz > Topaz:service=Connection Pool Information.
		 Lokalisieren Sie java.lang.String showConfigurationSummary() und klicken Sie auf die Schaltfläche Aufrufen.
		 Suchen Sie in den aktiven Konfigurationen der Verbindungs-Factory nach der entsprechenden Zeile für die Management- Datenbank.
		 Vergewissern Sie sich, dass in den Spalten für aktive Verbindungen und/oder Verbindungen im Leerlauf für die Management-Datenbank ein Wert größer als 0 angegeben ist.
		6. Wenn ein Problem mit der Verbindung zur Datenbank vorliegt, vergewissern Sie sich, dass der Datenbankcomputer hochgefahren ist und ausgeführt wird. Führen Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration gegebenenfalls erneut aus.
		Lösung 3: Vergewissern Sie sich, dass der Benutzer die erforderlichen Berechtigungen für den Zugriff auf BSM besitzt. Weitere Informationen zu Benutzerberechtigungen finden Sie unter "Berechtigungen" auf Seite 248.

Fehlernr.	Problem/mögliche Ursache(n)	Lösung(en)
		Lösung 4: Vergewissern Sie sich, dass eine Authentifizierungsstrategie ordnungsgemäß eingerichtet wurde. Details zu Authentifizierungsstrategien finden Sie unter "Authentifizierungsstrategien" auf Seite 385.
LI006	 Wird das Die BSM-Anmeldung schlägt fehl. Mögliche Ursachen: Falsche Cookie-Einstellungen im Webbrowser. Ein nicht unterstütztes Zeichen in den Namen der Computer, die die BSM-Server ausführen. 	Lösung 1: Vergewissern Sie sich, dass der Client-Webbrowser Cookies von BSM-Servern akzeptiert. Lösung 2: Vergewissern Sie sich, dass die Namen der Computer, die die BSM-Server ausführen, keine Unterstrichzeichen (_) enthalten. Wenn solche Zeichen vorhanden sind, benennen Sie den Server um oder verwenden Sie die IP-Adresse des Servers für den Zugriff auf den Computer. Verwenden Sie für den Zugriff auf BSM beispielsweise http://111.222.33.44/ <bsm-stammverzeichnis> anstelle von http://Mein_Server/<bsm-stammverzeichnis>.</bsm-stammverzeichnis></bsm-stammverzeichnis>

Fehlernr.	Problem/mögliche Ursache(n)	Lösung(en)
L1007	Die BSM-Anmeldung schlägt fehl. Die Ursache für diesen Fehler ist, dass die maximale Anzahl gleichzeitiger Anmeldungen von unterschiedlichen Computern erreicht wurde, die mit demselben Anmeldenamen auf BSM zugreifen können.	Lösung 1: Melden Sie sich bei Instanzen von BSM ab, die mit demselben Anmeldenamen von unterschiedlichen Computern angemeldet sind. Anschließend können Sie versuchen, die Anmeldung erneut durchzuführen, wenn die maximale Anzahl nicht erreicht wurde. Lösung 2: Melden Sie sich mit einem anderen Anmeldenamen an, sofern verfügbar.
		Lösung 3: Der Administrator kann die Infrastruktureinstellungen bearbeiten und die Beschränkung aufheben oder die maximale Zahl gleichzeitiger Anmeldungen mit demselben Anmeldenamen von unterschiedlichen Computern erhöhen.
		So bearbeiten Sie diese Einstellung: 1. Klicken Sie auf Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen.
		 Wählen Sie Foundation und Sicherheit aus, und navigieren Sie in der Tabelle Sicherheit - Anmeldung zu dem Eintrag Max. Anzahl an Computern pro Anmeldename.
		3. Ändern Sie den Wert nach Bedarf.
		Der Standardwert 0 ermöglicht unbeschränkte Anmeldungen.

Beschränken des Zugriffs durch unterschiedliche Computer mit demselben Anmeldenamen

In bestimmten Netzwerkkonfigurationen, in denen mehrere Clients von einem Standard-Gatewayoder Proxyserver verarbeitet werden, entspricht die für BSM aufgelöste IP-Adresse der Adresse
des Gateway- oder Proxyservers und nicht der IP-Adresse des Clients. Infolgedessen behandelt
BSM jeden Client so, als würde dieser von derselben IP-Adresse stammen. Da die Anzahl der
Anmeldungen von demselben Computer (IP-Adresse) nicht beschränkt ist, können sich alle Clients
bei BSM anmelden.

Konfigurieren der JMX-Konsole für die Verwendung von SSL-Beschränkungen

Nachdem Sie die JMX-Konsole für die Verwendung von SSL konfiguriert haben, ist der Zugriff auf die Seite **SSM-Stammverzeichnis>\AppServer\webapps\myStatus.war\myStatus.html** nicht mehr möglich, um die Verfügbarkeit von BSM anzuzeigen.

Zurücksetzen der LDAP/SSO-Einstellungen mit der JMX-Konsole

Wenn Ihre LDAP- oder SSO-Einstellungen nicht ordnungsgemäß konfiguriert sind, können Sie möglicherweise nicht auf BSM zugreifen. Wenn dies der Fall ist, müssen Sie Ihre LDAP- oder SSO-Einstellungen mit der JMX-Konsole des mit BSM gelieferten Applikationsservers remote zurücksetzen.

Kapitel 3

Navigieren in und Verwenden von BSM

BSM wird in einem Webbrowser ausgeführt. Sie navigieren mithilfe der folgenden Funktionen in BSM:

- Standortübersicht. Ermöglicht Ihnen einen schnellen Zugriff auf die Kontexte der obersten Ebene im Menü Applikationen oder in der Verwaltungskonsole. Die Standortübersicht ist die erste Seite die standardmäßig geöffnet wird, nachdem Sie sich bei BSM angemeldet haben. Wird die Standardseite nach dem Login geändert, können Sie auf die Standortübersicht zugreifen, indem Sie oben in der Menüleiste oder im Menü Hilfe auf Standortübersicht klicken.
- Menüleiste. Ermöglicht Ihnen die Navigation zu den Applikationen, den Seiten der Verwaltungskonsole, zu den Hilferessourcen und auf den Link zur Standortübersicht.



Sie können auf den Link **Vollbildansicht** klicken, um die aktuelle Seite auf dem gesamten Bildschirm anzuzeigen. Wenn Sie **Vollbildansicht** auswählen, werden der Aufgaben-Assistent (sofern angezeigt), die Menüleiste, Breadcrumbs und die Registerkarten ausgeblendet. Sie kehren wieder zur Standardansicht der Seite zurück, indem Sie auf **Standardansicht** klicken oder auf die Esc-Taste auf der Tastatur klicken.

Darüber hinaus befindet sich oben rechts auf der Seite die Schaltfläche **Abmelden**.

Abmelden

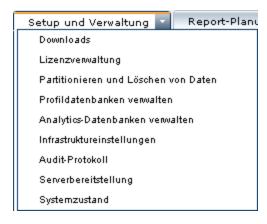
- Registerkarten. Ermöglichen Ihnen die Navigation zu verschiedenen Kontexten in einem bestimmten Bereich von BSM, beispielsweise zu verschiedenen Reporttypen in einer Applikation, zu Ansichten in einem Report oder zu Verwaltungsfunktionen in der Verwaltungskonsole. In bestimmten Kontexten werden Registerkarten verwendet, um zwischen Funktionen zu unterscheiden, in anderen Kontexten werden sie verwendet, um ähnliche Funktionen oder Features zusammenzufassen.
- Hauptmenüs der Registerkarten. Ermöglichen die Navigation von einer Titelseite der Registerkarte zu den verschiedenen Kontexten, die mit der Registerkarte verbunden sind. Die Hauptmenüs der Registerkarten werden angezeigt, wenn Sie eine Registerkarte auswählen, die verschiedene Kontexte enthält, wie Reporttypen oder Verwaltungseinstellungen. Zu den Hauptmenüs der Registerkarten gehören eine Beschreibung und eine Miniaturdarstellung des Registerkarteninhalts.



• Registersteuerelemente. Helfen bei der Navigation von einem Kontext zu einem anderen Kontext der Registerkarte. Sie öffnen das Hauptmenü der Registerkarte, indem Sie auf den Namen der Registerkarte klicken.



Sie wechseln problemlos zu einem andern Kontext einer Registerkarte, indem Sie den Mauszeiger über das Register führen und auf den Abwärtspfeil klicken , um das Dropdown-Menü des Registers zu öffnen. Klicken Sie auf eine Menüoption, um zu diesem Kontext zu wechseln.



Navigationsschaltflächen.



Mithilfe der Vor- und Zurückschaltflächen oben links im Fenster können Sie zwischen den angezeigten Seiten navigieren. Sie können zur vorher angezeigten Seite oder zur nächsten Seite wechseln, die Sie angezeigt haben, bevor Sie auf die Zurückschaltfläche geklickt haben.

Zuletzt verwendete Seiten.



Sie können aus einer Dropdownliste die Seiten auswählen, die in der Historie gespeichert werden. Die Aktivierung erfolgt durch Auswahl des Abwärtspfeils neben den Vor- und Zurückschaltflächen. In dieser Historie befinden Sie die letzten Kontexte, die Sie angezeigt haben. Es können bis zu 20 angezeigte Seiten aufgenommen werden.

Bei den in der Historie gespeicherten Seiten handelt es sich um die Seiten, die BSM auf dem Server gespeichert hat. Wenn Sie zu einer zuvor angezeigten Seite eines Reports zurückkehren, wird die Seite genau so angezeigt, wie Sie sie mit den zuvor gewählten Filtern und Bedingungen verlassen haben.

Es gibt auch einige Seiten, deren Kontexte und Auswahlen nicht gespeichert werden. Wenn Sie zu diesen Seiten zurückkehren, müssen Sie die Optionen möglicherweise erneut auswählen. Wenn Sie beispielsweise in einem bestimmten Kontext in den Infrastruktureinstellungen arbeiten und zu dieser Seite mithilfe der Historie zurückkehren, wurde der Kontext nicht gespeichert und auf der Seite werden die Standardeinstellungen angezeigt.

Tipp: Sie können die Anzahl der in der Historie angezeigten Seiten ändern (standardmäßig 20), indem Sie die Datei **<HPBSM-Stammverzeichnis>\conf\settings\website.xml** öffnen und den Wert unter **history.max.saved.pages** ändern. Diese Änderung wird auf Serverseite vorgenommen und ist daher für alle Benutzer gültig.

 Breadcrumbs. Ermöglichen Ihnen, bei einem Kontext mit mehreren Ebenen auf vorherige Seiten zu navigieren, indem Sie auf die entsprechende Seitenebene klicken. In der folgenden Breadcrumb-Anzeige würden Sie beispielsweise auf Aufschlüsselungsübersicht klicken, um zum Bericht Aufschlüsselungsübersicht zurückzukehren.

Geschäftsprozess > Aufschlüsselungsübersicht > Rohdaten für Transaktionsaufschlüsselung > WebTrace nach Standort

Ist die Breadcrumb-Anzeige länger als der Bildschirm, wird nur der abschließende Teil angezeigt. Klicken Sie auf das Symbol **Anzeigen** links von der Breadcrumb-Anzeige, um den ausgeblendeten Teil in der aktuellen Registerkarte anzuzeigen.

Tipp: Die Funktion **Zurück** des Webbrowsers wird in BSM nicht unterstützt. Mit der Funktion **Zurück** wird der aktuelle Kontext nicht immer auf den vorherigen Kontext umgestellt. Um zu einem vorherigen Kontext zu wechseln, verwenden Sie die Navigationsschaltflächen in BSM oder die Breadcrumb-Funktion.

Verbesserungen der Benutzeroberfläche

Die BSM-Oberfläche enthält viele Funktionen für eine verbesserte Bedienung. Dazu gehören die folgenden Komponenten:

 Konformität mit "Section 508". BSM entspricht den Normen zur Barrierefreiheit und Verwendbarkeit für Personen mit Behinderungen, die im "Electronic and Information Technology Accessibility and Compliance Act" ("Section 508") der USA (Gesetz zur Barrierefreiheit und Konformität in der elektronischen und Informationstechnologie) festgeschrieben sind, und unterstützt den JAWS®-Screenreader.

JAWS-Benutzer sollten die Einstellung **Eingabehilfen für Benutzer** von **false** in **true** ändern. Gehen Sie hierzu wie folgt vor:

- Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus.
- Wählen Sie Foundation aus.
- Wählen Sie Business Service Management-Schnittstelle aus.
- Suchen Sie im Bereich Business Service Management-Schnittstelle Anzeigen nach der Einstellung Eingabehilfen für Benutzer. Ändern Sie den Wert in true.
- **Personalisierung.** BSM behält die Anpassungen von Tabellen (z. B. Spaltenbreite und Spaltensichtbarkeit), die Sie mit einer Reihe von Anwendungen und Funktionen vornehmen können, z. B. Empfängerverwaltung, Reports-Verwaltung, Reports und Zeitplanung von Reports, für die nächste Sitzung bei.

Hinweis: Wenn zwei oder mehr Benutzer mit den gleichen Anmeldeinformationen angemeldet sind, kann BSM die persönlichen Einstellungen möglicherweise nicht abrufen.

- **Tabellenfunktionen.** Sie können Tabellen in BSM auf vielfältige Weise bearbeiten. Mit verschiedenen Steuerelementen könnten Sie z. B. folgende Aufgaben durchführen:
 - **Filtern.**BSM-Tabellen umfassen verschiedene Filteroptionen. Für eine erweiterte Bearbeitung von Filtern klicken Sie auf _____.
 - Sortieren. Klicken Sie auf eine Spaltenüberschrift, um die Tabelle anhand dieser Spalte zu sortieren. Bei jedem Klicken auf die Spaltenüberschrift ändert sich die Sortierreihenfolge von aufsteigend in absteigend und umgekehrt.
 - Auswählen von Spalten. Klicken Sie auf , um die anzuzeigenden Spalten auszuwählen.
 - Ändern der Spaltenbreite. Ziehen Sie die Begrenzung einer Spaltenüberschrift nach links oder rechts, um die Spaltenbreite zu ändern. Klicken Sie auf die ursprüngliche Breite zurückzusetzen.
 - Ändern der Spaltenreihenfolge. Ziehen Sie eine Spaltenüberschrift nach links oder rechts, um die Spaltenreihenfolge zu ändern.

Tabelle verschieben.

■ Exportieren. Klicken Sie auf die entsprechende Schaltfläche, um die Tabelle in ein anderes Format zu exportieren, z. B. Excel , PDF oder CSV.

Weitere Details zu Tabellenfunktionen in Reports finden Sie unter "Common Report and Page Elements".

Hinweis: Nicht alle Tabellen unterstützen alle Tabellenfunktionen.

- Anpassen des Mastertitels und Logos. Sie k\u00f6nnen den Applikationstitel und das Masterlogo (standardm\u00e4\u00df) das HP-Logo), die beide in der oberen linke Ecke des BSM-Fensters angezeigt werden, anpassen. Diese \u00e4nderung wird auf Serverseite vorgenommen und ist f\u00fcr alle Benutzer sichtbar, die auf BSM zugreifen. Weitere Informationen finden Sie unter "Anpassen von Mastertitel und Logo" auf der n\u00e4chsten Seite.
- Sitzungsablauf. Standardmäßig wird der Ablauf einer BSM-Sitzung durch einen Ping-an-Server-Mechanismus, ein sogenanntes Keep-Alive für Sitzung, verhindert. Sie können das automatische Ablaufen von Sitzungen durch Deaktivieren von Keep-Alive für Sitzung ermöglichen.

Wählen Sie zum Deaktivieren von **Keep-Alive für Sitzung** die Optionen **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen**:

- Wählen Sie Foundation aus.
- Wählen Sie Business Service Management-Schnittstelle aus.
- Suchen Sie im Bereich Business Service Management-Schnittstelle Zeitliche Steuerung nach der Einstellung Keep-Alive für Sitzung aktivieren. Ändern Sie den Wert in false.

Anpassen von Mastertitel und Logo

So ändern Sie den Text des Titels und das Logo:

- Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus.
- 2. Wählen Sie den Kontext Foundation aus.
- 3. Wählen Sie Business Service Management-Schnittstelle aus der Liste.
- 4. Ändern Sie in der Tabelle Business Service Management-Schnittstelle Benutzerdefinierter Mastertitel den folgenden Eintrag:
 - Geben Sie unter **Titel der Applikation im benutzerdefinierten Mastertitel** den Text ein, der als Titel für die Applikation verwendet werden soll. Wenn kein Wert für dieses Feld angegeben wurde, wird standardmäßig **Business Service Management** angezeigt. Sie können die HTML-Codierung für die Texteingabe verwenden, aber keine Skripts eingeben. Wenn Sie HTML verwenden, überprüfen Sie die Gültigkeit vor dem Speichern.
 - Geben Sie unter Logo-URL für benutzerdefinierten Mastertitel die URL der Datei ein, die das Logo enthält, das oben im Fenster angezeigt werden soll. Wenn kein Wert für dieses Feld angegeben wurde, wird standardmäßig das HP-Logo angezeigt. Es wird empfohlen, ein Bild mit einer Höhe von 19 Pixeln zu verwenden. Ist das Bild höher, wird es nicht ordnungsgemäß im Mastertitel angezeigt.

Nachdem Sie diese Einstellungen geändert haben, wird die Änderung angezeigt, sobald der Browser aktualisiert wird.

Client-Anforderungen für die Anzeige von BSM

In der folgenden Tabelle werden die minimalen und empfohlenen Clientsystemanforderungen für die Anzeige von BSM beschrieben:

Anzeige	Minimum: Farbpaletteneinstellung von mindestens 256 Farben
	Empfohlen: Farbpaletteneinstellung von 32.000 Farben
Auflösung	1280 x 1024 oder höher (unterstützt)
	1400 x 1200 oder höher (empfohlen)
Unterstützte Browser	Microsoft Internet Explorer (IE) 9.0
	Microsoft Internet Explorer (IE) 8.0
	Microsoft Internet Explorer (IE) 7.0
	Mozilla Firefox ESR 10.0
	Hinweis:
	Der Browser muss so eingestellt sein, dass alle Cookies akzeptiert werden.
	Der Browser muss so eingestellt sein, dass die JavaScript- Ausführung aktiviert ist.
	Der Browser muss Pop-up-Fenster unterstützen. HP Business Service Management funktioniert nicht ordnungsgemäß, wenn Sie Web-Anwendungen verwenden, die Pop-up-Fenster in Ihrem Browser blockieren.
	Benutzer von Internet Explorer müssen das Browser-Caching so einstellen, dass automatisch nach neueren Versionen gespeicherter Seiten gesucht wird.
Flash Player	Adobe Flash 10.1 oder höher
Schriftarten	Auf Client-Systemen müssen die folgenden Schriftarten installiert sein:
	MS Gothic für Japanisch
	Gulim für Koreanisch
	SimSun für vereinfachtes Chinesisch
	Arial für alle anderen Gebiete

Java-Plug-In (für die Anzeige von Applets)

Empfohlen: Version 6 Update 31

Unterstützt: Version 6 Update 26 und höher oder Version 7

Hinweis: Sie können mit einer früheren Java-Version möglicherweise nicht alle HP Business Service Management-Applets anzeigen und müssen die neueste Version von der Java-Download-Website (http://www.java.com/en/download/manual.jsp) herunterladen und installieren. Möglicherweise müssen Sie auch frühere Versionen nach dem Download deaktivieren.

Gehen Sie bei Internet Explorer folgendermaßen vor: Wählen Sie Extras > Internetoptionen > Registerkarte "Erweitert", suchen Sie das Element Java (Sun), aktivieren Sie das Kontrollkästchen für die richtige Java-Version, klicken Sie auf OK, schließen Sie den Browser und öffnen Sie diesen wieder.

Details zum Überprüfen der Java-Version in Mozilla Firefox finden Sie in der Mozilla Firefox-Dokumentation.

Anzeigen der Dokumentbibliothek

Die Dokumentbibliothek lässt sich am besten im Internet Explorer anzeigen.

Die Dokumentbibliothek kann am besten in einem Browser mit Java-Unterstützung angezeigt werden. Verfügt Ihr Browser nicht über Java-Unterstützung, laden Sie das Sun Java-Plug-In von der Sun Java-Website (http://java.com/de/index.jsp) herunter. Beachten Sie, dass die Dokumentbibliothek automatisch mit der JavaScript-Implementierung geöffnet wird, wenn Java nicht unterstützt wird. Die JavaScript-Implementierung bietet die gleichen Grundfunktionen wie die Java-Implementierung, sie ermöglicht jedoch nicht die Verwendung der Registerkarte für Favoriten im Navigationsbereich.

Wenn beim Öffnen der Dokumentbibliothek ein JavaScript-Fehler auftritt, deaktivieren Sie das Kontrollkästen für die Anzeige von Ausnahmen in der Java-Konsole und öffnen Sie die Hilfe erneut.

Tipps zu Problemen beim Öffnen von Java-Applets:

Wenn Probleme beim Öffnen von Java-Applets über die Benutzeroberfläche auftreten, können Sie einen oder beide der folgenden Schritte durchführen:

- Wählen Sie, wenn Sie Internet Explorer verwenden, Extras > Internetoptionen >
 Verbindungen > LAN-Einstellungen aus. Deaktivieren Sie die folgenden Optionen:
 Automatische Suche der Einstellungen und Automatisches Konfigurationsskript verwenden.
- Wählen Sie unter Systemsteuerung > Java > Registerkarte Allgemein >
 Netzwerkeinstellungen die Option Direktverbindung aus (anstelle der Standardoption Browsereinstellungen verwenden).

Menüs und Optionen

In der oberen Menüleiste können Sie die folgenden Applikationen und Ressourcen auswählen:

MyBSM

Öffnet die Applikation MyBSM, ein Portal, das die Benutzer so anpassen können, dass die für sie wichtigen Schlüsselinhalte angezeigt werden. Weitere Informationen finden Sie unter "Überwachen Ihrer Umgebung mit MyBSM" im BSM-Benutzerhandbuch.

Applikationen für Geschäftsbenutzer

BSM stellt die weiter unten aufgeführten Applikationen für Geschäftsbenutzer zur Verfügung. Sie können über das Menü **Applikationen** auf alle Applikationen zugreifen. Eine Ausnahme bildet die Applikation MyBSM, auf die über die obere Menüleiste zugegriffen wird.

Menüoption	Beschreibung
Service Health	Öffnet die Anwendung Service Health, ein Dashboard für die Anzeige von Leistungs- und Verfügbarkeitsdaten aus einer Geschäftsperspektive. Weitere Informationen finden Sie unter "Einführung in Service Health" im BSM-Benutzerhandbuch.
CI-Status	Öffnet die Oberfläche für CI-Status-Reports. Details finden Sie unter "Benutzeroberfläche für CI-Status-Reports"
Service Level Management	Öffnet die Service Level Management-Applikation, in der Sie proaktiv Servicelevel aus einer Geschäftsperspektive verwalten können. Service Level Management bietet den Teams für IT-Operationen und Serviceprovidern ein Werkzeug für die Verwaltung von Servicelevels und stellt darüber hinaus SLA-Compliance (Service Level Agreement, Vereinbarung zum Servicelevel) für das Berichten von komplexen Geschäftsapplikationen in verteilten Umgebungen zur Verfügung. Weitere Informationen finden Sie unter "Working with the Service Level Management Application" im BSM-Benutzerhandbuch.
End User Management	Öffnet die End User Management-Applikation, die für das Überwachen von Applikationen aus der Endbenutzerperspektive und für das Analysieren der wahrscheinlichsten Ursache für Leistungsaspekte verwendet wird. Weitere Informationen finden Sie unter "Übersicht über End User Management-Reports" im BSM-Benutzerhandbuch.
Operations Management	Öffnet die Operations Management-Applikation, die für das proaktive Verwalten von Ereignissen aus einer Geschäftsperspektive zum Wiederherstellen von Services und zum Minimieren von Serviceunterbrechungen verwendet wird. Weitere Informationen finden Sie unter "Operationenverwaltung - Übersicht" im BSM-Benutzerhandbuch.
Transaction Management	Zeigt die Transaktionstopologie und -infrastruktur für die Datensammlung und Reportanzeige an. Weitere Informationen finden Sie unter "Transaction Management Overview" im BSM-Benutzerhandbuch.

Menüoption	Beschreibung
System Availability Management	Öffnet die System Availability Management-Applikation, die für die vollständige System- und Infrastrukturüberwachung sowie für die Ereignisverwaltung verwendet wird. Weitere Informationen finden Sie unter "System Availability Management - Übersicht" im BSM-Benutzerhandbuch.
Service Health Analyzer	Öffnet die Service Health Analyzer-Applikation zum Anzeigen von CIs mit Anomalien. Weitere Informationen finden Sie unter "Service Health Analyzer Overview" im BSM-Benutzerhandbuch.
Benutzerreports	Öffnet den Report Manager, der für das Erstellen und Speichern von Benutzerreports verwendet wird. (Diese Reports enthalten benutzerdefinierte Daten und Formatierungen, mit denen Sie sich auf spezielle Aspekte der Applikations- und Infrastrukturressourcenleistung Ihrer Organisation konzentrieren können.) Weitere Informationen zum Report Manager finden Sie unter "User Reports Overview" im BSM-Benutzerhandbuch.

Verwaltungskonsole

Mithilfe der Verwaltungskonsole verwalten Administratoren die BSM-Plattform und -Applikationen. Die Verwaltungskonsole besteht aus mehreren Abschnitten, die nach ihrer Funktion organisiert sind. Sie greifen über das Menü **Admin** auf die Funktionsbereiche zu. Sie können die folgenden Menüoptionen auswählen:

Menüoption	Beschreibung
Service Health	Öffnet die Service Health-Verwaltung-Seiten, in denen Sie KPIs (Key Performance Indicators) an die CIs anfügen können. Ferner können Sie benutzerdefinierte und geografische Karten und Repositories definieren. Weitere Informationen finden Sie unter "Introduction to Service Health Administration" im BSM Application Administration Guide.
Service Level Management	Öffnet die Service Level Management-Verwaltungsseiten, in denen Sie die Servicevereinbarungen (SLAs, OLAs, UCs) erstellen und Services einrichten können, die mit den von Service Level Management erfassten Daten verknüpft werden. Weitere Informationen finden Sie unter "Introduction to SLM Administration" im BSM Application Administration Guide.
Operations Management	Öffnet die Operations Management-Verwaltungsseiten. Weitere Informationen finden Sie unter "Setup" im BSM Application Administration Guide.
End User Management	Öffnet die End User Management-Verwaltungsseiten, in denen Sie Daten-Collectoren von Business Process Monitor und Real User Monitor konfigurieren und verwalten. Darüber hinaus können Sie Transaktionsreihenfolgen, Farbeinstellungen und Report-Filter konfigurieren. Weitere Informationen finden Sie unter "End User Management Administration" im BSM Application Administration Guide.

Menüoption	Beschreibung
System Availability Management	Öffnet die System Availability Management-Verwaltungsseiten, in denen Sie den SiteScope-Daten-Collector konfigurieren und verwalten können. Weitere Informationen finden Sie unter "System Availability Management Administration Overview" im BSM Application Administration Guide.
RTSM - Verwaltung	Öffnet die RTSM-Verwaltungsseiten, in denen Sie ein Modell Ihres IT Universe in Run-time Service Model (RTSM) erstellen und verwalten können. In der RTSM-Verwaltung verwenden Sie die Datenflussverwaltung- und die Adapterquellen, die für die Erstellung des IT Universe-Modells mit CIs (Configuration Items), den Vorlagen für das Erstellen von CIs und dem System für die Anzeige der CIs in BSM-Applikationen eingesetzt werden. Sie können CIs auch manuell erstellen und zum Modell hinzufügen. Weitere Informationen finden Sie im Modeling Guide.
Business Service Management for Siebel- Verwaltung	Öffnet die Application Management für Siebel-Verwaltungsseite.
Plattform	Öffnet die Plattformverwaltungsseiten, die umfassende Funktionen zur Plattformverwaltung und -konfiguration bieten.
Integrationen	Öffnet den Verwaltungsbereich für BSM-Integrationen, in dem Sie folgende Verwaltungsaufgaben ausführen können:
	BSM Connector-Integrationen zur Erfassung und Weiterleitung von Daten aus Drittanbietersystemen in BSM.
	Zuordnungen zwischen CIs und Operations Orchestration-Run Books.
	Application Lifecycle Management-Integrationen für den Export zugehöriger Daten und die Überwachung von Werkzeugkonfigurationen.
	Veraltete Integrationsmethoden - Integration Adapter- und EMS-Integrationen.
	Details finden Sie unter "Integrating with Other Applications - Overview" im BSM Application Administration Guide
Mit dieser Seite verknüpfen	Wählen Sie diese Option aus, um auf die Funktion zum Verknüpfen einer Seite zuzugreifen, mit der Sie eine URL erstellen können, der direkten Zugriff auf eine bestimmte Seite in BSM ermöglicht. Weitere Informationen finden Sie unter "Fenster "Mit dieser Seite verknüpfen" auf Seite 35.
	Hinweis: Standardmäßig verfügen nur Administratoren über Sicherheitsrechte für den Zugriff auf diese Funktion.

Menüoption	Beschreibung
Persönliche Einstellungen	Wählen Sie diese Option aus, um die Registerkarte mit den persönlichen Einstellungen zu öffnen, in der Sie verschiedene Aspekte von BSM wie Menüs und Kennwörter individuell festlegen können. Beachten Sie, dass die Funktion Persönliche Einstellungen allen Benutzern zur Verfügung steht. Weitere Informationen finden Sie unter "Persönliche Einstellungen" auf Seite 377.

Menü "Hilfe"

Sie können die folgenden Online-Ressourcen über das BSM-Menü **Hilfe** öffnen:

Menüoption	Beschreibung
Hilfe zu dieser Seite	Öffnet die Dokumentationsbibliothek mit dem Thema, das die aktuelle Seite oder den Kontext beschreibt.
Dokumentationsbibliothek	Öffnet die Dokumentationsbibliothek-Homepage. Die Homepage bietet direkte Links auf die wichtigsten Hilfethemen.
Diagnostics-Hilfe	Öffnet die Diagnostics-Hilfe, wenn ein Diagnostics-Server mit BSM verbunden ist.
Fehlerbehebung & Wissensdatenbank	Öffnet die HP Software-Unterstützung-Website direkt auf der Seite mit den Optionen zur Fehlerbehebung (Anmeldung mit HP Passport ist erforderlich). Die URL für diese Website lautet http://h20230.www2.hp.com/troubleshooting.jsp.
HP Software- Unterstützung	Öffnet die HP Software-Unterstützung-Website. Auf dieser Seite können Sie die Wissensdatenbank durchsuchen, Ihre eigenen Artikel hinzufügen, Beiträge in den Diskussionsforen für Benutzer veröffentlichen oder die Beiträge von anderen durchsuchen, Supportanfragen übermitteln, Patches und aktualisierte Dokumentationen herunterladen usw. Die URL für diese Website lautet http://www.hp.com/go/hpsoftwaresupport.
HP Software-Website	Öffnet die HP Software-Website, die Informationen und Ressourcen zu HP Software-Produkten und -Diensten enthält. Die URL für diese Website lautet http://www.hp.com/go/software.
Aufgaben-Assistent	Öffnet den Aufgaben-Assistenten , mit dessen Hilfe bestimmte Aufgaben durch Auflisten der entsprechenden Aufgabenschritte und Bereitstellen der Links zu den jeweiligen Hilfethemen für jeden Schritt vereinfacht werden.

Menüoption	Beschreibung
Standortübersicht	Öffnet die Standortübersicht , die Ihnen einen schnellen Zugriff auf die Kontexte der obersten Ebene im Menü Applikationen oder in der Verwaltungskonsole ermöglicht.
	Hinweis: Bei der Standortübersicht handelt es sich um die standardmäßige Eingangsseite, die nach der Anmeldung an BSM angezeigt wird. Klicken Sie in der Standortübersicht auf Standardseite ändern, um die Registerkarte für Persönliche Einstellungen zu öffnen und eine andere Eingangsseite zu wählen. Weitere Informationen zum Konfigurieren der Registerkarte für Persönliche Einstellungen finden Sie unter "Persönliche Einstellungen" auf Seite 377.
Neues	Öffnet das Dokument mit den Neuigkeiten, in dem die neuen Funktionen und Erweiterungen der Version beschrieben werden.
Info HP Business Service Management	Öffnet das Dialogfeld mit den Informationen zu HP Business Service Management, in dem Versions-, Lizenz-, Patch- und Drittanbieterinformationen angezeigt werden.

Teil 2

Setup und Verwaltung

Kapitel 4

Downloads

Sobald die Server für BSM installiert sind, müssen mehrere Komponenten heruntergeladen werden. Zu diesen Komponenten gehören Werkzeuge zum Überwachen Ihres Unternehmens und Aufzeichnen von Geschäftsprozessen.

Zum Anzeigen und Herunterladen von Komponenten von der Downloadseite nach der Installation von BSM müssen Sie die Setup-Datei der Datenerfassung installieren. Weitere Informationen finden Sie unter "Installing Component Setup Files" im BSM-Installationshandbuch.

Aufgaben

Herunterladen von Komponenten

In dieser Aufgabe wird beschrieben, wie Komponenten über die Seite **Komponenten herunterladen** heruntergeladen werden:

- 1. Wählen Sie die Komponente aus, die Sie herunterladen möchten.
- 2. Speichern Sie die Setup-Datei auf Ihrem Computer.
- 3. Führen Sie die Setup-Datei der Komponente aus, um die Komponente zu installieren.

Komponenten der Benutzeroberfläche

Seite "Komponenten herunterladen"

Auf dieser Seite werden die BSM-Komponenten aufgelistet, die zum Herunterladen zur Verfügung stehen. Dazu gehören auch Werkzeuge zum Überwachen des Unternehmens und zum Aufzeichnen von Geschäftsprozessen.

Zugriff	Wählen Sie Admin> Plattform > Setup und Verwaltung > Downloads aus.
Wichtiger Hinweis	Sie können die herunterzuladenden Komponenten entweder nach Kategorie oder nach System filtern.
	 Da einige Dateien sofort ausgeführt werden, wenn Sie auf die Option für den Download klicken, klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen Ziel speichern unter und anschließend den Speicherort für die Datei aus.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
	Setzt die Breite der Tabellenspalten auf die Standardeinstellung zurück. Sie können die Breite der Tabellenspalten anpassen, indem Sie die Ränder der Spalte nach rechts oder links ziehen.
	Öffnet das Dialogfeld Spalten auswählen , in dem Sie die in der Tabelle anzuzeigenden Spalten auswählen können.
1 V /1 Seiten	Teilt die Datentabelle in Seiten ein. Sie können mit der entsprechenden Schaltfläche von Seite zu Seite blättern:
	Um weitere Reports anzuzeigen, klicken Sie auf Nächste Seite oder Letzte Seite.
	Um frühere Reports anzuzeigen, klicken Sie auf Vorherige Seite oder Erste Seite.

Elemente der Oberfläche	Beschreibung
Kategorie	Die Kategorie der herunterzuladenden Komponente. Verfügbare Kategorien sind:
	Business Process Insight. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen von Business Process Insight-Komponenten in BSM ermöglichen.
	Business Process Monitor. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen von Business Process Monitor-Komponenten in BSM ermöglichen.
	Data Flow Probe. Die herunterladbare Data Flow Probe-Datei, die es Ihnen ermöglicht, die Data Flow Probe-Komponente in BSM zu installieren und auszuführen.
	Diagnostics. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen von Diagnostics- Komponenten ermöglichen.
	Sonstiges. Wird für den Download sonstiger Applikationen verwendet. Wenn für diese Kategorie keine Applikationen aufgelistet sind, stehen keine zur Verfügung.
	Real User Monitor. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen von Real User Monitor-Komponenten ermöglichen.
	SiteScope. Herunterladbare SiteScope-Dateien, die Ihnen das Installieren und Ausführen von SiteScope- Komponenten ermöglichen.
	Hinweis: Stellen Sie sicher, dass die ausgewählte Datei dem Betriebssystem entspricht, mit dem Sie arbeiten.
	TransactionVision. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen von TransactionVision-Komponenten ermöglichen.
	TransactionVision oder Diagnostics. Herunterladbare Dateien, die Ihnen das Installieren und Ausführen der Datei HP-Diagnostics/TransactionVision Agent für Java ermöglichen.
Beschreibung	Eine Erklärung der jeweiligen herunterladbaren Datei.

Elemente der Oberfläche	Beschreibung
Dokument	Eine Verknüpfung zur PDF-Beschreibung der Komponente.
	Hinweis: Nicht für alle Komponenten ist ein entsprechendes PDF-Dokument verfügbar.
Dateiname	Der Name der jeweiligen Datei, die für das Download verfügbar ist.
System	Das Betriebssystem, auf dem die BSM-Komponenten ausgeführt werden sollen.

Kapitel 5

Lizenzverwaltung

Sie müssen über eine gültige Lizenz zum Ausführen von Monitoren und Transaktionen und für die Verwendung verschiedener integraler Applikationen in BSM verfügen.

Mit der BSM-Lizenz können Sie eine zuvor bestimmte Anzahl von Monitoren und Transaktionen über einen bestimmten Zeitraum gleichzeitig ausführen. Wie viele Monitore und Transaktionen Sie gleichzeitig ausführen können, welche Applikationen Sie ausführen können sowie das Ablaufdatum der Lizenz ist abhängig von der jeweiligen Lizenz, die Ihr Unternehmen von HP erworben hat.

Die Erstlizenz kann nur während des Installationsprozesses im Rahmen des Konfigurations-Assistenten installiert werden.

BSM veröffentlicht 15 Tage vor Ablauf der Lizenz eine Lizenzablauferinnerung im Anschluss an die Anmeldeseite der Website (nur für Administratoren).

Für eine Reihe von BSM-Applikationen sind jedoch zusätzliche Lizenzen erforderlich. Um diese Applikationen verwenden zu können, müssen Sie eine Lizenz von HP erhalten und die Lizenzdatei dann in BSM hochladen. Weitere Informationen zur Lizenzstruktur von Operations Manager i (OMi) finden Sie unter "Licensing" im BSM-Benutzerhandbuch.

Zugriff

Zum Öffnen der Seite für die Lizenzverwaltung wählen Sie **Admin > Plattform > Setup und Verwaltung > Lizenzverwaltung** aus.

Zum Anzeigen des Lizenzstatus wählen Sie Admin > Plattform > Lizenzverwaltung aus.

Aufgaben

Hinzufügen einer neuen Lizenz

So aktualisieren Sie Ihre Bereitstellung mit einer neuen Lizenz:

- 1. Wählen Sie Admin > Plattform > Setup und Verwaltung > Lizenzverwaltung aus.
- 2. Klicken Sie auf **Lizenz aus Datei hinzufügen**, um das Dialogfeld **Lizenz hinzufügen** zu öffnen, in dem Sie nach der entsprechenden .dat-Datei suchen können. Die Datei wird vom Clientcomputer auf den BSM-Server hochgeladen.
- 3. Klicken Sie unten in der Seite Lizenzverwaltung auf den Link Serverbereitstellung.

Beschreibung der Benutzeroberfläche

Seite "Lizenzverwaltung"

Elemente der Oberfläche	Beschreibung
+	Lizenz hinzufügen. Öffnet das Dialogfeld Lizenz hinzufügen.
	Verwenden Sie das Dialogfeld zum Hochladen einer Lizenzdatei. Sie müssen den Speicherort der Lizenzdatei festlegen. Bei diesen Dateien handelt es sich um Datendateien mit der Dateiendung .DAT.
Name	Dies ist der Name der lizenzierten Funktion. Er beinhaltet eine Verknüpfung mit der Produktressource, in deren Lieferumfang er enthalten ist.
Lizenztyp	Es gibt drei Arten von Lizenzen:
	Evaluierung: Eine Lizenz mit einer festgelegten Testperiode von maximal 60 Tagen.
	Dieser Lizenztyp ist nur bis zum Erwerb einer zeitbasierten oder permanenten Lizenz verfügbar. Mit ihrem Erwerb ist die Testperiode sofort beendet.
	Hinweis: Eine Evaluierungslizenz ist nicht verlängerbar.
	Zeitbasiert: Eine Lizenz mit einem zeitbasierten Ablaufdatum.
	Permanent: Eine Lizenz, die nicht abläuft.
Restlaufzeit (Tage)	Zeigt die Anzahl der Tage an, die die Lizenz noch verwendet werden kann.
	Bei der Anzeige in Grün steht das Ablaufdatum noch bevor; bei der Anzeige in Rot ist die Lizenz abgelaufen.
Ablaufdatum	Zeigt das feststehende Ablaufdatum der Lizenz an.
	Dieses Datum wird nur für zeitbasierte Lizenzen angezeigt.
Kapazität	Bei einer kapazitätsbasierten Lizenz werden die verfügbare und die genutzte Kapazität durch eine Statuszeile angegeben.
	Verfügbar wenn:
	Diese Funktion ist verfügbar, wenn die Lizenz kapazitätsbasiert ist. Ist die Lizenz nicht kapazitätsbasiert, werden in der Kapazitätsspalte die Worte Nicht anwendbar angezeigt.

Elemente der Oberfläche	Beschreibung
Kapazitätsdetails	Bei einer kapazitätsbasierten Lizenz werden die verfügbare und die genutzte Kapazität im Verhältnis zueinander angegeben.
	Verfügbar wenn:
	Diese Funktion ist verfügbar, wenn die Lizenz kapazitätsbasiert ist. Ist die Lizenz nicht kapazitätsbasiert, werden in der Kapazitätsspalte die Worte Nicht anwendbar angezeigt.
Link "Serverbereitstellung"	Nachdem Sie eine Lizenz zu BSM hinzugefügt haben, müssen Sie die Applikation auf der Seite Serverbereitstellung aktivieren. Dabei müssen Sie auch überprüfen, ob die physischen Ressourcen Ihrer Bereitstellung für die hinzugefügte Applikation ausreichend sind. Weitere Informationen finden Sie unter "Serverbereitstellung" auf Seite
	67.

Tipps/Fehlerbehebung

Manuelle Lizenzaktivierung

Einige Lizenzen werden bei der Installation nicht automatisch aktiviert. Diese Lizenzen müssen zur besonderen Verwendung aktiviert werden und werden nicht ständig ausgeführt. Klicken Sie zum Aktivieren einer solchen Lizenz auf den Link **Serverbereitstellung** unten im Ausschnitt **Lizenzverwaltung**.

Installierte Lizenzen und Serverbereitstellung

Unter Umständen werden Sie feststellen, dass nicht alle von einer installierten Lizenz bereitgestellten Funktionen für Sie verfügbar sind. Dies kann an der Art und Weise liegen, wie diese Funktionen in BSM konfiguriert sind. Sie können diese Funktionen auf der BSM-Seite Serverbereitstellung konfigurieren, indem Sie auf den Link Serverbereitstellung unten im License Manager-Ausschnitt klicken oder das BSM-Dienstprogramm für die Setup- und Datenbankkonfiguration ausführen. Weitere Informationen finden Sie unter "Server Deployment and Setting Database Parameters" im BSM-Installationshandbuch.

Tipp: Stellen Sie sicher, dass die aktivierte Applikation stets mit den installierten Lizenzen übereinstimmt.

Kapitel 6

Serverbereitstellung

Dieser Abschnitt enthält Informationen zum Bestimmen und Konfigurieren der optimalen BSM-Serverbereitstellung.

Zugriff

Wählen Sie Admin > Plattform > Setup und Verwaltung > Serverbereitstellung aus.

Weitere Informationen

Übersicht über die Serverbereitstellung

BSM umfasst zahlreiche Applikationen und Untersysteme, die Hardware- und Softwareressourcen verbrauchen. Die verfügbaren Applikationen liefern Antworten zu einer Vielzahl von Verwendungsfällen, von denen nicht alle für jeden Benutzer erforderlich sind. Sie können die Bereitstellung der BSM-Server mit den Geschäftsanforderungen Ihres Unternehmens abstimmen.

Die Seite für die BSM-Serverbereitstellung bietet einen Mechanismus zur Bereitstellung nur derjenigen Applikationen, die für Ihr Unternehmen erforderlich sind. Sie können die erforderliche Hardware anhand der erforderlichen Kapazität für Ihre jeweilige Bereitstellung bestimmen. Die Funktion zur Serverbereitstellung zeigt genau an, welche Hardwarekapazität Sie für Ihre Bereitstellung benötigen. Des Weiteren bietet sie die Möglichkeit, nicht verwendete Ressourcen freizugeben.

Die Seite **Serverbereitstellung** steht im Setup- und Datenbank-Konfigurationsdienstprogramm, das einmal nach der Installation der BSM-Server ausgeführt wird, und im Bereich für die Plattformverwaltung der BSM-Benutzeroberfläche zur Verfügung. Die Seite bietet Ihnen die Möglichkeit, Ihre Bereitstellung zu aktualisieren, Applikationen nach Bedarf zu aktivieren oder zu deaktivieren und die Kapazitäten Ihrer Bereitstellung anzupassen, und zwar auch nach Abschluss der Installation und jedes Mal, wenn Sie an Ihrer BSM-Bereitstellung Änderungen durchgeführt haben. Sie können Applikationen nach Bedarf aktivieren oder deaktivieren, sodass für Ihre Bereitstellung keine unnötigen Ressourcen verbraucht werden.

Kapazitätsrechner

Sie können das Excel-Datenblatt des Kapazitätsrechners verwenden, um den Umfang und die Größe der BSM-Bereitstellung zu bestimmen. Sie geben die Informationen zum Umfang der Bereitstellung hinsichtlich der Anzahl der ausgeführten Applikationen, der Benutzer und der erwarteten Daten ein. Der Kapazitätsrechner berechnet dann den erforderlichen Speicherplatz, die CPU-Kerne, und er bestimmt die Größe Ihrer Bereitstellung. Wenn Sie Änderungen an Ihrer Bereitstellung durchführen, zum Beispiel durch Hinzufügen einer Lizenz für eine Applikation, verwenden Sie die Informationen des Kapazitätsrechners, um Ihre Hardwareanforderungen und Ihre Bereitstellungskonfiguration zu bestimmen.

Sie können eine mit Ihren Daten gespeicherte Datei direkt in die Seite **Serverbereitstellung** hochladen. Auf diese Weise können Sie die Felder der Seite automatisch mit den Daten füllen, die Sie in das Excel-Datenblatt eingegeben haben.

Wenn Sie die Datei bei der ersten BSM-Installation verwendet haben, verwenden Sie Ihre gespeicherte Version jedes Mal, wenn Sie Änderungen an Ihrer Bereitstellung durchführen. Wenn Sie keine eigene Version besitzen, können Sie die Datei im Ordner **Documentation** der Hauptinstallations-DVD von BSM verwenden oder die aktuelle Version von der Website mit den Produkthandbüchern von HP Software herunterladen (http://h20230.www2.hp.com/selfsolve/manuals).

Sie geben die Informationen entsprechend Ihrer Bereitstellung in das Datenblatt für den Bereitstellungsrechner der Datei ein. Geben Sie in die Spalten des Kapazitätsfragebogens Informationen wie Applikationen und Größe ein. Die Ausgabetabellen berechnen die Hardware- und Softwareanforderungen dann automatisch. Achten Sie darauf, die Datei an einem Speicherort zu speichern, von dem Sie sie in die Seite **Serverbereitstellung** hochladen können. Es wird empfohlen, jedes Mal eine Kopie der Datei zu erstellen, bevor Sie diese aktualisieren.

BSM-Plattformverwaltungshandbuch

Kapitel 6: Serverbereitstellung

Wenn Sie den Kapazitätsrechner aktualisieren, führen Sie keine Änderungen an Ihrer Bereitstellung durch. Sie verwenden den Kapazitätsrechner, um die Werte auf der Seite für die Serverbereitstellung zu aktualisieren. Nur wenn Sie Werte ändern und auf der Seite Serverbereitstellung auf Speichern klicken, wird Ihre Bereitstellung aktualisiert.

Aufgaben

Aktualisieren Ihrer BSM-Lizenzen, Applikationen oder des Bereitstellungsumfangs

In dieser Aufgabe wird beschrieben, wie Sie Änderungen an Ihrer Serverbereitstellung durchführen.

1. Verwenden des Kapazitätsrechners zum Bestimmen der erforderlichen Kapazität für Ihre Bereitstellungsänderung

Bevor Sie Änderungen an Ihrer BSM-Bereitstellung durchführen, zum Beispiel Hinzufügen einer Lizenz für eine Applikation, wird empfohlen, die Excel-Datei des Kapazitätsrechners zu verwenden, um zu bestimmen, ob Ihre aktuellen Server die erforderliche Kapazität bieten.

Es wird empfohlen, die gespeicherte Version des Kapazitätsrechners zu ändern, die vor der BSM-Installation verwendet wurde. Wenn Sie vor oder nach der Installation keine eigene Version des Kapazitätsrechners besitzen, können Sie im Ordner **Documentation** der Hauptinstallations-DVD von BSM auf eine Version zugreifen oder die aktuelle Version von der Website mit den Produkthandbüchern von HP Software herunterladen (http://h20230.www2.hp.com/selfsolve/manuals).

Achten Sie darauf, die Datei mit Ihren aktuellen Anforderungen an einem Speicherort zu speichern, von dem Sie sie in die Seite **Serverbereitstellung** hochladen können.

2. Hinzufügen einer neuen Lizenz – optional

Führen Sie diesen Schritt aus, wenn Sie Ihre Bereitstellung mit einer neuen Lizenz aktualisieren.

Wählen Sie Admin > Plattform > Setup und Verwaltung > Lizenzverwaltung aus.

Klicken Sie auf **Lizenz aus Datei hinzufügen**, um das Dialogfeld **Lizenz hinzufügen** zu öffnen, in dem Sie nach der entsprechenden .dat-Datei suchen können. Die Datei wird vom Clientcomputer auf den BSM-Server hochgeladen.

Klicken Sie unten in der Seite Lizenzverwaltung auf den Link Serverbereitstellung.

3. Aktualisieren der Bereitstellung auf der Seite "Serverbereitstellung"

Wählen Sie Admin > Plattform > Setup und Verwaltung > Serverbereitstellung aus.

■ Eingabetabelle. Klicken Sie auf die Schaltfläche Durchsuchen, um die gespeicherte Version der Excel-Datei Ihres Kapazitätsrechners hochzuladen. Wenn Sie eine Datei für den Upload auswählen, werden die in der Kapazitätsrechnerdatei eingegebenen Werte für Ihre Bereitstellung automatisch in die Seite Serverbereitstellung eingetragen.

Alternativ dazu können Sie die erforderlichen Informationen manuell in die obere Tabelle eingeben, jedoch wird die Verwendung des Kapazitätsrechners empfohlen, sodass dieser die Kapazität für Sie berechnet und den Umfang Ihrer Bereitstellung basierend auf den von Ihnen eingegebenen Werten bestimmt.

Serverstatustabelle. Vergewissern Sie sich in der unteren Tabelle, die den Status der Server angibt, dass der erforderliche Speicherplatz nicht größer ist als der ermittelte Speicherplatz auf den Servern. Wenn dies der Fall ist, müssen Sie entweder ausgewählte Applikationen entfernen, die Kapazitätsstufe ändern oder den Speicherplatz auf den Servern vergrößern.

4. BSM neu starten

Nachdem Sie auf der Seite **Serverbereitstellung** auf **Speichern** geklickt haben, müssen Sie BSM deaktivieren und aktivieren.

Wählen Sie Start > Programme > HP Business Service Management > Verwaltung > HP Business Service Management deaktivieren/HP Business Service Management aktivieren aus.

5. Ergebnisse

Wenn Sie Applikationen zu Ihrer Bereitstellung hinzugefügt haben, werden diese nun in den BSM-Menüs angezeigt. Wenn Sie beispielsweise die Applikation System Availability Management aktiviert haben, finden Sie die Menüoption jetzt sowohl im Menü **Admin** als auch im Menü **Applikationen**.

Wenn Sie hingegen Applikationen aus Ihrer Bereitstellung entfernt haben, sind diese in den entsprechenden Menüs nicht mehr verfügbar.

Beschreibung der Benutzeroberfläche

Seite "Serverbereitstellung"

Diese Seite bietet Ihnen die Möglichkeit, Ihre Bereitstellung zu aktualisieren und festzustellen, ob Ihre Hardware die Speicheranforderungen erfüllt, die sich aus durchgeführten Änderungen ergeben. Nachdem Sie die Änderungen an dieser Seite gespeichert haben, muss BSM neu gestartet werden, damit die Änderungen wirksam werden.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der Oberfläche	Beschreibung
<kapazitätsrechner- Dateiname></kapazitätsrechner- 	Klicken Sie auf die Schaltfläche Durchsuchen , um die gespeicherte Version der Excel-Datei Ihres Kapazitätsrechners zu lokalisieren und hochzuladen.
	Wenn Sie noch keine Werte in einen Kapazitätsrechner eingegeben haben, wird dies empfohlen, bevor Sie Änderungen an dieser Seite vornehmen. Sie finden eine Kapazitätsrechnerdatei im Ordner Documentation der Hauptinstallations-DVD von BSM. Alternativ dazu können Sie die aktuelle Version von der Website mit den Produkthandbüchern von HP Software (http://h20230.www2.hp.com/selfsolve/manuals) herunterladen.

Elemente der Oberfläche	Beschreibung
<kapazitätstabelle></kapazitätstabelle>	In der oberen Tabelle der Seite werden aktuelle Informationen zur Bereitstellung und zu Applikationen angezeigt. Wenn Sie eine Kapazitätsrechnerdatei hochladen, wird diese automatisch mit den Informationen im Kapazitätsrechner aktualisiert.
	Sie können die Kapazitätsstufe Ihrer Bereitstellung ändern für:
	Users. Anzahl der angemeldeten Benutzer.
	Model. Die Anzahl der Konfigurationselemente in Ihrem Modell legt fest, ob das Modell klein, mittelgroß, groß oder besonders groß ist.
	Metric Data. Die Anzahl der überwachten Applikationen, Transaktionen, Speicherorte und Hosts legt fest, ob die Messdatenbelastung gering, mittelgroß oder groß ist.
	Sie können Applikationen und Funktionen auch aktivieren/deaktivieren und Ihre Kapazitätsstufe ändern.
	End User Management
	TransactionVision
	Diagnostics
	Business Process Insight
	• OMi.
	■ TBEC. Die zum Verbinden von Ereignissen mit OMi verwendete topologiebasierte Ereigniskorrelation (Topology-Based Event Correlation).
	■ Custom Rules. Für die Ereignisverarbeitung verwendet. Beispielsweise, um das Ereignis-Enrichment oder um benutzerdefinierte Aktionen im Ereignis-Browser anzupassen. Wenn Sie nicht sicher sind, ob Benutzer benutzerdefinierte Regeln verwenden werden, aktivieren Sie diese Funktion, wenn OMi aktiviert ist.
	System Availability Management
	Service Level Management
	Service Health Analyzer
	Baselining
	Nachdem Sie auf Speichern geklickt und BSM neu gestartet haben:
	Wenn Sie eine zuvor nicht ausgewählte Applikation ausgewählt haben, steht diese im BSM-Menü und in allen anderen entsprechenden Menüs zur Verfügung.
	Wenn Sie eine zuvor ausgewählte Applikation deaktivieren, ist die Applikation nicht mehr zugreifbar.

Elemente der Oberfläche	Beschreibung
<serverstatustabelle></serverstatustabelle>	In der unteren Tabelle werden alle Server aufgeführt, die BSM ausführen, einschließlich:
	Status. Gibt an, ob der Computer ausgeführt wird.
	Abgestimmt. Gibt an, ob dieser Computer mit der aktuellen Bereitstellungskonfiguration abgestimmt ist. Er ist nur abgestimmt, wenn BSM auf diesem Computer neu gestartet wurde, nachdem Änderungen durchgeführt wurden. Wenn BSM auf diesem Computer nicht neu gestartet wurde, nachdem auf dieser Seite Konfigurationsänderungen durchgeführt wurden, ist der Computer nicht abgestimmt.
	Computer. Der Name des Servers.
	Installiert. Welcher Typ von BSM-Server auf dem Computer installiert ist bzw. Gateway- oder Datenverarbeitung oder beides (typische Installation, wenn Gateway- und Datenverarbeitung auf demselben Computer erfolgen).
	Aktiviert. Welcher Typ von BSM-Server aktuell auf dem Computer, Gateway oder Datenverarbeitungsserver aktiviert ist.
	Entdeckt. Der auf dem Computer ermittelte freie Speicherplatz.
	Erforderlich. Der erforderliche Speicherplatz für jeden Servertyp basierend auf den Applikationen und Kapazitätsstufen, die in der oberen Tabelle aufgelistet sind.
	Wenn der erforderliche Speicherplatz größer ist als der Speicherplatz des erkannten Speicherplatzes, müssen Sie eine der folgenden Aktionen durchführen:
	 Ändern Sie die Kapazitätsstufen für Ihre Bereitstellung, zum Beispiel durch Deaktivieren von Applikationen aus der Liste der verfügbaren Applikationen.
	 Fügen Sie Speicherplatz zu den physischen Computern hinzu und versuchen Sie, Ihre Bereitstellung erneut zu aktualisieren.
Deaktivieren von Maschine	Link zur Seite, auf der Sie Servercomputer deaktivieren können, deren installierte BSM-Komponenten für den fortgesetzten Betrieb des Systems nicht mehr erforderlich sind. Vergewissern Sie sich vor dem Deaktivieren eines Computers, dass dieser nicht mehr zu einem Teil der BSM-Serverarchitektur gehört, der für den Betrieb erforderlich ist. Um einen Computer, der an dieser Stelle deaktiviert wurde, erneut zu aktivieren, müssen Sie auf dem Computer das Dienstprogramm für die Setup- und Datenbankkonfiguration ausführen.

Fehlerbehebung und Einschränkungen

Fehlerbehebung

- Wenn eine Applikation auf der BSM-Oberfläche nicht angezeigt wird, aktivieren Sie sie über die Seite **Serverbereitstellung**.
- Wenn eine Applikation aktiviert wurde, aber dennoch nicht auf der BSM-Oberfläche angezeigt wird, starten Sie alle BSM-Server neu.
- Wenn eine Applikation im Kapazitätsrechner ausgewählt, aber nicht in die Seite Serverbereitstellung importiert wurde, überprüfen Sie, ob Sie über eine gültige Lizenz für die Applikation verfügen.

Kapitel 7

Datenbankverwaltung

Diese Seiten werden von HP Operations verwaltet und die Schnittstelle ist ausgeblendet.

Sie können die Datenbanken warten und verwalten, die von BSM zum Speichern der Überwachungsdaten verwendet werden. Sie können Profildatenbanken direkt über die Plattformverwaltung erstellen und verwalten. Mithilfe des Partitions- und Purging Managers können Sie die Daten in der Datenbank periodisch Ihren Anforderungen entsprechend löschen.

Bevor Sie die Überwachungsumgebung konfigurieren, müssen Sie die Datenbank konfigurieren, in der die Überwachungsdaten gespeichert werden sollen. In einer Profildatenbank können Daten für verschiedene Typen von Datenquellen gespeichert werden (Business Process Monitor, SiteScope). Sie können entweder eine Datenbank für alle Daten erstellen oder spezielle Datenbanken erstellen (beispielsweise für jeden Datentyp).

Hinweis: Der Begriff **Datenbank** bezieht sich auf eine Datenbank in Microsoft SQL Server. Der Begriff **Benutzerschema** bezieht sich auf eine Datenbank in Oracle Server.

BSM unterstützt zwei Datenbanktypen:

- Microsoft SQL Server. Diese Datenbank wird nur auf Windows-Betriebssystemen ausgeführt. Weitere Informationen zum Konfigurieren einer Datenbank unter Microsoft SQL Server finden Sie unter "Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server" auf Seite 82.
- Oracle Server. Diese Datenbank wird auf allen von BSM unterstützten Betriebssystemen ausgeführt. Eine Datenbank unter Oracle Server wird als Benutzerschema bezeichnet. Weitere Informationen zum Konfigurieren eines Benutzerschemas unter Oracle Server finden Sie unter "So konfigurieren Sie ein Benutzerschema auf einem Oracle-Server" auf Seite 83.

Die Seite der Profildatenbankverwaltung, auf die Sie über **Admin > Plattform > Setup und Verwaltung** zugreifen können, ermöglicht Ihnen das Durchführen der folgenden Datenbankverwaltungsaufgaben.

- Erstellen einer neuen Datenbank. BSM erstellt automatisch eine neue Datenbank und fügt dieser Profiltabellen hinzu.
- **Zuweisen einer Standard-Profildatenbank**. Sie müssen eine Standard-Profildatenbank zuweisen, damit BSM die folgenden Datentypen erfassen kann:
- Service Level Management-Daten
- SOA-Daten
- Daten aus Real User Monitor und Business Process Monitor
- Daten, die in Service Health verwendet werden
- Diagnostics-Daten

Persistente benutzerdefinierte Daten

Hinweis: Die erste Datenbank, die zur Seite **Datenbankverwaltung** hinzugefügt wird, wird automatisch als Standard-Profildatenbank angesehen.

- Fügen Sie Profiltabellen zu einer bestehenden, leeren Datenbank hinzu. BSM stellt eine Verbindung zu einer leeren Datenbank her, die manuell auf Ihrem Datenbankserver erstellt wurde, und fügt ihr Profiltabellen hinzu.
- Stellen Sie eine Verbindung zu einer bestehenden Datenbank her, der Profiltabellen hinzugefügt wurden. BSM stellt eine Verbindung zu einer Profildatenbank her, die entweder manuell erstellt und mit Profiltabellen bestückt oder vorher in der Plattformverwaltung definiert wurde.

Um Profildatenbanken unter Microsoft SQL Server oder Oracle Server für die spezielle Umgebung Ihrer Organisation bereitzustellen, folgen Sie den Anleitungen unter "Introduction to Preparing the Database Environment" im BSM Database Guide. Es wird empfohlen, die entsprechenden Abschnitte im BSM Database Guide zu lesen, bevor die Verwaltungsaufgaben für die Profildatenbank durchgeführt werden.

Hinweis: Daten-Collectoren von BSM sammeln Leistungsdaten und übertragen sie an den Gateway-Server, der die Daten mithilfe des Lademechanismus an die Profildatenbanken übermittelt. Die Daten werden zusammen mit einem Zeitstempel in die Datenbank eingefügt. BSM-Komponenten synchronisieren ihre Zeituhren mit der Zeituhr des Datenbankservers, auf dem sich die BSM-Datenbank befindet. Auf diese Weise entspricht der Zeitstempel der in die Datenbank eingefügten Messdaten der Uhr des Datenbankservers zum Zeitpunkt der Datenerfassung.

Partitionieren und Löschen von historischen Daten aus Datenbanken

Hinweis: Diese Seiten werden von HP Operations verwaltet und die Schnittstelle ist ausgeblendet.

Sie verwenden den Partitions- und Purging Manager, um die Plattform anzuweisen, die historischen Daten automatisch zu partitionieren, sodass sie später aus den Profil- und SHP-Datenbanken entfernt werden können.

Die Datensammlungstabellen in den Profil- und SHP-Datenbanken können sehr groß werden. Im Lauf der Zeit kann sich das negativ auf die Systemleistung auswirken.

Mithilfe des Partitions- und Purging Managers von BSM werden Tabellen mit schnell anwachsenden Datenmengen in festgelegten Intervallen geteilt. Sobald die definierte Zeitspanne verstrichen ist, kann auf Daten in einer Partition nicht mehr zugegriffen werden, um sie in BSM-Reports zu verwenden. Nach weniger als zwei Stunden wird die Partition aus der Profildatenbank gelöscht.

Der Partitions- und Purging Manager wird für jede Profil- oder SHP-Datenbank aktiviert und führt das Partitionieren und spätere Löschen von historischen Daten gemäß der Zeitdauer aus, die für die Datenbanktabelle aufgeführt ist. Die Größe der einzelnen Partitionen richtet sich nach dem EPM-Wert (Ereignisse pro Minute), der auf der Seite **Purging Manager** angezeigt wird. Die standardmäßigen EPM-Werte sind entsprechend der jeweiligen Ebene der angegebenen Datentabelle voreingestellt. Optional können Sie den EPM-Wert wie folgt einstellen:

- Wenn die Datenpartitionen zu groß sind (mehr als 1 Million Zeilen), erhöhen Sie den EPM-Wert, um häufiger neue Partitionen zu erstellen.
- Wenn die Datenpartitionen zu klein sind (deutlich weniger als 1 Million Zeilen), verkleinern Sie den EPM-Wert, um seltener neue Partitionen zu erstellen.

Hinweis: Bei der vom Partitions- und Purging Manager verwendeten
Partitionierungsmethode handelt es sich um die systemeigene Partitionierung. (Informationen finden Sie in der entsprechenden Matrix für die Datenbankunterstützung in den Versionshinweisen für die SQL SERVER- und Oracle Enterprise-Editionen, die in dieser Version unterstützt werden). In Oracle-Datenbanken sollte die Option Oracle-Partitionierung aktiviert sein. Steht die Option Oracle-Partitionierung nicht zur Verfügung, werden vom Partitions- und Purging Manager keine Daten partitioniert oder gelöscht. Fehler bei der Partitionierung oder beim Löschen können zu größeren Leistungseinbußen führen.

Sie haben auch die Möglichkeit, den Partitions- und Purging Manager für das Festlegen einer bestimmten Zeitdauer pro Tabelle für das Entfernen von historischen Daten einzusetzen. Details zur Benutzeroberfläche für diese Aufgabe finden Sie unter "Seite "Purging Manager" auf Seite 98.

Der Partitions- und Purging Manager wird stündlich ausgeführt und überprüft, ob eine neue Datenpartition erstellt und Daten gelöscht werden müssen, die den pro Tabelle festgelegten Wert für die Speicherdauer überschreiten.

Hinweis: Standardmäßig löscht der Partitions- und Purging Manager keine Daten. Überprüfen Sie die Richtlinien für das Löschen der Datenstichproben mithilfe des Verwaltungsbildschirms des Partitions- und Purging Managers.

Richtlinien und Tipps zur Verwendung des Partitions- und Purging Managers finden Sie unter "Richtlinien und Tipps zur Verwendung des Partitions- und Purging Manager" unten.

Die Seite **Purging Manager** ist in folgende Bereiche unterteilt:

• Vorlage und mehrere Datenbanken. Wird verwendet, um die Vorlagenkonfigurationen und die Datenbankkonfigurationen in mehreren Datenbanken zu ändern. Alle Datenbanken, die später hinzugefügt werden, übernehmen die Vorlagenkonfigurationen.

Nachdem Sie Änderungen vorgenommen haben, werden auf der Registerkarte **Vorlage und mehrere Datenbanken** weiterhin die Vorlageneinstellungen angezeigt, auch wenn Sie keine Änderungen an der Vorlage vorgenommen haben, sondern die Einstellungen für bestimmte Datenbanken manuell geändert haben. Nachdem diese manuellen Änderungen angewendet wurden, werden die angezeigten Einstellungen auf die Vorlageneinstellungen zurückgesetzt. Um die Einstellungen zu sehen, die Sie für bestimmte Datenbanken geändert haben, navigieren Sie zur Registerkarte **Datenbankspezifisch** und wählen die entsprechende Datenbank aus.

• **Datenbankspezifisch.** Zeigt die Konfigurationen für die angegebene Datenbank an.

Weitere Informationen zu zusätzlichen Partitionierungs- und Löschfunktionen finden Sie unter "Data Partitioning and Purging" im BSM Database Guide.

Richtlinien und Tipps zur Verwendung des Partitions- und Purging Manager

Dieser Abschnitt enthält Richtlinien und Tipps zur Verwendung des Partitions- und Purging Manager.

 Vor dem Bereinigen führt der Partitions- und Purging Manager eine zusätzliche Prüfung durch, um zu gewährleisten, dass Rohdaten erst gelöscht werden, nachdem diese aggregiert und an BSM gemeldet wurden.

Wenn ein bestimmter Datensatz für die Bereinigung geplant ist, die Rohdaten jedoch noch nicht aggregiert wurden, führt der Partitions- und Purging Manager die Datenbereinigung nicht wie geplant durch. Der Partitions- und Purging Manager bereinigt die Daten bei der nächsten stündlichen Ausführung nur dann, wenn die Daten aggregiert wurden.

Wenn die Datenbereinigung beispielsweise am Sonntag um 8:00 Uhr geplant war, das Aggregieren der Daten jedoch nur am Sonntag um 10:00 Uhr erfolgt, prüft der Partitions- und Purging Manager die Daten um 8:00 Uhr, er bereinigt sie jedoch nicht, sondern führt die Bereinigung automatisch bei der nächsten stündlichen Ausführung nach Sonntag 10:00 Uhr durch, nachdem die Daten aggregiert wurden.

- Wenn Sie feststellen, dass Daten nicht entsprechend den im Partitions- und Purging Manager festgelegten Zeitplänen bereinigt wurden und Ihre Profildatenbanken zu groß werden, vergewissern Sie sich, dass der Aggregator ordnungsgemäß ausgeführt wird, und zeigen Sie die Protokolle des Partitions- und Purging Managers an. Sie finden diese auf dem Datenverarbeitungsserver unter < HPBSM-Serverstammverzeichnis>\log\pmanager.log.
- Verwenden Sie zum Definieren der Bereinigung Ihrer Rohdaten und aggregierten Daten das

folgende Prinzip: Der Zeitraum, für den Rohdaten gespeichert werden, muss kürzer sein als der Zeitraum, für den Ein-Stunden-Chunks mit aggregierten Daten gespeichert werden, und dieser Zeitraum ist kürzer als der Zeitraum, für den Ein-Tages-Chunks mit aggregierten Daten gespeichert werden.

 In der Registerkarte Vorlage und mehrere Datenbanken durchgeführte Änderungen wirken sich auf die Standardzeiträume für neue Profildatenbanken aus, die im System erstellt werden. Wenn eine neue Profildatenbank erstellt wird, nachdem Sie in der Registerkarte Vorlage und mehrere Datenbanken Änderungen an den Zeiträumen durchgeführt haben, werden die Daten in den Tabellen der neuen Profildatenbank für die Zeiträume gespeichert, die nun unter Vorlage und mehrere Datenbanken für alle Tabellen aufgelistet sind.

Entfernen unerwünschter Daten aus der Profildatenbank

Hinweis: Dieser Abschnitt ist für HP Software-as-a-Service-Kunden nicht relevant.

Mithilfe des Dienstprogramms für Datenmarkierung können BSM-Benutzer mit Superuser-Sicherheitsberechtigungen bestimmte Gruppen von Daten in Profildatenbanken als unerwünscht kennzeichnen. Dadurch werden unerwünschte Daten herausgefiltert und BSM kann nur die relevantesten Daten für den angegebenen Zeitraum anzeigen. Nachdem das Dienstprogramm die angegebenen Daten als unerwünscht gekennzeichnet hat, werden die verbleibenden Rohdaten von BSM automatisch für den ausgewählten Zeitraum neu aggregiert.

Das Dienstprogramm für Datenmarkierung ermöglicht auch das Entfernen unerwünschter Business Process Monitor- und SiteScope-Daten.

Wenn Sie eine bestimmte Gruppe Daten aus einem bestimmten Zeitraum als unerwünscht gekennzeichnet haben, führt BSM den Aggregationsprozess für die über den entsprechenden Zeitraum verbleibenden Rohdaten erneut aus, sodass die markierten Daten nicht angezeigt werden. Mit dem Dienstprogramm für Datenmarkierung können Sie eine definierte Gruppe von Daten auch erneut aggregieren, ohne diese als nicht verfügbar zu kennzeichnen. Details finden Sie unter "Aktivieren der Option "Nur Neuaggregierung ausführen"" auf Seite 87.

BSM installiert das Dienstprogramm für Datenmarkierung während der Installation auf dem Gateway-Server. Daten werden vom Dienstprogramm für Datenmarkierung nicht physikalisch aus der Datenbank entfernt, sondern in Reports und Applikationen unbrauchbar gemacht, indem ihnen der Datenmarkierungsstatus **nicht verfügbar** zugewiesen wird.

Das Dienstprogramm für Datenmarkierung unterstützt Partitionen. So können Benutzer, die Partition und Purging Manager ausführen, auch das Dienstprogramm für Datenmarkierung verwenden.

Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server

In dieser Aufgabe wird beschrieben, wie Sie eine oder mehrere Profildatenbanken auf einem Microsoft SQL-Server konfigurieren.

1. Voraussetzungen

Stellen Sie zunächst sicher, dass Sie über folgende Verbindungsparameter für den Datenbankserver verfügen:

a. **Servername.** Der Name des Computers, auf dem MS SQL Server installiert ist. Wenn Sie eine Verbindung mit einer nicht standardmäßigen Microsoft SQL Server-Instanz im dynamischen Modus herstellen, geben Sie den Servernamen im folgenden Format ein:

<Hostname>\<Instanzname>

- Den Benutzernamen und das Kennwort für die Datenbank. Der Benutzername und das Kennwort eines Benutzers mit Administratorrechten auf einem Microsoft SQL-Server (falls die SQL Server-Authentifzierung verwendet wird).
- c. **Server-Port.** Der TCP/IP-Port des Microsoft SQL-Servers. Der Standardport 1433 wird automatisch angezeigt. Sie müssen die Portnummer in einem der folgenden Fälle ändern:
 - Die Microsoft SQL Server-Standardinstanz h
 ört einen anderen Port ab als 1433.
 - Sie stellen eine Verbindung zu einer nicht standardmäßigen Microsoft SQL Server-Instanz im statischen Modus her.
 - Sie stellen eine Verbindung zu einer nicht standardmäßigen Microsoft SQL Server-Instanz im dynamischen Modus her. Geben Sie in diesem Fall Portnummer 1434 ein.

Fragen Sie bei Bedarf den Datenbankadministrator in Ihrem Unternehmen nach diesen Daten.

2. Hinzufügen einer Datenbank

- a. Rufen Sie die Seite Datenbankverwaltung über Admin > Plattform > Setup und Verwaltung > Profildatenbanken verwalten auf.
- b. Wählen Sie MS SQL aus der Dropdownliste aus, und klicken Sie auf Hinzufügen.
- c. Geben Sie die Parameter der Datenbank auf der Seite Profildatenbank-Eigenschaften -MS SQL Server ein. Informationen zur Benutzeroberfläche finden Sie unter "Seite "Profildatenbank-Eigenschaften - MS SQL Server"" auf Seite 93.

So konfigurieren Sie ein Benutzerschema auf einem Oracle-Server

In dieser Aufgabe wird beschrieben, wie Sie ein oder mehr Profilbenutzerschemata auf Ihrem Oracle-Server konfigurieren.

1. Voraussetzungen

Stellen Sie zunächst Folgendes sicher:

- a. Sie haben einen dedizierten Standard-Tablespace für Profilbenutzerschemata (und einen dedizierten temporären Tablespace, falls erforderlich) erstellt.
- b. Sie verwenden eine sichere Netzwerkverbindung (für den Fall, dass keine Datenbankadministrator-Verbindungsparameter über eine nicht sichere Netzwerkverbindung übertragen werden sollen). Falls gar keine Datenbankadministrator-Verbindungsparameter über den Webbrowser übertragen werden sollen, können Sie die Profilbenutzerschemata manuell erstellen und dann über die Seite **Datenbankverwaltung** eine Verbindung zu ihnen herstellen.

2. Zusammenstellen von Verbindungsparametern

Stellen Sie sicher, dass Sie über folgende Verbindungsparameter für den Datenbankserver verfügen:

- a. Hostname. Der Name des Computers, auf dem der Oracle-Server installiert ist.
- b. **SID.** Der Oracle-Instanzname, mit dem die verwendete Oracle-Datenbankinstanz eindeutig identifiziert wird (falls abweichend vom Standardwert **orcl**).
- c. **Port.** Der Oracle-Listenerport, falls abweichend vom Standardwert **1521**.
- d. Benutzername und Kennwort für den Datenbankadministrator. Name und Kennwort eines Benutzers mit Administratorberechtigungen für den Oracle-Server. Mit diesen Parametern wird der BSM-Benutzer erstellt, und sie werden nicht im System gespeichert.
- e. **Standard-Tablespace**. Der Name des dedizierten Standard-Tablespace, den Sie für Profilbenutzerschemata erstellt haben (Details zum Erstellen eines dedizierten Tablespace finden Sie unter "Overview of Oracle Server Deployment" im BSM Database Guide). Wenn Sie keinen dedizierten Standard-Tablespace erstellt haben und diesen auch nicht benötigen, können Sie einen alternativen Tablespace angeben. Der standardmäßige Oracle-Tablespace lautet **users**.
- f. **Temporärer Tablespace.** Der Name des dedizierten temporären Tablespace, den Sie für die Profilbenutzerschemata erstellt haben. Wenn Sie keinen dedizierten temporären Tablespace erstellt haben und diesen auch nicht benötigen, können Sie einen alternativen Tablespace angeben, Der standardmäßige temporäre Oracle-Tablespace ist **temp**.

Fragen Sie bei Bedarf den Datenbankadministrator in Ihrem Unternehmen nach diesen Daten.

3. Hinzufügen eines Benutzerschemas

 a. Rufen Sie die Seite Datenbankverwaltung über Admin > Plattform > Setup und Verwaltung > Profildatenbanken verwalten auf.

- b. Wählen Sie Oracle aus der Dropdownliste aus, und klicken Sie auf Hinzufügen.
- c. Geben Sie die Parameter des Benutzerschemas auf der Seite Profildatenbank-Eigenschaften - Oracle Server ein. Informationen zur Benutzeroberfläche finden Sie unter "Seite "Profilbenutzerschema-Eigenschaften – Oracle Server" auf Seite 95.

Wenn Ihre Profildatenbank Teil von Oracle Real Application Cluster (RAC) ist, finden Sie weitere Informationen unter "Support for Oracle Real Application Cluster" im Handbuch BSM Database Guide.

Verwenden des Purging Manager

In dieser Aufgabe wird beschrieben, wie Sie den Purging Manager verwenden.

Diese Aufgabe umfasst die folgenden Themen:

- "Voraussetzungen"
- "Ändern der Datenbankvorlage"
- "Ändern der Einstellungen für mehrere Datenbanken"
- "Ändern der Einstellungen für einzelne Datenbanken"

1. Voraussetzungen

Vergewissern Sie sich, dass mindestens eine Profildatenbank im BSM-System konfiguriert ist. Weitere Informationen zum Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server finden Sie unter "Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server" auf Seite 82.

Weitere Informationen zum Konfigurieren eines Benutzerschemas auf einem Oracle-Server finden Sie unter "So konfigurieren Sie ein Benutzerschema auf einem Oracle-Server" auf Seite 83.

2. Ändern der Datenbankvorlage

Gehen Sie wie folgt vor, um Einstellungen für die Datenbankvorlage zu ändern:

- a. Wechseln Sie auf der Seite Purging Manager zur Registerkarte Vorlage und mehrere Datenbanken.
- b. Aktivieren Sie das Kontrollkästchen neben der zu ändernden Einstellung. Sie können mehrere Kontrollkästchen gleichzeitig aktivieren.
- c. Nehmen Sie die entsprechenden Änderungen an den Einstellungen in den Feldern **Daten** beibehalten für und Ändern in EPM vor und klicken Sie auf Übernehmen.
- d. Klicken Sie auf den Link Anwenden auf und stellen Sie sicher, dass die entsprechende Vorlage (Enterprise für Datenbanken mit systemeigener Partitionierung und Standard für Datenbanken mit Ansichtspartitionierung) ausgewählt ist.
- e. Klicken Sie auf **OK**, um die Änderungen an der Vorlage zu übernehmen.

Hinweis: Nachdem Sie Änderungen vorgenommen haben, werden auf der Registerkarte Vorlage und mehrere Datenbanken weiterhin die Vorlageneinstellungen angezeigt, auch wenn Sie keine Änderungen an der Vorlage vorgenommen haben, sondern die Einstellungen für bestimmte Datenbanken manuell geändert haben. Nachdem diese manuellen Änderungen angewendet wurden, werden die angezeigten Einstellungen auf die Vorlageneinstellungen zurückgesetzt. Um die Einstellungen zu sehen, die Sie für bestimmte Datenbanken geändert haben, navigieren Sie zur Registerkarte Datenbankspezifisch und wählen die entsprechende Datenbank aus.

3. Ändern der Einstellungen für mehrere Datenbanken

Gehen Sie wie folgt vor, um Einstellungen für mehrere Datenbanken gleichzeitig zu ändern:

- a. Wechseln Sie auf der Seite **Purging Manager** zur Registerkarte **Vorlage und mehrere Datenbanken**.
- b. Aktivieren Sie das Kontrollkästchen neben der zu ändernden Einstellung. Sie können mehrere Kontrollkästchen gleichzeitig aktivieren.
- c. Nehmen Sie die entsprechenden Änderungen an den Einstellungen in den Feldern **Daten** beibehalten für und Ändern in EPM vor und klicken Sie auf Übernehmen.
- d. Klicken Sie auf den Link **Übernehmen** und stellen Sie sicher, dass die entsprechenden Datenbanken ausgewählt sind. Deaktivieren Sie das Kontrollkästchen neben der Vorlage, wenn Ihre Änderungen nicht auf die Vorlage angewendet werden sollen.
- e. Klicken Sie auf **OK**, um die Änderungen in den ausgewählten Datenbanken zu registrieren.

Hinweis: Änderungen an den Datenbanken werden nur auf der Registerkarte **Datenbankspezifisch** angezeigt, nachdem die entsprechende Datenbank im Dropdown **Profildatenbank auswählen** ausgewählt wurde.

4. Ändern der Einstellungen für einzelne Datenbanken

Gehen Sie wie folgt vor, um Einstellungen für einzelne Datenbanken zu ändern:

- a. Wechseln Sie auf der Seite **Purging Manager** zur Registerkarte **Datenbankspezifisch**.
- b. Aktivieren Sie das Kontrollkästchen neben den zu ändernden Einstellungen.
- c. Wählen Sie die Profildatenbank, auf die Sie Ihre Änderungen anwenden wollen, im Feld **Profildatenbank auswählen** aus.
- d. Nehmen Sie die entsprechenden Änderungen an den Einstellungen in den Feldern **Daten** beibehalten für und Ändern in EPM vor und klicken Sie auf Übernehmen.

Aktivieren der Option "Nur Neuaggregierung ausführen"

Standardmäßig wird die Datenmarkierung immer vom Dienstprogramm für Datenmarkierung ausgeführt, gefolgt von dem Neuaggregierungsprozess. Falls erforderlich, können Sie eine Funktion aktivieren, um BSM anzuweisen, nur die Neuaggregierung auszuführen. Dies kann erforderlich sein, wenn die Datenmarkierung erfolgreich durchgeführt wurde, die Neuaggregierung jedoch fehlgeschlagen ist. Alternativ können Sie diese Funktion verwenden, um einen Satz definierter Daten neu zu aggregieren, ohne ihn als nicht verfügbar zu markieren (z. B., wenn Daten aggregiert wurden und spät eintreffende Daten in die Rohdatentabellen der Datenbank eingefügt wurden).

So aktivieren Sie die Option "Nur Neuaggregierung ausführen":

- Öffnen Sie die Datei <Gateway-Server-Stammverzeichnis>\tools\dataMarking\dataMarking.bat in einem Texteditor.
- Fügen Sie die Eigenschaft DadvanceMode mit dem Wert true zur Zeile SET SERVICE_ MANAGER_OPTS hinzu. Beispiel:

```
SET SERVICE_MANAGER_OPTS=-DhacProcessName=%PROCESS_NAME % -
DadvancedMode=true
```

3. Speichern Sie die Datei. Beim nächsten Öffnen des Dienstprogramms zur Datenmarkierung wird die Schaltfläche **Erweitert** angezeigt.

Nachdem Sie diese Funktion aktiviert haben, können Sie das Dienstprogramm zur Datenmarkierung anweisen, den Neuaggregierungsprozess für Daten nur auszuführen, wenn auf die Schaltfläche **Start** geklickt wird.

So führen Sie die Option "Nur Neuaggregierung ausführen" für Daten aus:

- 1. Definieren Sie die Daten für die Neuaggregierung, wie unter "Entfernen unerwünschter Daten aus der Profildatenbank" auf Seite 81 beschrieben.
- Klicken Sie auf die Schaltfläche Erweitert. Das Fenster Erweitert wird angezeigt.
- 3. Aktivieren Sie das Kontrollkästchen Nur Neuaggregierung ausführen.
- 4. Wählen Sie die Datenkategorien für die Neuaggregierung aus und klicken Sie auf **OK**, um die Auswahl zu bestätigen.
- Klicken Sie auf Starten.

Festlegen der Ereignisse pro Minute für das Eintreffen von Daten in BSM

Sie können die Menge der Daten festlegen, die in BSM eintreffen. Sie geben diesen Wert in das Feld **Ändern in EPM** oben auf der Seite **Purging Manager** ein.

So legen Sie die Ereignisse pro Minute für den ausgewählten Datentyp fest:

- Öffnen Sie die Datei unter:
 - <Gateway-Server-Stammverzeichnis>\log\db_loader\LoaderStatistics.log
- 2. Suchen Sie die folgende Zeile in der ausgewählten Datenstichprobe:

Statistics for: DB-Name: <Datenbankname> Sample: <Stichprobenname> - (collected over <Zeitraum>):

3. Suchen Sie die folgende Zeile im Statistikabschnitt der ausgewählten Datenstichprobe:

Insert to DB EPS (MainFlow)

Die ausgewählte Zahl steht für die Ereignisse pro Sekunde. Multiplizieren Sie die Zahl mit 60, um die Ereignisse pro Minute zu erhalten.

Um zu ermitteln, zu welcher Datentabelle im Partitions-Manager die Stichprobe gehört, folgen Sie den Anweisungen unter "Generic Reporting Engine API" im BSM Extensibility Guide. Die Ergebnisliste zeigt die Datentabelle in Klammern neben dem Namen des Beispiels an. Sie können anschließend den EPM-Wert für die richtige Tabelle angeben.

Liegen mehrere Gateway-Server vor, müssen Sie die Werte summieren, die Sie von den einzelnen Servern erhalten.

Anpassen der Konfigurationen von Dienstprogrammen für Datenmarkierungen

Sie können die maximale Dauer für die Ausführung jeder Datenmarkierung festlegen. Der aktuelle Standardwert beträgt 6 Stunden und 59 Minuten.

So konfigurieren Sie die maximale Dauer:

- Öffnen Sie die Datei <Gateway-Server-Stammverzeichnis>\tools\dataMarking\dataMarking.bat in einem Texteditor.
- 2. Fügen Sie die Eigenschaft **DmaximumDuration** mit einem Wert für die maximale Dauer in Stunden zur Zeile **SET SERVICE_MANAGER_OPTS** hinzu.

Es folgt ein Beispiel, in dem die maximale Dauer auf 23 Stunden und 59 Minuten geändert wird:

```
SET SERVICE_MANAGER_OPTS=
-DhacProcessName=%PROCESS_NAME%
-Dlog.folder.path.output=%PROCESS NAME% -DmaximumDuration=24
```

3. Speichern und schließen Sie die Datei.

Benutzeroberfläche der Datenbankverwaltung

Dieser Abschnitt umfasst die folgenden Themen:

- "Seite "Datenbankverwaltung""
- "Seite "Dienstprogramm für Datenmarkierung""
- "Seite "Profildatenbank-Eigenschaften MS SQL Server""
- "Seite "Profilbenutzerschema-Eigenschaften Oracle Server""
- "Seite "Purging Manager""

Seite "Datenbankverwaltung"

Auf dieser Seite können Sie die Datenbanken warten und verwalten, die von BSM zum Speichern der Überwachungsdaten verwendet werden.

Zugriff	Wählen Sie Admin > Plattform > Setup und Verwaltung > Profildatenbanken verwalten aus.
Wichtiger Hinweis	Die erste Datenbank, die zur Seite Datenbankverwaltung hinzugefügt wird, wird automatisch als Standard-Profildatenbank angesehen.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
×	Löst die Verbindung der Datenbank oder des Benutzerschemas.
	Hinweis: Das Löschen der Standard-Profildatenbank oder einer Datenbank, die gerade verwendet wird, ist nicht möglich.
Hinzufügen	Fügt eine Microsoft SQL Server-Datenbank oder ein Oracle Server-Benutzerschema hinzu, wie in der Dropdownliste der Datenbanken angegeben.
Datenbankname	Der Name der Datenbank.
Datenbanktyp	Der Typ der Datenbank, entweder Microsoft SQL oder Oracle.
Servername	Der Name des Servers, auf dem die Datenbank ausgeführt wird.

Seite "Dienstprogramm für Datenmarkierung"

Auf dieser Seite können Sie Datengruppen nach Applikation oder Speicherort für Business Process Monitor-Daten und nach SiteScope-Zielcomputer für SiteScope-Daten für das Entfernen auswählen.

Zugriff	Doppelklicken Sie auf dem Gateway-Server auf die Datei <hpbsm-gateway-server-stammverzeichnis>\tools\dataMarking\dataMarking.bat. Es wird ein Eingabeaufforderungsfenster gefolgt von einem Anmeldefeld für das Dienstprogramm zur Datenmarkierung angezeigt. Geben Sie den Benutzernamen und das Kennwort eines BSM-Benutzers mit Superuser-Berechtigungen ein.</hpbsm-gateway-server-stammverzeichnis>	
Wichtiger Hinweis	Führen Sie nicht mehrere Instanzen eines Dienstprogramms zur Datenmarkierung gleichzeitig aus, da dies den Neuaggregierungsprozess beinträchtigen kann.	
	Markieren Sie keine Datengruppen für Zeiträume, die bereinigte Daten enthalten (Daten die mithilfe des Partitions-Managers und des Purging Managers entfernt wurden), da dies den Neuaggregierungsprozess beinträchtigen kann.	
Siehe	"Entfernen unerwünschter Daten aus der Profildatenbank" auf Seite 81	
auch	"Fehlerbehebung und Einschränkungen" auf Seite 101	

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Applikationen	Eine Liste von Applikationen, die als veraltet markiert werden können.
Geschäftstransaktionsflüsse	Eine Liste der Geschäftstransaktionsflusss, die als veraltet markiert werden können.
	Hinweis: Dieses Feld wird nur in der Ansicht Applikationen angezeigt (wenn Sie Applikationen in der Dropdownliste Anzeigen nach auswählen).
Dauer	Wählen Sie einen Zeitraum, beginnend mit der angegebenen Startzeit, ab dem das Dienstprogramm Daten als nicht verfügbar markieren soll.
	Hinweis: Sie können eine maximale Dauer von 6 Stunden und 59 Minuten für jede Datenmarkierungsausführung einstellen. Weitere Informationen zum Anpassen dieses Werts finden Sie unter "Anpassen der Konfigurationen von Dienstprogrammen für Datenmarkierungen" auf Seite 89.
Informationen abrufen	Klicken Sie auf diese Schaltfläche, bevor Sie das Dienstprogramm zur Datenmarkierung ausführen, um die Anzahl der zu markierenden Datenzeilen anzuzeigen. Weitere Informationen finden Sie unter "Seite "Dienstprogramm für Datenmarkierung"" auf der vorherigen Seite.
Speicherorte	Eine Liste der Speicherorte, die als veraltet markiert werden können.

Elemente der Oberfläche	Beschreibung
Daten als veraltet markieren	Markiert die gefilterten Kriterien (Applikationen, Geschäftstransaktionsflüsse, Transaktionen, Speicherorte oder SiteScope-Ziele) als veraltet.
Daten als gültig markieren (Markierung als veraltet rückgängig machen)	Stellt die ausgewählten Daten wieder zur Verfügung, nachdem sie als veraltet markiert wurden.
Fortschritt	Zeigt den Fortschritt des Datenmarkierungs- und des Neuaggregierungsverfahrens an.
SiteScope-Ziele	Eine Liste der SiteScope-Zielcomputer (d. h. Computer, die von SiteScope überwacht werden), die als veraltet markiert werden können.
	Hinweis: Dieses Feld wird nur in der SiteScope-Ansicht angezeigt (wenn Sie SiteScope-Ansicht in der Dropdownliste Anzeigen nach auswählen).
Starten	Aktiviert das Dienstprogramm zur Datenmarkierung und markiert Daten als veraltet.
Startzeit	Wählen Sie ein Startdatum und eine Zeit für die Markierung als nicht verfügbar aus.
Transaktionen	Eine Liste der Transaktionen, die als veraltet markiert werden können.
	Hinweis: Dieses Feld wird nur in der Ansicht Applikationen angezeigt (d. h., wenn Sie Applikationen in der Dropdownliste Anzeigen nach: auswählen).
Anzeigen nach	Wählen Sie den Anzeigetyp aus, der im Dienstprogramm zur Datenmarkierung angezeigt werden soll:
	Applikationen
	Speicherorte
	SiteScope-Ziele

Informationsfenster Datenmarkierung

In diesem Fenster werden die Daten angezeigt, die vom Dienstprogramm für Datenmarkierung als veraltet markiert werden sollen.

Zugriff	Klicken Sie auf der Seite des Dienstprogramms für Datenmarkierung auf die	
	Schaltfläche Informationen abrufen.	

Wichtiger Hinweis	Im unteren Teil des Informationsfensters Datenmarkierung werden die SLAs angezeigt, die von den markierten Daten betroffen sind. Sie können die betroffenen SLAs auf der Registerkarte Vereinbarungs-Manager unter Admin > Service Level Management neu berechnen. Weitere Informationen finden Sie unter "Recalculation for SLAs" im BSM Application Administration Guide.	
Siehe auch	"Entfernen unerwünschter Daten aus der Profildatenbank" auf Seite 81"Fehlerbehebung und Einschränkungen" auf Seite 101	

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Applikationsname	Der Name der Applikation, die als veraltet markiert werden soll.
Anzahl der zu aktualisierenden Zeilen	Die Anzahl der Datenzeilen, die als veraltet markiert werden sollen.
Insgesamt zu aktualisierende Zeilen	Die Anzahl der Zeilen, die insgesamt als veraltet markiert werden sollen. Diese Zahl kann von dem Wert des Felds Anzahl der zu aktualisierenden Zeilen abweichen.

Seite "Profildatenbank-Eigenschaften - MS SQL Server"

Auf dieser Seite können Sie eine neue oder bestehende Profildatenbank unter Microsoft SQL Server konfigurieren.

Zugriff	Wählen Sie Admin> Plattform > Setup und Verwaltung > Profildatenbanken verwalten aus, wählen Sie Microsoft SQL aus der Datenbank-Dropdownliste aus und klicken Sie auf Hinzufügen.
Wichtiger Hinweis	 Es wird empfohlen, dass Sie die Microsoft SQL Server-Datenbanken manuell konfigurieren und dann über die Seite Datenbankverwaltung eine Verbindung zu ihnen herstellen. Weitere Informationen zum manuellen Konfigurieren der Microsoft SQL Server-Datenbanken finden Sie unter "Overview of Microsoft SQL server Deployment" im BSM Database Guide. Das Erstellen von Datenbanken kann mehrere Minuten dauern.
Relevante Aufgaben	"Konfigurieren einer Profildatenbank auf einem Microsoft SQL-Server" auf Seite 82
Siehe auch	"Datenbankverwaltung" auf Seite 76

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Datenbank bzw.	Wählen Sie dies je nach Bedarf aus.
Tabellen erstellen	Um eine neue Datenbank zu erstellen oder eine Verbindung zu einer bestehenden leeren Datenbank herzustellen und sie mit Profiltabellen zu füllen, müssen Sie das Kontrollkästchen aktivieren.
	Um eine Verbindung zu einer bestehenden Datenbank herzustellen, die bereits mit Profiltabellen gefüllt ist, müssen Sie das Kontrollkästchen deaktivieren.
Datenbankname	Geben Sie beim Konfigurieren einer neuen Datenbank einen aussagekräftigen Namen für die Datenbank an.
	 Wenn Sie eine Verbindung zu einer bereits erstellten Datenbank herstellen, müssen Sie den Namen dieser bestehenden Datenbank angeben.
Trennen	Trennt die Datenbank von BSM.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie auf die
	Schaltfläche Datenbank trennen auf der Seite Datenbankverwaltung geklickt haben.
Als Standard-	Wählen Sie dies je nach Bedarf aus.
Profildatenbank festlegen (für	Hinweis:
benutzerdefinierte Datentypen erforderlich)	Diese Einstellung ist erforderlich, wenn Sie Service Health-, Real User Monitor-, HP Diagnostics- (sofern installiert), Service Level Management-, SOA- oder persistente benutzerdefinierte Daten sammeln.
	Durch Aktivieren dieses Kontrollkästchens wird die bestehende Standard-Profildatenbank überschrieben.
Kennwort	Sollte nicht ausgefüllt werden, wenn Sie die Windows- Authentifizierung verwenden. Stellen Sie sicher, dass der BSM- Service ausgeführt wird, indem Sie eine Anmeldung als Windows- Benutzer durchführen, der im Datenbankserver als autorisierter Benutzer konfiguriert wurde.
	Bei Verwendung der SQL Server-Authentifizierung geben Sie das Kennwort eines Benutzers mit Administratorrechten für Microsoft SQL Server ein.

Elemente der Oberfläche	Beschreibung
Port	Geben Sie die Portnummer für die folgenden Fälle ein:
	Der TCP/IP-Port von Microsoft SQL Server ist für einen nicht standardmäßigen Port (1433) konfiguriert.
	Sie verwenden einen nicht standardmäßigen Port im statischen Modus.
	Sie verwenden einen nicht standardmäßigen Port im dynamischen Modus. Geben Sie in diesem Fall Port 1434 ein.
Servername	Geben Sie den Namen des Computers ein, auf dem Microsoft SQL Server installiert ist. Wenn Sie eine nicht standardmäßige Microsoft SQL Server-Instanz im dynamischen Modus verwenden, geben Sie den Servernamen im folgenden Format ein: <mein_server\meine_ instanz></mein_server\meine_
SQL Server- Authentifizierung	Wählen Sie aus, ob Microsoft SQL Server die SQL Server- Authentifizierung verwenden soll.
Benutzername	Sollte nicht ausgefüllt werden, wenn Sie die Windows- Authentifizierung verwenden.
	Bei Verwendung der SQL Server-Authentifizierung geben Sie den Benutzernamen eines Benutzers mit Administratorrechten für Microsoft SQL Server ein.
Windows- Authentifizierung	Wählen Sie aus, ob Microsoft SQL Server die Windows- Authentifizierung verwenden soll.

Seite "Profilbenutzerschema-Eigenschaften – Oracle Server"

Auf dieser Seite können Sie ein oder mehr Profilbenutzerschemata auf Ihrem Oracle-Server konfigurieren.

Z	ugriff	Wählen Sie Admin> Plattform > Setup und Verwaltung > Profildatenbanken	
		verwalten, wählen Sie Oracle aus der Datenbank-Dropdownliste, und klicken Sie	
		auf Hinzufügen .	

Wichtiger Hinweis	 Es wird empfohlen, dass Sie die Oracle-Serverbenutzerschemata manuell konfigurieren und dann über die Seite Datenbankverwaltung eine Verbindung zu ihnen herstellen. Weitere Informationen zum manuellen Konfigurieren der Oracle-Serverbenutzerschemata finden Sie unter "Overview of Oracle Server Deployment" im Handbuch BSM Database Guide. Das Erstellen von Benutzerschemata kann mehrere Minuten dauern. Im Browser tritt möglicherweise eine Zeitüberschreitung auf, bevor der Erstellungsprozess abgeschlossen ist. Er wird jedoch auf Serverseite fortgeführt. Wenn die Zeitüberschreitung auftritt, bevor eine Bestätigungsmeldung angezeigt wird, sollten Sie prüfen, ob der Name des Benutzerschemas in der Datenbankliste auf der Seite Datenbankverwaltung angezeigt wird, um sicherzustellen, dass das Benutzerschema erfolgreich erstellt wurde.
Relevante Aufgaben	"So konfigurieren Sie ein Benutzerschema auf einem Oracle-Server" auf Seite 83
Siehe auch	"Datenbankverwaltung" auf Seite 76

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Datenbank bzw. Tabellen	Wählen Sie dies je nach Bedarf aus.
erstellen	Um ein neues Benutzerschema zu erstellen oder eine Verbindung zu einem bestehenden leeren Benutzerschema herzustellen und es mit Profiltabellen füllen, müssen Sie das Kontrollkästchen aktivieren.
	Um eine Verbindung zu einem bestehenden Benutzerschema herzustellen, das bereits mit Profiltabellen gefüllt ist, müssen Sie das Kontrollkästchen deaktivieren.
	Hinweis: Durch Deaktivieren dieses Kontrollkästchens werden die Felder mit dem Datenbank-Verbindungsparameter und Tablespace auf der Seite deaktiviert, und die Plattform wird angewiesen, die Informationen in diesen Feldern beim Verbinden mit dem Oracle-Server zu ignorieren.
Kennwort für Datenbankadministrator	Geben Sie das Kennwort eines Benutzers mit Administratorberechtigungen für den Oracle-Server ein.
	Hinweis: Dieses Feld ist nur aktiviert, wenn Sie das Kontrollkästchen Datenbank bzw. Tabellen erstellen aktiviert haben.

Elemente der Oberfläche	Beschreibung
Benutzername des Datenbankadministrators	Geben Sie den Benutzernamen und das Kennwort eines Benutzers mit Administratorberechtigungen für den Oracle-Server ein.
	Hinweis: Dieses Feld ist nur aktiviert, wenn Sie das Kontrollkästchen Datenbank bzw. Tabellen erstellen aktiviert haben.
Standard-Tablespace	Geben Sie den Namen des Standard-Tablespaces an, der für die Profilbenutzerschemata vorgesehen ist.
	Standardwert: users
Trennen	Trennt das Benutzerschema von BSM.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie auf die Schaltfläche Datenbank trennen auf der Seite Datenbankverwaltung geklickt haben.
Hostname	Geben Sie den Namen des Computers ein, auf dem der Oracle- Server installiert ist.
Als Standard-	Wählen Sie dies je nach Bedarf aus.
Profildatenbank festlegen (für	Hinweis:
benutzerdefinierte Datentypen erforderlich)	Diese Einstellung ist erforderlich, wenn Sie Service Health-, Real User Monitor-, HP Diagnostics- (sofern installiert), Service Level Management-, SOA- oder persistente benutzerdefinierte Daten sammeln.
	Durch Aktivieren dieses Kontrollkästchens wird die bestehende Standard-Profildatenbank überschrieben.
Port	Geben Sie den erforderlichen Oracle-Listenerport ein, oder übernehmen Sie den Standardwert.
Kennwort erneut eingeben	Geben Sie das Benutzerschema-Kennwort erneut ein.
SID	Geben Sie den erforderlichen Oracle-Instanznamen ein, oder übernehmen Sie den Standardwert.
Temporärer Tablespace	Geben Sie den Namen des temporären Tablespaces an, der für die Profilbenutzerschemata vorgesehen ist.
	Standardwert: temp
TNS-Name	Geben Sie den TNS-Namen des Oracle-Clients ein, der in der Datei tnsnames.ora auf dem Gateway-Server angegeben ist. Diese Datei befindet sich im Verzeichnis <oracle_home>\network\admin.</oracle_home>

Elemente der Oberfläche	Beschreibung
Name des Benutzerschemas	Geben Sie beim Konfigurieren eines neuen Benutzerschemas einen aussagekräftigen Namen für das Benutzerschema an.
	Wenn Sie eine Verbindung zu einem bereits erstellten Benutzerschema herstellen, müssen Sie den Namen dieses bestehenden Benutzerschemas angeben.
Kennwort für Benutzerschema	Geben Sie beim Konfigurieren eines neuen Benutzerschemas ein Kennwort ein, das den Zugriff auf das Benutzerschema ermöglicht.
	Wenn Sie eine Verbindung zu einem bereits erstellten Benutzerschema herstellen, müssen Sie das Kennwort für dieses bestehende Benutzerschema angeben.
	Hinweis: Für jedes Benutzerschema, das Sie für BSM auf dem Oracle-Server erstellen, müssen Sie einen eindeutigen Benutzerschema-Namen angeben.

Wenn Ihre Profildatenbank Teil von Oracle Real Application Cluster (RAC) ist, finden Sie weitere Informationen unter "Support for Oracle Real Application Cluster" im Handbuch BSM Database Guide.

Seite "Purging Manager"

Auf dieser Seite können der Partitions-Manager und der Purging Manager aktiviert oder deaktiviert werden, wodurch BSM angewiesen wird, den Partitionierungsprozess der Daten zu starten bzw. zu beenden.

Zugriff	Wählen Sie Admin> Plattform > Setup und Verwaltung > Partitionieren und Löschen von Daten aus.
Wichtiger Hinweis	Der Partitions- und der Purging Manager verwenden die native Partitionierung. In Oracle-Datenbanken sollte die Option Oracle-Partitionierung aktiviert sein. Weitere Informationen zum Bereinigen von Daten in einer Oracle-Datenbank finden Sie unter "About Data Partitioning and Purging" im Handbuch BSM Database Guide.
Siehe auch	"Partitionieren und Löschen von historischen Daten aus Datenbanken" auf Seite 78

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Anwenden auf	Hiermit können die Datenbanken und die Vorlage ausgewählt werden, auf die die Konfigurationen der Registerkarte Vorlage und mehrere Datenbanken angewendet werden sollen. Sie können die Auswahl der Datenbanken aufheben, um ausschließlich Änderungen an der ausgewählten Vorlage vorzunehmen.
Ändern in EPM	Die konfigurierte Datenmenge, die pro Minute bei BSM eingehen soll.
	Hinweis: Lassen Sie dieses Feld leer, um den bestehenden EPM-Wert beizubehalten.
	Details zum Festlegen dieses Werts finden Sie unter "Festlegen der Ereignisse pro Minute für das Eintreffen von Daten in BSM" auf Seite 88.
Datenbankspezifisch	Auf dieser Registerkarte können Sie den Zeitbereich für das Bereinigen von Daten in einer Tabelle je nach Profildatenbank ändern.
Beschreibung	Beschreibt die betreffende Datenbanktabelle.
EPM-Wert	Die Datenmenge, die pro Minute bei BSM eingeht. Details zum Festlegen dieses Werts finden Sie unter "Festlegen der Ereignisse pro Minute für das Eintreffen von Daten in BSM" auf Seite 88.
Daten beibehalten für	Hier wird festgelegt, wie lange die Daten in den Datenbanktabellen gespeichert bleiben sollen, deren Kontrollkästchen aktiviert sind. Dieses Element besteht aus folgenden Komponenten:
	Auswahlfelder. Legen Sie oben auf der Seite fest, wie lange die Daten in den ausgewählten Datenbanktabellen gespeichert bleiben sollen.
	Spaltenüberschrift. Zeigt an, wie lange die Daten in den einzelnen Datenbanktabellen gespeichert bleiben. Der Wert wird in den Auswahlfeldern unter Daten beibehalten oben auf der Seite konfiguriert.
	Hinweis: Mit dem Zeitraum unter Daten beibehalten wird angegeben, wie lange die Daten mindestens gespeichert bleiben, es wird damit aber nicht angegeben, wann die Daten bereinigt werden. Standardmäßig ist die Speicherdauer auf Unendlich festgelegt, was bedeutet, dass keine Bereinigung vorgesehen ist.

Elemente der Oberfläche	Beschreibung
Name der Tabelle in	Der Name der Tabelle in der Datenbank.
Datenbank	Die Datenbanktabellen werden anhand des Daten-Collectors aufgelistet, aus dem die Daten abgerufen wurden. Folgende Datentypen stehen zur Verfügung:
	Warnungen
	• BPI
	Business Logic Engine
	Business Process Monitor
	Diagnose
	Real User Monitor
	• SOA
	Service Level Management
	SiteScope
	• TV
	UDX (benutzerdefinierte Daten)
	WebTrace
Profildatenbank auswählen	Wählen Sie eine Profildatenbank aus, für die Sie den Zeitbereich für die Datenbereinigung ändern möchten.
	Hinweis: Dieses Feld ist nur auf der Registerkarte Datenbankspezifisch sichtbar.
Vorlage und	Auf dieser Registerkarte können Sie folgende Aufgaben ausführen:
mehrere Datenbanken	Ändern der Partitionierungs- und Bereinigungsparameter für mehrere Profildatenbanken
	Ändern der Datenbankvorlage, damit die Parameter in später erstellte Datenbanken übernommen werden
	Hinweis: Nachdem Sie Änderungen vorgenommen haben, werden auf der Registerkarte Vorlage und mehrere Datenbanken weiterhin die Vorlageneinstellungen angezeigt, auch wenn Sie keine Änderungen an der Vorlage vorgenommen haben, sondern die Einstellungen für bestimmte Datenbanken manuell geändert haben. Nachdem diese manuellen Änderungen angewendet wurden, werden die angezeigten Einstellungen auf die Vorlageneinstellungen zurückgesetzt. Um die Einstellungen zu sehen, die Sie für bestimmte Datenbanken geändert haben, navigieren Sie zur Registerkarte Datenbankspezifisch und wählen die entsprechende Datenbank aus.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Fehlerbehebungen und Einschränkungen für die Datenbankverwaltung.

Dieser Abschnitt umfasst die folgenden Themen:

- "Fehlerbehebung beim Dienstprogramm für Datenmarkierungen"
- "Beschränkungen bei Dienstprogrammen für Datenmarkierungen"

Fehlerbehebung beim Dienstprogramm für Datenmarkierungen

Bei der Verwendung von Dienstprogrammen für Datenmarkierungen können unterschiedliche Fehlertypen auftreten. Im Allgemeinen wird die folgende Fehlermeldung angezeigt, wenn ein Fehler auftritt:

The Data Marking utility must shut down due to an internal error. (Das Dienstprogramm für Datenmarkierungen muss aufgrund eines internen Fehlers beendet werden.) Weitere Informationen finden Sie unter: <HPBSM-Gateway-Server-Stammverzeichnis>\log\datamarking.log

Gründe für die Anzeige der Fehlermeldung im Dienstprogramm:

- Fehler beim Verbinden zum Datenbankserver oder zur Profildatenbank.
- Fehler beim Fertigstellen des Datenmarkierungsverfahrens, beispielsweise aufgrund eines Verbindungsfehlers zwischen dem Aggregationsserver und der Datenbank.
- BSM-Fehler beim erneuten Aggregieren von Rohdaten für die definierte Datenreihe.

Überprüfen Sie im Fall eines Fehlers die Datei < HPBSM-Gateway-Server-Stammverzeichnis>\log\datamarking.log auf entsprechende Informationen.

Beschränkungen bei Dienstprogrammen für Datenmarkierungen

Im Folgenden werden die Beschränkungen aufgeführt, die bei Dienstprogrammen für Datenmarkierungen vorliegen:

- Das Dienstprogramm unterstützt nicht das Entfernen von spät eintreffenden Daten.
 - Wenn beispielsweise eine Datenreihe in einem bestimmten Zeitraum für das Entfernen markiert wird und BSM später Daten aus diesem Zeitraum erhält (die spät eingetroffen sind, weil Business Process Monitor zeitweise keine Verbindung zum Gateway-Server herstellen konnte), stehen die spät eintreffenden Daten nicht für die Verwendung in Reports zur Verfügung. Verwenden Sie die Schaltfläche **Informationen abrufen**, um nach spät eintreffenden Daten zu suchen. Wird eine anderer Wert als 0 für die Zeilen angezeigt, führen Sie ggf. das Dienstprogramm erneut aus, um die spät eingetroffenen Daten zu entfernen.
- Das Dienstprogramm unterstützt nicht das Entfernen von Daten, die während des Datenmarkierungsverfahrens eintreffen.

Wenn beispielsweise eine Datenreihe in einem bestimmten Zeitraum für das Entfernen markiert wurde und in demselben Zeitraum (während der Dienstprogrammausführung) Daten eintreffen und in die Profildatenbank aufgenommen werden, werden die Zeilen der neu eingetroffenen Daten nicht für das Entfernen markiert und daher auch nicht entfernt. Verwenden Sie in diesem Fall nach Ausführung des Dienstprogramms die Schaltfläche **Informationen abrufen**, um festzulegen, ob alle Datenzeilen für den ausgewählten Zeitraum entfernt wurden. Werden Zeilen

angezeigt, führen Sie ggf. das Dienstprogramm erneut aus, um die Daten zu entfernen, die während der Ausführung eingetroffen sind. Es handelt sich hierbei um ein seltenes Szenario, da normalerweise Daten für einen früheren Zeitraum markiert werden und nicht für einen Zeitraum, der in der Zukunft endet.

 Während der Ausführung des Dienstprogramms und des Entfernens der Daten zeigen die Reports, die in diesem Zeitraum erzeugt werden, möglicherweise keine genauen Ergebnisse an. Es wird daher empfohlen, das Dienstprogramm außerhalb der Spitzenzeiten von BSM zu verwenden.

Kapitel 8

Infrastruktureinstellungen

Sie können BSM-Einstellungen konfigurieren, um die Anforderungen Ihrer Organisation in Bezug auf die Plattform und deren Applikationen zu erfüllen. Die meisten Infrastruktureinstellungen konfigurieren Sie direkt über die Verwaltungskonsole.

BSM ermöglicht es Ihnen, die Werte vieler Einstellungen anzupassen, mit denen festgelegt wird, wie BSM und die entsprechenden Applikationen ausgeführt werden.

Achtung: Das Anpassen bestimmter Einstellungen kann sich negativ auf die Leistung von BSM auswirken. Es wird daher dringend empfohlen, keine Anpassungen vorzunehmen, ohne vorher die HP Software-Unterstützung oder einen HP Services-Mitarbeiter zu kontaktieren

Im Infrastructure Settings Manager können Sie verschiedene Kontexte auswählen, über die Sie Einstellungen anzeigen und bearbeiten. Diese Kontexte sind in die folgenden Gruppen unterteilt:

- Applikationen. In dieser Liste sind die Kontexte enthalten, mit denen festgelegt wird, wie sich
 die verschiedenen Applikationen bei der Ausführung in BSM verhalten. Es werden Kontexte wie
 die Applikation Service Health, MyBSM und Service Level Management aufgelistet.
- **Foundation.** In dieser Liste sind die Kontexte enthalten, mit denen festgelegt wird, wie die verschiedenen Bereiche der BSM-Foundation ausgeführt werden. Es werden Kontexte wie RTSM (Run-time Service Model) und LDAP-Konfiguration aufgelistet.

Beschreibungen der einzelnen Einstellungen werden in der Tabellenspalte **Beschreibung** der Seite **Infrastruktureinstellungen** angezeigt.

Weitere Informationen zum Konfigurieren der meisten Infrastruktureinstellungen finden Sie unter "Ändern der Infrastruktureinstellungen im Infrastructure Settings Manager" auf der nächsten Seite.

Einige Infrastruktureinstellungen werden außerhalb des Infrastructure Settings Manager vorgenommen. Weitere Informationen finden Sie unter "Ändern des Ping-Zeitintervalls" auf Seite 105 und "Ändern des Speicherorts und Ablaufs von temporären Bilddateien" auf Seite 106.

Ändern der Infrastruktureinstellungen im Infrastructure Settings Manager

In dieser Aufgabe wird das Ändern von Infrastruktureinstellungen im Infrastructure Settings Manager beschrieben.

So ändern Sie die Infrastruktureinstellungen mithilfe des Infrastructure Settings Managers:

- Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus
- Wählen Sie eine Gruppe von Kontexten zur Ansicht aus: Applikationen, Foundation oder Alle.
- 3. Wählen Sie einen bestimmten Kontext aus der Dropdownliste aus.
- 4. Alle konfigurierbaren Infrastruktureinstellungen, die mit diesem Kontext verknüpft sind, werden zusammen mit den Beschreibungen und den aktuellen Werten der jeweiligen Einstellungen angezeigt. Klicken Sie auf die Schaltfläche Einstellung bearbeiten und bearbeiten Sie den Wert einer bestimmten Einstellung.

Ändern des Ping-Zeitintervalls

Hinweis: Diese Aufgabe für Infrastruktureinstellungen wird nicht im Infrastructure Settings Manager durchgeführt.

Sie können das Zeitintervall ändern, nach dem BSM dem Server ein Ping-Signal zum Aktualisieren einer Sitzung sendet.

So ändern Sie das Ping-Zeitintervall:

- 1. Öffnen Sie die Datei **<Gateway-Server-Stammverzeichnis>\conf\settings\website.xml** in einem Texteditor.
- 2. Suchen Sie nach dem Parameter. user.session.ping.timeinterval.
- Ändern Sie den Wert (Standard: 120) für das Ping-Zeitintervall. Dieser Wert muss weniger als die Hälfte, idealerweise jedoch weniger als ein Drittel des Werts betragen, der für die Sitzungszeitüberschreitung (der Parameter user.session.timeout) angegeben ist.
- 4. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- 5. Wenn Sie über mehrere Gateway-Servercomputer verfügen, wiederholen Sie dieses Verfahren auf allen Computern.

Ändern des Speicherorts und Ablaufs von temporären Bilddateien

Hinweis: Diese Aufgabe für Infrastruktureinstellungen wird nicht im Infrastructure Settings Manager durchgeführt.

Wenn Sie in BSM-Applikationen einen Report generieren oder wenn BSM automatisch einen Report zum Senden über den Mechanismus für geplante Reports generiert, werden Bilder (z. B. Diagramme) erstellt. BSM speichert diese Bilder für einen begrenzten Zeitraum in temporären Verzeichnis auf den Gateway-Servercomputern, auf denen die Bilder generiert werden.

Sie können die folgenden Einstellungen für diese Bilder ändern:

- Den Pfad zum Verzeichnis, in dem die temporären Bilddateien gespeichert sind Weitere Informationen finden Sie unter "Ändern des Verzeichnisses, in dem temporäre Bilddateien gespeichert werden" auf der nächsten Seite.
- Die Konfiguration eines freigegebenen Speicherorts für temporäre Bilddateien
 Weitere Informationen finden Sie unter "Zugreifen auf temporäre Verzeichnisse mit mehreren Gateway-Servercomputern" auf Seite 108.
- Die Dauer, für die BSM temporäre Bilddateien behält, bevor sie entfernt werden
 Weitere Informationen finden Sie unter "Ändern der Beibehaltungsdauer temporärer Bilddateien durch BSM" auf Seite 111.
- Die Verzeichnisse, aus denen temporäre Bilddateien entfernt werden

 Weitere Informationen finden Sie unter "Angeben der Verzeichnisse, aus denen temporäre
 Bilddateien entfernt werden" auf Seite 114.

Ändern des Verzeichnisses, in dem temporäre Bilddateien gespeichert werden

Sie können den Pfad zu dem Verzeichnis ändern, in dem BSM in geplanten Reports verwendete generierte Bilder speichert. So können Sie beispielsweise generierte Bilder auf einer anderen Datenträgerpartition, Festplatte oder einem anderen Computer mit mehr Speicherplatz als der Partition/Festplatte bzw. dem Computer speichern, auf dem der Gateway-Servercomputer installiert ist.

So ändern Sie den Pfad zum Verzeichnis mit den temporären Bilddateien:

- Öffnen Sie die Datei < Gateway-Server-Stammverzeichnis > \conf\topaz.config in einem Texteditor.
- 2. Suchen Sie nach dem Parameter images.save.directory.offline.
- Entfernen Sie das Kommentarzeichen (#) aus der Zeile, die mit #images.save.directory.offline= beginnt, und ändern Sie den Wert anhand des erforderlichen Pfades.

Hinweis: Verwenden Sie in einer Windows-Umgebung beim Definieren des Pfades die UNC-Pfadsyntax (\\\\Server\\Pfad). Verwenden Sie in einer Solaris-Umgebung beim Definieren des Pfades Schrägstriche (/) und keine umgekehrten Schrägstriche (\).

- 4. Speichern Sie die Datei topaz.config.
- 5. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.
- 7. Ordnen Sie das neu definierte physische Verzeichnis mit den Bildern einem virtuellen Verzeichnis im Webserver auf allen Gateway-Servercomputern zu. Weitere Informationen finden Sie unter "Zugreifen auf temporäre Verzeichnisse mit mehreren Gateway-Servercomputern" auf der nächsten Seite.

Zugreifen auf temporäre Verzeichnisse mit mehreren Gateway-Servercomputern

Wenn BSM-Reports mithilfe einer virtuellen IP auf den Gateway-Servercomputer zugreifen, könnte der Load Balancer Anforderungen an einen beliebigen Gateway-Servercomputer senden. Deshalb müssen sich die Bilddateien an einem gemeinsamen Speicherort befinden, der auf allen Gateway-Servercomputern konfiguriert und an alle freigegeben ist. Dies ist typisch für ein Szenario, in dem mehrere Gateway-Servercomputer in der BSM-Architektur hinter einem Load Balancer ausgeführt werden.

Zur Unterstützung eines freigegebenen Speicherorts für temporäre Bilder in einer Windows-Umgebung wird folgende Konfiguration empfohlen:

- Alle Gateway-Server und der Computer, auf dem das freigegebene Bildverzeichnis definiert ist, falls dieser kein Gateway-Server ist sollten sich in derselben Windows-Domäne befinden.
- Das virtuelle IIS-Verzeichnis sollte für die Verwendung der Anmeldeinformationen eines Kontos konfiguriert werden, das Mitglied der Gruppe der Domänenbenutzer ist.
- Das Konto für das virtuelle Verzeichnis sollte Lese-/Schreibberechtigungen für das freigegebene Bildverzeichnis erhalten.

Hinweis: Wenn Ihre Serverkonfiguration eine Platzierung von Servern in verschiedenen Windows-Domänenkonfigurationen erfordert, wenden Sie sich an den HP Software-Unterstützung.

Wenn Sie einen benutzerdefinierten Pfad zu temporären Bildem festlegen, wie im Parameter **images.save.directory.offline** definiert (weitere Informationen siehe "Ändern des Verzeichnisses, in dem temporäre Bilddateien gespeichert werden" auf der vorherigen Seite), müssen Sie das physische Verzeichnis mit den Bildem einem virtuellen Verzeichnis im Webserver auf allen Gateway-Servercomputern zuordnen.

So konfigurieren Sie das virtuelle Verzeichnis in IIS:

1. Benennen Sie das physische Standarverzeichnis mit den temporären Bildern für geplante Reports auf dem Gateway-Servercomputer um.

Benennen Sie beispielsweise:

```
<Gateway-Server-Stammverzeichnis>\AppServer\webapps\
site.war\Imgs\chartTemp\offline
```

um in

```
<Gateway-Server-Stammverzeichnis>\AppServer\webapps
\site.war\Imgs\chartTemp\old_offline
```

 Navigieren Sie im Internetdienste-Manager von IIS auf dem Gateway-Servercomputer zu Standardwebsite > Topaz > Imgs > ChartTemp.

Das umbenannte Offlineverzeichnis wird im rechten Frame angezeigt.

3. Klicken Sie im rechten Frame mit der rechten Maustaste und wählen Sie Neu > Virtuelles

Verzeichnis. Der Assistent zum Erstellen eines virtuellen Verzeichnisses wird angezeigt. Klicken Sie auf **Weiter**.

- 4. Geben Sie im Dialogfeld **Alias für virtuelles Verzeichnis** im Feld **Alias** den Alias offline ein, um das neue virtuelle Verzeichnis zu erstellen. Klicken Sie auf **Weiter**.
- 5. Geben Sie im Dialogfeld Verzeichnis des Websiteinhalts den Pfad des physischen Verzeichnisses mit den temporären Bilddateien wie im Parameter images.save.directory.offline definiert (weitere Informationen siehe "Ändern des Verzeichnisses, in dem temporäre Bilddateien gespeichert werden" auf Seite 107) ein oder suchen Sie diesen. Klicken Sie auf Weiter.
- Befindet sich das physische Verzeichnis mit den temporären Bildern auf einem lokalen Computer, geben Sie im Dialogfeld Zugriffsberechtigungen die Berechtigungen Lesen und Schreiben an.

Befindet sich das physische Verzeichnis mit den temporären Bildern auf einem Computer im Netzwerk, geben Sie im Dialogfeld **Benutzername und Kennwort** den Benutzernamen und das Kennwort eines Benutzers mit Zugriffsberechtigungen für diesen Computer ein.

- 7. Klicken Sie auf **Weiter** und dann **Fertig stellen**, um das Erstellen des virtuellen Verzeichnisses abzuschließen.
- 8. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- 9. Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.

So konfigurieren Sie das virtuelle Verzeichnis auf einem Apache HTTP-Webserver:

1. Benennen Sie das physische Standarverzeichnis mit den temporären Bildern für geplante Reports auf dem Gateway-Servercomputer um.

Benennen Sie beispielsweise:

```
<Gateway Server-
Stammverzeichnis>\AppServer\webapps\site.war\Imgs\chartTemp\offline
um in

<Gateway Server-
Stammverzeichnis>\AppServer\webapps\site.war\Imgs\chartTemp\old_
offline
```

- Öffnen Sie die Apache-Konfigurationsdatei < Gateway-Server-Stammverzeichnis>\WebServer\conf\httpd.conf in einem Texteditor.
- 3. Ordnen Sie dem physischen Standort des gemeinsamen Verzeichnisses ein virtuelles Verzeichnis namens **offline** zu, indem Sie der Datei die folgende Zeile hinzufügen:

```
Alias /Imgs/chartTemp/offline <Freigegebenes_Verzeichnis_für_temporäre Bilder>,
```

wobei Freigegebenes_Verzeichnis_für_temporäre_Bilder> den Pfad zum
physischen Verzeichnis mit den temporären Bildern geplanter Reports darstellt, wie im
Parameter images.save.directory.offline definiert (weitere Informationen siehe "Ändern des
Verzeichnisses, in dem temporäre Bilddateien gespeichert werden" auf Seite 107).

- 4. Speichern Sie die Datei.
- 5. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- 6. Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.

So konfigurieren Sie das virtuelle Verzeichnis auf einem Sun Java System Web Server:

1. Benennen Sie das physische Standarverzeichnis mit den temporären Bildern für geplante Reports auf dem Gateway-Servercomputer um.

Benennen Sie beispielsweise:

```
<Gateway-Server-
Stammverzeichnis>\AppServer\webapps\site.war\Imgs\chartTemp\offline
um in
```

```
<Gateway-Server-
Stammverzeichnis>\AppServer\webapps\site.war\Imgs\chartTemp\old_
offline
```

- Öffnen Sie die Sun Java System Web Server-Konfigurationsdatei <Sun Java System Web Server-Installationsverzeichnis>\server\<Servername>\config\obj.conf in einem Texteditor.
- 3. Fügen Sie der Direktive <object name=default> folgende Zeile hinzu (vor der Zeile NameTrans fn=document-root root="\$docroot" und, falls vorhanden, vor der Zeile NameTrans fn="pfx2dir" from="/lmgs" dir="ProductDir/Site Imgs/":

```
NameTrans fn="pfx2dir" from="/topaz/Imgs/chartTemp/offline" dir="<Freigegebenes Verzeichnis für temporäre Bilder>"
```

wobei Freigegebenes_Verzeichnis_für_temporäre_Bilder> den Pfad zum
physischen Verzeichnis mit den temporären Bildern geplanter Reports darstellt, wie im
Parameter images.save.directory.offline definiert (weitere Informationen siehe "Ändern des
Verzeichnisses, in dem temporäre Bilddateien gespeichert werden" auf Seite 107).

- 4. Speichern Sie die Datei.
- 5. Starten Sie den Sun Java System Web Server auf dem Gateway-Servercomputer neu.
- 6. Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.

Ändern der Beibehaltungsdauer temporärer Bilddateien durch BSM

Sie können die Einstellungen ändern, die bestimmen, wie lange BSM vom Gateway-Servercomputer generierte temporäre Bilddateien beibehält, bevor diese aus den definierten temporären Verzeichnissen entfernt werden. Sie können Einstellungen für die folgenden Verzeichnisse in der Datei < HPBSM-Gateway-Server-Stammverzeichnis>\conf\topaz.config ändern:

Verzeichniseinstellung	Beschreibung
remove.files.0.path=//AppServer/webapps/site.war/Imgs/chartTemp/offline	Pfad zu den beim Generieren von Reports erstellten Bildern
remove.files.1.path=//AppServer/webapps/site.war/Imgs/chartTemp/online	Pfad zu den beim Generieren von Reports in BSM-Applikationen erstellten Bildern
remove.files.3.path=//AppServer/webapps/site.war/snapshots	Pfad zu Bildern, die durch den Baseline bei Fehler-Mechanismus erstellt und in Reports mit Fehlerübersicht angezeigt werden

Bei den oben genannten Verzeichnissen mit temporären Bilddateien können Sie die folgenden Einstellungen ändern:

remove.files.directory.number=<Anzahl Verzeichnisse>

Gibt die Gesamtzahl der Verzeichnisse an, für die Sie Einstellungen definieren.

• remove.files.<Pfadnummer>.path=<Verzeichnispfad>

Gibt den Pfad zum Verzeichnis mit den Dateien an, die entfernt werden sollen. Befinden sich zu entfernende temporäre Bilddateien in Standardverzeichnissen, müssen diese Werte den Parametern **images.save.directory.online** und **images.save.directory.offline** entsprechen, die ebenfalls in der Datei **topaz.config** definiert sind.

Hinweis: Verwenden Sie in einer Windows-Umgebung beim Definieren des Pfades die UNC-Pfadsyntax (\\\\Server\\Pfad). Verwenden Sie in einer Solaris-Umgebung beim Definieren des Pfades nur Schrägstriche (/).

remove.files.<Pfadnummer>.expirationTime=<Dateiablaufzeit in Sek.>

Gibt den Zeitraum in Sekunden an, für den eine Datei im angegebenen Verzeichnis von BSM beibehalten wird. Wenn Sie beispielsweise "3600" angeben (die Anzahl der Sekunden in einer Stunde), werden Dateien, die älter sind als eine Stunde, entfernt.

Lassen Sie diese Einstellung leer, wenn BSM nur maximale Größenkriterien verwenden soll (siehe unten).

remove.files.<Pfadnummer>.maxSize=<max. Verzeichnisgröße in KB>

Gibt die Gesamtgröße in KB an, bis zu der das definierte Verzeichnis anwachsen kann, bevor BSM Dateien entfernt. Wenn Sie beispielsweise "100000" (100 MB) angeben, werden bei Überschreiten von 100 MB im Verzeichnis die ältesten Dateien entfernt, um die Verzeichnisgröße auf 100 MB zu reduzieren.

Wenn Sie auch einen Wert im Parameter **remove.files.<Pfadnummer>.expirationTime** definieren, entfernt BSM zuerst abgelaufende Dateien. Ist die maximale Verzeichnisgröße dann immer noch überschritten, entfernt BSM weitere Dateien, und zwar die ältesten Dateien zuerst. Wenn keine Dateien ihre Ablaufzeit überschritten haben, entfernt BSM Dateien ausschließlich nach den Kriterien für die maximale Verzeichnisgröße.

Dieser Parameter wird zusammen mit dem Parameter remove.files.<Nummer_des_definierten_Pfads>.deletePercents (siehe unten) verwendet, der BSM anweist, den angegebenen Prozentsatz an Dateien zu entfernen, zusätzlich zu den Dateien, die über den Parameter remove.files.<Pfadnummer>.maxSize entfernt werden.

Lassen Sie dies und die Einstellungen in **remove.files.<Nummer_des_definierten_ Pfads>.deletePercents** leer, wenn BSM nur das Kriterium für die Ablaufzeit verwenden soll.

remove.files.<Pfadnummer>.deletePercents=<zu entfernende Prozent>

Gibt die zusätzliche Menge an, um die BSM die Verzeichnisgröße reduziert – ausgedrückt als Prozentsatz der maximal zulässigen Verzeichnisgröße –, nachdem die Verzeichnisgröße zunächst gemäß dem Parameter **remove.files.<Pfadnummer>.maxSize** reduziert wurde. BSM löscht die ältesten Dateien zuerst.

Lassen Sie dies und die Einstellungen in **remove.files.<Pfadnummer>.maxSize** leer, wenn BSM nur das Kriterium für die Ablaufzeit verwenden soll.

remove.files.<Pfadnummer>.sleepTime=<Dauer des Thread-Ruhezustands in Sek.>
 Gibt an, wie häufig BSM den Mechanismus zur Durchführung der definierten Aufgaben ausführt.

Beispiel:

BSM ist angewiesen, die folgende Aufgabe einmal alle 30 Minuten durchzuführen: BSM prüft zunächst, ob Dateien älter als eine Stunde sind, um diese ggf. zu löschen. Dann prüft BSM, ob die Gesamtgröße des Verzeichnisses größer ist als 250 MB, um die Verzeichnisgröße ggf. durch Entfernen der ältesten Dateien auf 250 MB zu reduzieren. Schließlich reduziert BSM die Gesamtverzeichnisgröße durch Entfernen der ältesten Dateien um 50 %. Auf diese Weise lässt BSM Dateien mit insgesamt 125 MB im Verzeichnis übrig.

remove files older than 1 hour (3600 sec.)

remove.files.0.expirationTime=3600

reduce folder size to 250 MB

remove.files.0.maxSize=250000

remove an additional 50% of max. folder size (125 MB)

remove.files.0.deletePercents=50

perform work once every 30 min. (1800 sec)

remove.files.0.sleepTime=1800

Tipp: Sie können den Mechanismus zum Entfernen von Dateien so konfigurieren, dass Dateien aus einem definierten Verzeichnis entfernt werden. Sie definieren die Parameter und erweitern den Index in Inkremenenten. Beispiel: Zum Bereinigen eines temporären Verzeichnisses geben Sie als Verzeichnisanzahl 6 statt 5 im Parameter remove.files.directory.number an. Anschließend definieren Sie Pfad und Einstellungen des Verzeichnisses mithilfe des Indexwerts 4 (da 0-4 bereits in den Standardeinstellungen verwendet werden) im Abschnitt Pfadnummer des Parameters. Verwenden Sie diesen Mechanismus zum Entfernen von Dateien nicht, ohne zunächst den zuständigen HP Software-Unterstützung-Mitarbeiter konsultiert zu haben.

So ändern Sie die Standardeinstellungen:

- Öffnen Sie die Datei < HPBSM-Gateway-Server-Stammverzeichnis > \conf\topaz.config in einem Texteditor.
- 2. Bevor Sie die Werte ändern, sichern Sie die Datei oder kommentieren Sie die Standardzeilen (mithilfe von #), damit die Standardwerte als Referenz zur Verfügung stehen.
- 3. Ändern Sie die Einstellungen nach Bedarf.
- 4. Speichern Sie die Datei topaz.config.
- 5. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- 6. Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.

Angeben der Verzeichnisse, aus denen temporäre Bilddateien entfernt werden

Standardmäßig werden temporäre Bilddateien aus dem Stammverzeichnis des angegebenen Verzeichnisses entfernt. Sie können BSM auch so konfigurieren, dass temporäre Bilddateien aus den Unterverzeichnissen des angegebenen Pfads entfernt werden.

So konfigurieren Sie BSM zum Entfernen temporärer Bilddateien aus Unterverzeichnissen:

- Öffnen Sie die Datei < Gateway-Server-Stammverzeichnis > \conf\topaz.config in einem Texteditor.
- 2. Fügen Sie nach den anderen Einstellungen (die im vorherigen Abschnitt beschrieben wurden) des angegebenen Pfads die folgende Zeile ein:

```
remove.files.<Pfadnummer>.removeRecursively=yes
```

- 3. Speichern Sie die Datei topaz.config.
- 4. Starten Sie BSM auf dem Gateway-Servercomputer neu.
- 5. Führen Sie die oben genannten Schritte auf allen Gateway-Servercomputern durch.

Beschreibung der Benutzeroberfläche - Seite "Infrastructure Settings Manager"

Auf dieser Seite können Sie die Werte zahlreicher Einstellungen definieren, mit denen festgelegt wird, wie BSM und die entsprechenden Applikationen ausgeführt werden.

Zugriff	Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus.
Wichtiger Hinweis	Das Anpassen bestimmter Einstellungen kann sich negativ auf die Leistung von BSM auswirken. Es wird daher dringend empfohlen, keine Anpassungen vorzunehmen, ohne vorher die HP Software-Unterstützung oder einen HP Services-Mitarbeiter zu kontaktieren
Siehe auch	"Datenbankverwaltung" auf Seite 76

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Alle	Wählen Sie diese Option, um alle Einstellungen für Applikationen und Foundations anzuzeigen.
Applikationen	Wählen Sie diese Option, um eine der BSM-Applikationen zu bearbeiten.
Beschreibung	Beschreibt die jeweilige Infrastruktureinstellung.
	Hinweis: Dieses Feld wird sowohl auf der Seite Infrastructure Settings Manager als auch im Dialogfeld Einstellung bearbeiten angezeigt, wenn
	Sie auf die Schaltfläche Einstellung bearbeiten neben der entsprechenden Einstellung klicken.
Foundation	Wählen Sie diese Option, um eine der BSM-Foundations zu bearbeiten.
Name	Der Name der Einstellung.
	Hinweis: Dieses Feld wird sowohl auf der Seite Infrastructure Settings Manager als auch im Dialogfeld Einstellung bearbeiten angezeigt, wenn
	Sie auf die Schaltfläche Einstellung bearbeiten neben der entsprechenden Einstellung klicken.
Standard	Stellt den Standardwert der Einstellung wieder her.
wiederherstellen	Hinweis: Diese Schaltfläche wird im Dialogfeld Einstellung bearbeiten
	angezeigt, wenn Sie auf die Schaltfläche Einstellung bearbeiten neben der entsprechenden Einstellung klicken.

Elemente der Oberfläche	Beschreibung
Wert	Der aktuelle Wert der jeweiligen Einstellung.
	Hinweis: Dieses Feld wird sowohl auf der Seite Infrastructure Settings Manager als auch im Dialogfeld Einstellung bearbeiten angezeigt, wenn
	Sie auf die Schaltfläche Einstellung bearbeiten neben der entsprechenden Einstellung klicken.

Kapitel 9

Audit-Protokoll

Mit dem Audit-Protokoll können Sie die verschiedenen Aktionen verfolgen, die von den Benutzern für bestimmte Kontexte im System durchgeführt wurden.

Zugriff

Wählen Sie Admin> Plattform > Setup und Verwaltung > Audit-Protokoll.

Weitere Informationen

Informationen zum Audit-Protokoll

Mit dem Audit-Protokoll können Sie die verschiedenen Aktionen verfolgen, die von den Benutzern für bestimmte Kontexte im System durchgeführt wurden.

- Warnungsverwaltung. Zeigt Aktionen in Zusammenhang mit dem Erstellen und Verwalten von Warnungen an.
- Verwaltung von CI-Status-Warnungen. Zeigt Aktionen in Zusammenhang mit dem Erstellen von Warnungsschemata für die Statuswarnung eines Konfigurationselements (Configuration Item, CI) an.
- **Daten-Collector-Verwaltung.** Zeigt Aktionen in Zusammenhang mit dem Entfernen von Business Process Monitor-Collectoren und SiteScope-Collectoren an.
- **Datenbankverwaltung.** Zeigt Aktionen in Zusammenhang mit dem Erstellen, Löschen und Ändern von Benutzern und Kennwörtern für Profildatenbanken und dem Ändern des Status des Purging Manager an.
- Gelöschte Entitäten. Zeigt Aktionen in Zusammenhang mit dem Hinzufügen und Löschen von Daten-Collectoren (Geschäftsprozessprofile, Real User Monitor-Engines und SiteScope-Monitore) in der End User Management-Verwaltung an.
- **Zeitplanung für Ausfallzeit/Ereignis.** Zeigt Aktionen in Zusammenhang mit dem Erstellen und Ändern von geplanten Ausfallzeiten/Ereignissen an.
- End User Management-Applikationen. Zeigt Aktionen in Zusammenhang mit dem Hinzufügen, Bearbeiten, Aktualisieren, Deaktivieren und Löschen von ereignisbasierten Warnungen sowie mit dem Registrieren und Aufheben der Registrierung von Warnungsempfängern an.
- IT-Umgebungskonfiguration. Zeigt Aktionen wie das Bearbeiten, Aktualisieren und Entfernen von CIs und Beziehungen an, die in der Applikation IT Universe Manager durchgeführt wurden.
- **Standortverwaltung.** Zeigt Aktionen in Zusammenhang mit dem Hinzufügen, Ändern und Löschen von Standorten an, die in der Applikation Standortverwaltung durchgeführt wurden.
- Verwaltung von Benachrichtigungsvorlagen. Zeigt Aktionen in Zusammenhang mit dem Ändern von Informationen zu offenen Tickets, Ticketeinstellungen, geschlossenen Tickets, Ticketvorlagen und Abonnementinformationen an: Benachrichtigungstypen (Standorte oder allgemeine Meldungen) und Empfänger.
- **Operationenverwaltung.** Zeigt Aktionen in Zusammenhang mit Operationenverwaltung an, z. B. Erstellen und Ändern von Content Packs, Ereignisregeln und Benachrichtigungen.
- Berechtigungsverwaltung. Zeigt alle Aktionen in Zusammenhang mit dem Zuweisen von Berechtigungen, Rollen und Berechtigungsoperationen für Ressourcen bei Benutzern und Benutzergruppen an.
- **Empfängerverwaltung.** Zeigt Aktionen in Zusammenhang mit dem Ändern von Informationen zu den Empfängern von Audit-Protokollen an.
- Verwaltung des geplanten Reports. Zeigt Aktionen in Zusammenhang mit dem Ändern der Reporting-Methode und der Zeitplanung von berichteten Ereignissen an.

- Service Health. Zeigt Aktionen in Zusammenhang mit der Service Health-Applikation an.
- **Service Health-Verwaltung**. Zeigt Aktionen in Zusammenhang mit Konfigurationen in der Service Health-Verwaltung an.
- Service Level Management-Konfiguration. Zeigt Aktionen an, die in Zusammenhang mit Vereinbarungen zum Servicelevel in der Applikation Service Level Management vorgenommen wurden.
- **SLA-Warnungsverwaltung.** Zeigt Aktionen in Zusammenhang mit dem Erstellen, Ändern oder Löschen von SLA-Warnungen an.
- **System Availability Manager.** Zeigt Aktionen in Zusammenhang mit der Systemverfügbarkeit und SiteScope an.
- **Benutzerdefinierte Reports.** Zeigt Aktionen in Zusammenhang mit dem Erstellen und Ändern von benutzerdefinierten Reports an.
- **Benutzer-/Gruppenverwaltung.** Zeigt Aktionen in Zusammenhang mit dem Hinzufügen, Ändern und Löschen von Benutzern und Benutzergruppen an.
- View Manager. Zeigt Aktionen in Zusammenhang mit KPIs an, wie Hinzufügen, Bearbeiten und Löschen von KPIs. Zeigt außerdem Aktionen in Zusammenhang mit Änderungen der Optionen KPI-Verlaufsdaten für dieses CI speichern und Änderungen überwachen an.

Aufgaben

Verwenden des Audit-Protokolls

In dieser Aufgabe wird beschrieben, wie Sie auf das Audit-Protokoll zugreifen, das auf der Seite **Audit-Protokoll** im Menü **Setup und Verwaltung** in Platform Administration zur Verfügung steht.

So verwenden Sie das Audit-Protokoll:

- Wählen Sie Admin> Plattform > Setup und Verwaltung > Audit-Protokoll. Die Seite Audit-Protokoll wird geöffnet.
- 2. Wählen Sie einen Kontext über den Kontextfilter aus.
- 3. Wählen Sie ggf. ein Profil aus der Liste. BSM aktualisiert die Tabelle mit den entsprechenden Informationen.
- 4. Klicken Sie optional auf den Link **Auditfilter**, um den Ausschnitt **Auditfilter** zu öffnen und Filterkriterien festzulegen. Folgende Filter stehen zur Verfügung:
 - **Benutzer.** Geben Sie einen Benutzer im System an, um nur die Aktionen anzuzeigen, die dieser Benutzer durchgeführt hat.
 - Enthaltener Text. Geben Sie eine Textzeichenfolge ein, die die anzuzeigende Aktion enthalten soll.
 - **Beginn nach und Ende vor.** Geben Sie einen Start- und Endzeitpunkt an, um nur die Aktionen in diesem Zeitraum anzuzeigen. Klicken Sie auf die Schaltfläche **Mehr** , um das Dialogfeld **Kalender** zu öffnen, in dem Sie ein Datum auswählen können.
- 5. Klicken Sie auf **Übernehmen**. BSM aktualisiert die Tabelle mit den entsprechenden Informationen.

Falls erforderlich können Sie mit dem Pfeil **Vorherige Seite** zur vorherigen Seite des Audit-Protokolls navigieren oder mit dem Pfeil **Nächste Seite** zur nächsten Seite des Audit-Protokolls navigieren.

Anpassen einer Protokolldatei für das Audit-Protokoll

Für das Audit-Protokoll wird das Apache-Protokollierungsdienstprogramm log4j verwendet.

Um die Protokolldatei anzupassen, müssen Sie die zugehörige Konfigurationsdatei unter **<HPBSM Stammverzeichnis>\conf\core\Tools\log4j\EJB\auditlog.properties** mithilfe der log4j-Konfigurationssyntax bearbeiten. Die Protokollebene sollte mindestens auf **Info** festgelegt sein. Der Appendername **com.mercury.topaz.tmc.bizobjects.audit.AuditManager.writeAudit** sollte nicht geändert werden.

Beschreibung der Benutzeroberfläche

Seite "Audit-Protokoll"

Auf dieser Seite können Sie die verschiedenen Aktionen verfolgen, die von Benutzern im System durchgeführt wurden.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der Oberfläche	Beschreibung	
A	Wechselt zur vorherigen oder nächsten Seite im Audit-Protokoll.	
<tabelle "audit-="" protokoll"=""></tabelle>	Zeigt den Inhalt des Audit-Protokolls an.	
<eum- Applikationen></eum- 	Wählen Sie die <eum-applikation>, für die Sie durchgeführte Aktionen anzeigen möchten.</eum-applikation>	
	Hinweis: Dieses Feld wird nur angezeigt, wenn Sie den Kontext End User Management – Applikationen ausgewählt haben.	
Auditfilter	Klicken Sie auf die Überschrift Auditfilter , um Filterkriterien festzulegen.	
Kontext	Wählen Sie den anzuzeigenden Kontext aus.	
Für Benutzer	Zeigt die Benutzer an, deren Aktionen im Audit-Protokoll angezeigt werden (entsprechend den Einstellungen im Ausschnitt Auditfilter).	
	Standardwert: Alle	
SiteScope	Wählen Sie einen SiteScope, für den Sie durchgeführte Aktionen anzeigen möchten.	
	Hinweis: Dieses Feld wird nur angezeigt, wenn Sie den Kontext System Availability Manager ausgewählt haben.	
Zeitraum	Zeigt an, für welchen Zeitraum die Aktionen im Audit-Protokoll erfasst wurden (entsprechend den Einstellungen im Ausschnitt Auditfilter).	
	Standardwert: Alle	

Ausschnitt "Auditfilter"

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
	Öffnet das Dialogfeld Kalender , in dem Sie ein Datum auswählen können.

Elemente der Oberfläche	Beschreibung	
⊗	Blendet den Ausschnitt Auditfilter ein.	
⊗	Blendet den Ausschnitt Auditfilter aus.	
Übernehmen	Wendet die ausgewählten Filter an.	
Abbrechen	Bricht das Filtern ab und schließt den Ausschnitt Auditfilter .	
Alle löschen	Löscht den Filter und zeigt alle Protokollelemente an.	
Enthaltener Text	Geben Sie hier eine Textzeichenfolge an, um alle Aktionen auszuschließen, die diese Textzeichenfolge nicht enthalten.	
Ende vor	Geben Sie hier den Zeitpunkt an, bis zu dem Sie Aktionen anzeigen möchter	
Beginn nach	Geben Sie hier den Zeitpunkt an, ab dem Sie Aktionen anzeigen möchten.	
Benutzer	Wählen Sie einen Benutzer aus, um nur die Aktionen anzuzeigen, die dieser Benutzer durchgeführt hat.	

Tabelle "Audit-Protokoll"

Wichtiger	Weitere Informationen zum Audit-Protokoll für die EUM-Warnungsverwaltung
Hinweis	finden Sie unter "Alerts Log Report" im BSM-Benutzerhandbuch.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Aktionen	Zeigt die vom angegebenen Benutzer durchgeführten Aktionen an.
Zusätzliche Informationen	Zeigt zusätzliche Informationen an, falls zutreffend.
Änderungsdatum	Zeigt Datum und Uhrzeit des Zeitpunkts an, zu dem die Aktionen durchgeführt wurden.
Geändert von:	Zeigt den Benutzer an, der die angegebenen Aktionen durchgeführt hat.

Kapitel 10

Zeitsynchronisierung bei BSM-Servern

Um sicherzustellen, dass die Uhren der BSM-Server korrekt eingestellt und synchronisiert sind, vergleichen die BSM-Server ihre Systemuhren standardmäßig alle zwanzig Minuten mit einem NTP-Server.

Standardmäßig sind mehrere NTP-Server konfiguriert, aber Sie können einen Server manuell in der Konfigurationsdatei hinzufügen:

<BSM_HOME>\conf\settings\mtime\mtime.xml

Wenn kein NTP-Server erreichbar ist, wird die Datenbankuhr für die Synchronisation verwendet.

Anzeigen der BSM-Serverzeit

Sie können die aktuelle BSM-Serverzeit über die folgenden URLs anzeigen:

So zeigen Sie die Unix-Zeit im Nur-Text-Format an:

http://<BSM_Server>/topaz/services/technical/time?alt=text/plain

Beispielergebnisse:

1314089070858

So zeigen Sie die aktuelle Zeit im XML-Format an:

http://<BSM_Server>/topaz/services/technical/time

Beispielergebnisse:

```
<entry xmlns="http://www.w3.org/2005/Atom">
<id>tid>timeService:1</id>
<title type="text" xml:lang="en">Time service.</title>
<summary type="text" xml:lang="en">The time is 2011-08-23 08:44:30,
858</summary>
<published>2011-08-23T11:44:31.382+03:00</published>
<content type="text">1314089070858</content>
</entry>
```

Das Protokoll für diese Funktion finden Sie unter:

<BSM_HOME>\logs\topaz_all.ejb.log

Kapitel 11

Arbeiten in nicht englischen Gebietsschemata

In diesem Abschnitt wird beschrieben, wie Sie BSM zum Arbeiten mit anderen Sprachen als Englisch konfigurieren, und es werden einige der Probleme erläutert, die bei Verwendung eines Zeichensatzes mit nicht lateinischen Zeichen auftreten.

Installations- und Bereitstellungsaspekte

- Wenn Sie eine CJK-Sprache in Ihrem Browser verwenden, müssen Sie sicherstellen, dass auf dem Gateway-Server mit BSM ostasiatische Sprachen installiert sind. Sie müssen auf dem Computer, auf dem der BSM-Gateway-Server installiert ist, Systemsteuerung > Regionsund Sprachoptionen > Sprachen > Dateien für ostasiatische Sprachen installieren auswählen.
- Wenn Sie BSM unter einem nicht englischen Windows-Betriebssystem installiert haben, wird die Ausgabe des Befehlszeilenwerkzeug möglicherweise nicht ordnungsgemäß angezeigt, da die Windows- und die OEM-Codeseiten voneinander abweichen. Dies trifft nicht so häufig bei asiatischen Sprachen, sondern eher bei europäischen nicht englischen Systemen zu.

Um dieses Problem zu beheben, muss die Windows-Eingabeaufforderung so konfiguriert werden, dass eine TrueType-Schriftart verwendet wird und die OEM-Codeseite der Windows-Codeseite entspricht.

Klicken Sie im Fenster der Windows-Eingabeaufforderung (Ausführen von **cmd.exe**) mit der rechten Maustaste auf die Titelleiste, wählen Sie **Eigenschaften** aus und öffnen Sie die Registerkarte **Schriftart**. Ändern Sie die Schriftart von **Rasterschriftart** in eine TrueType-Schriftart und ändern Sie ggf. den Schriftgrad (wählen Sie beispielsweise Lucida Console, 12 pt). Wenn Sie dazu aufgefordert werden, ändern Sie Verknüpfung, um die Schriftart global zu ändern.

Hinweis: Wenn Sie andere Befehlszeilenwerkzeuge wie PowerShell oder Cygwin Bash verwenden, müssen Sie die Schriftart für diese Werkzeuge separat ändern.

Um das Codeset für das System zu ändern, öffnen Sie den Registrierungs-Editor (regedit) und wechseln Sie zu: Computer\HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\Nls\CodePage. Wenn die Werte von ACP und OEMCP abweichen, stellen Sie für OEMCP dieselben Werte ein wie für ACP und starten Sie das System erneut.

Hinweis: Wenn die OEM-Codeseite nicht für das System geändert werden kann, ändern Sie den Codeseitenwert für jedes neu geöffnete Befehlszeilenfenster mithilfe des folgenden Befehls: **chcp <APC-Wert>**.

- Business Process Monitor und der Gateway-Server müssen unter einem Betriebssystem installiert werden, das dasselbe Gebietsschema aufweist wie die Daten.
- Während der Business Process Monitor-Installation können nicht lateinische Zeichen nicht für den Hostnamen und -speicherort verwendet werden. Fall notwendig, können Sie nach der Installation nicht lateinische Zeichen in den Namen aufnehmen, indem Sie Admin > End User Management > Einstellungen auswählen.
- Der Installationspfad für alle BSM-Komponenten darf keine nicht lateinischen Zeichen enthalten.
- Wenn Content Packs in mehreren Sprachen verfügbar sind, ist die Sprache der Content Packs, die automatisch während der BSM-Installation geladen wird, vom aktuellen Gebietsschema des Host-Betriebssystems abhängig. Wenn passende Content Packs für das aktuelle Gebietsschema vorliegen, werden diese installiert. Wenn das Gebietsschema nicht über

lokalisierte Content Packs verfügt, werden englische Content Packs verwendet. Später kann der Benutzer ein Content Pack in einer anderen Sprache manuell laden.

Bei jedem Start des Gateway-Servers wird der Inhalt des folgenden Verzeichnisses überprüft: <hp><hr/> <hr/> <hr/>

Beim Start dieses Servers werden alle noch nicht geladenen Pakete geladen, die keine unaufgelösten Paketabhängigkeiten beinhalten (d. h. Verweise auf Pakete, die weder bereits geladen wurden noch sich im selben Ordner befinden).

Anschließend wird folgendes Verzeichnis überprüft: <**HP BSM-Stammverzeichnis**>/conf/opr/content/en_US

Jetzt werden alle Content Packs hochgeladen, die nicht aus dem ersten Speicherort hochgeladen wurden. Dies kann dazu führen, dass der Inhalt in einer Mischung aus verschiedenen Sprachen vorliegt.

Die Pakete werden im Standardimportmodus geladen, wobei bereits vorhandene Artefakte unverändert beibehalten werden. Es werden lediglich neue Artefakte hinzugefügt.

Hinweis: Der Fortschritt lässt sich in der Protokolldatei des Back-Ends für die Administration verfolgen. Der Vorgang wird im Hintergrund ausgeführt und ist möglicherweise aktiv, während sich ein Benutzer anmeldet. Das System verhindert, dass mehrere Inhaltspakte gleichzeitig geladen werden.

Probleme der Datenbankumgebung

- Um in einer BSM-Umgebung in einer Sprache zu arbeiten, in der keine lateinischen Zeichen verwendet werden, können Sie entweder eine Oracle Server-Datenbank oder eine Microsoft SQL Server-Datenbank verwenden. Wenn Sie eine Microsoft SQL Server-Datenbank verwenden, sollte dieselbe Codierung verwendet werden wie in den BSM-Servern. Wenn Sie eine Oracle Server-Datenbank verwenden, kann auch eine UTF-8- oder AL32UTF-8-Codierung verwendet werden, die Sprachen mit nicht lateinischen Zeichen sowie die Option für mehrere Sprachen unterstützt. Eine Liste der unterstützten und getesteten Datenbankserver finden Sie unter Systemanforderungen für BSM und Matrizes für die BSM-Unterstützung.
- Wenn Sie in einer Oracle-Datenbank eine neue Instanz erstellen, müssen Sie den Zeichensatz für die Instanz angeben. Sämtliche Zeichendaten, einschließlich der Daten im Datenwörterbuch, werden in dem Zeichensatz der Instanz gespeichert. Weitere Informationen zum Arbeiten mit Oracle-Datenbanken finden Sie unter "Deploying and Maintaining the Oracle Server Database" im BSM Database Guide. Informationen zu unterstützten und zertifizierten Oracle-Zeichensätzen finden Sie in der "Oracle Summary Checklist" im BSM Database Guide.
- Der SiteScope-Datenbankabfrage-Monitor kann eine Verbindung zu einer Oracle-Datenbank herstellen, sofern die Oracle-Benutzernamen und -Kennwörter ausschließlich lateinische Zeichen enthalten.

Verwaltungsprobleme

- E-Mail-Warnungen, die mit ISO-2022-JP kodiert sind, werden nur von SMTP-Servern unterstützt, die auf einer Windows-Plattform ausgeführt werden. Die Verwendung dieser Codierung wirkt sich auf alle BSM-Server aus.
- Bei Verwendung der standardmäßigen Authentifizierungsmethode Lightweight SSO für die Authentifizierung von Benutzern, die sich bei BSM anmelden, können die Benutzernamen und Kennwörter aus nichtlateinischen Zeichen bestehen.
- Damit nichtlateinische Zeichen in BSM-Datenbanken unterstützt werden, muss die Codierung für Datenbanken als UTF-8 oder AL32UTF-8 (nur Oracle) definiert sein oder auf die spezifische Sprache festgelegt sein.
- Damit nichtlateinische Zeichen in Protokolldateien unterstützt werden, muss die Codierungseigenschaft log4j für die log4j-Konfigurationsdateien entsprechend festgelegt werden.

Um eine bestimmte Protokolldatei mit UTF-8 zu kodieren, gehen Sie wie folgt vor:

- Suchen Sie in der log4j-Konfiguration unter conf/core/Tools/log4j nach dem Namen der Protokolldatei.
- Fügen Sie in der Eigenschaftendatei, in der diese Protokolldatei definiert ist, folgende Eigenschaft hinzu:

log4j.appender.<Appendername>.Encoding=UTF-8

Beispiel für die Konfiguration von jboss_server.log:

Probleme in Service Health

Möglicherweise müssen Sie mehrere Schritte ausführen, um die Anzeige von nicht lateinischen Zeichen in der Service Health-Topologie-Ansicht zu aktivieren.

So zeigen Sie nicht lateinische Zeichen in der Service Health-Topologie-Ansicht an:

- Überprüfen Sie, ob Sie die Anleitungen beim Installieren von JRE auf einem nicht westlichen Windows-System beachtet haben. Die Anleitungen finden Sie unter Sun Microsystems site (http://java.sun.com/j2se/1.5.0/jre/install-windows.html).
- 2. Stellen Sie Folgendes sicher:
 - Sie haben Administratorberechtigungen für die Installation von J2SE Runtime Environment unter Microsoft Windows 2000 und XP.
 - (Benutzer, die JRE auf nicht westlichen 32-Bit-Computern installieren:) Wählen Sie den benutzerdefinierten Setuptyp aus. Wählen Sie im benutzerdefinierten Setup unter der zweiten Option (Unterstützung für weitere Sprachen) die Option zur Installation auf der lokalen Festplatte aus.
- 3. Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus, klicken Sie auf Applikationen, wählen Sie Service Health-Applikation und ermitteln Sie den Eintrag Name der Schriftart in der Topologie-Ansicht in der Tabelle Service Health-Applikation - Eigenschaften der Topologie-Ansicht. Ändern Sie den Wert in Arial Unicode MS.

Achtung: Wurde der Wert für den Eintrag Name der Schriftart in der Topologie-Ansicht auf Default gesetzt, müssen Sie diesen Schritt nicht durchführen, da für Name der Schriftart in der Topologie-Ansicht in diesem Fall automatisch der Wert Arial Unicode MS vorausgesetzt wird.

- Schließen Sie alle Instanzen des Webbrowsers.
- 5. Melden Sie sich bei BSM an und öffnen Sie die Service Health-Topologie-Ansicht. Überprüfen Sie, ob die chinesischen oder japanischen Zeichen jetzt ordnungsgemäß angezeigt werden.

Probleme mit Service Level Management

Service Level Management unterstützt keine Servicenamen, die mehr als 50 Multibyte-Zeichen enthalten.

Reportprobleme

- BSM unterstützt keine Namen für benutzerdefinierte Reports, die mehr als 50 Multibyte-Zeichen enthalten.
- Der Report über Seiten mit Komponentenaufschlüsselung unterstützt keine URLs, die Multibyte-Zeichen enthalten. Bei der Angabe einer URL und eines Speicherorts für die Ausführung der Aufschlüsselung müssen Sie lateinische Zeichen in das URL-Feld eingeben.
- Excel-Reports müssen beim Hochladen in BSM unter einem Betriebssystem in vereinfachtem Chinesisch Dateinamen in lateinischen Buchstaben haben. Wählen Sie zum Anzeigen von Excel-Reports Applikationen > Benutzerreports > Report Manager.
- Reports, die aus BSM in Excel heruntergeladen wurden, können auf einem Betriebssystem mit einer anderen Sprache als der Datensprache nicht ordnungsgemäß angezeigt werden.
 - Wenn BSM auf einem englischsprachigen Computer installiert ist, müssen Sie zum Herunterladen von Excel-Dateien mit Multibyte-Daten im Eintrag **user.encoding** in der Datei **<HPBSM-Stammverzeichnis>\AppServer\resources\strings.properties** die entsprechende Codierung festlegen.

Business Process Monitor-Probleme

- Sollten die Business Process Monitor (BPM)-Protokolldateien Daten mit nicht lateinischen Zeichen enthalten, müssen Sie diese in einem Anzeigeprogramm öffnen, das UTF-8-Parsing unterstützt, wie beispielsweise der Editor, und nicht im Fenster BPM-Dateien anzeigen aus der BPM Admin-Konsole.
 - Protokolldateien, die in der Standardcodierung des Servers gespeichert werden, auf dem die BPM Admin-Konsole installiert ist, werden korrekt im Fenster **BPM-Dateien anzeigen** angezeigt.
- Sämtliche BPM-Instanzen (Applikation, Skripts, Parameter usw.) sollten nur mit lateinischen Zeichen oder Zeichen des BPM-Servers benannt werden.

Probleme mit SiteScope

- In internationalen SiteScope-Versionen (die mehrsprachige Zeichensätze unterstützen) gibt der bei der Erstellung des Monitorsatzes angezeigte Link **Zurück zu Gruppe** den indexbasierten Gruppennamen an (zum Beispiel **group0**) und nicht den benutzerdefinierten Gruppennamen.
- Der Datenbankabfrage-Monitor kann nur eine Verbindung zu einer Oracle-Datenbank herstellen, sofern die Oracle-Benutzernamen und -Kennwörter ausschließlich lateinische Zeichen enthalten.
- SiteScope unterstützt nicht lateinische Zeichen im Benutzemamen/Kennwort.
- Die Benutzeroberfläche kann in mehreren Sprachen angezeigt werden. Weitere Informationen finden Sie unter "Verwenden von SiteScope in einer Internationalisierungsumgebung (I18N)" in der SiteScope-Hilfe.
- Eine Liste der für die Internationalisierung getesteten Monitore finden Sie unter "Für Internationalisierung unterstützte Monitore" in der SiteScope-Hilfe.

Probleme mit Real User Monitor

- Real User Monitor unterstützt nichtlateinische Zeichen im UTF-8-Format. Weitere Informationen zum Konfigurieren der HPReal User Monitor-Probe für die Unterstützung von Nicht-Unicode-Codierungen finden Sie unter "Configuring the HP Real User Monitor Probe for I18N" im Real User Monitor Administration Guide
- Damit nichtlateinische Zeichen aus Real User Monitor unterstützt werden, muss die Codierung für BSM-Datenbanken als UTF-8 definiert oder auf die spezifische Sprache festgelegt sein.
 Weitere Informationen finden Sie unter "Probleme der Datenbankumgebung" auf Seite 128.
- Die Windows-Installationsbildschirme der Real User Monitor-Probe sind nicht übersetzt und nur auf Englisch verfügbar. Weitere Informationen zum Installieren der Real User Monitor-Probe finden Sie unter "Installing the HP Real User Monitor Probe" im Real User Monitor Administration Guide.

Probleme bei der Endbenutzerverwaltung

- Das globale Ersetzen kann nicht in Sprachen mit nicht lateinischen Zeichen durchgeführt werden.
- Wenn Sie auf die Status-Baseline in End User Management zugreifen (Applikationen > End
 User Management > Status-Baseline), werden bestimmte Zeichen unleserlich angezeigt. Sie
 lösen dieses Problem, indem Sie wie folgt sicherstellen, dass Sie die Dateien für die
 ostasiatischen Sprachen auf Ihrem Computer installiert sind:

Wählen Sie Start > Systemsteuerung > Regions- und Sprachoptionen > Sprachen > Dateien für ostasiatische Sprachen installieren aus.

Probleme mit der Datenflussverwaltung

Beim Exportieren einer CI-Instanz in eine PDF-Datei werden japanische Zeichen nicht in der PDF-Datei angezeigt. (**Datenflussverwaltung > Discovery-Systemsteuerung > Basismodus**. Führen Sie die Discovery aus. Nach dem Ausführen der Discovery wählen Sie einen CIT im Ausschnitt **Statistikergebnisse** aus. Klicken Sie auf die Schaltfläche **Instanzen anzeigen**. Wählen Sie im Dialogfeld **Discovery durch > Daten in Datei exportieren > Daten in PDF-Datei exportieren** aus.)

Probleme bei mehreren Sprachen

- Die SNMP-Benachrichtigungsmethode unterstützt keinen mehrsprachigen Text und kann eine Benachrichtigung nur im Zeichensatz des Gateway-Servercomputers senden. Dies liegt daran, dass BSM SNMP-Version 1.0 verwendet, die keine Unterstützung für mehrsprachige Daten bietet.
- Fehlermeldungen im Report Fehlgeschlagene Transaktionen werden nicht richtig angezeigt, wenn BSM auf einem englischen und Business Process Monitor auf einem japanischen Betriebssystem ausgeführt wird. Für den Zugriff auf den Report Fehlgeschlagene Transaktionen wählen Sie Applikationen > End User Management > Geschäftsprozesse > Fehlerübersicht. Suchen Sie nach der Tabelle Allgemeine Fehler und klicken Sie auf einen Link, um das Fenster Fehlgeschlagene Transaktionen zu öffnen.
- BSM kann mehrsprachige Daten speichern. Eine reguläre ausführbare Datei kann im Allgemeinen jedoch keine mehrsprachigen Daten in der Befehlszeile akzeptieren.

In der folgenden Tabelle werden die Verfahren erläutert, die Sie durchführen müssen, um mehrsprachige Daten zur Befehlszeile hinzuzufügen, wenn Sie bei einer Warnung eine ausführbare Datei ausführen:

Plattform	Verfahren
Windows	Um zu verhindern, dass mehrsprachige Daten verloren gehen, schreiben Sie die Applikation mit einer wmain- statt einer main-Funktion. Sie können auch eine andere Funktion vom Typ "main" verwenden, die Befehlszeilenparameter vom Typ "wchar" statt vom Typ "char" akzeptiert.
	Hinweis: Wenn Sie die Befehlszeilenoption SubAlerts verwenden, enthält die erstellte XML-Datei kein Codierungsattribut und die Codierung entspricht nicht der UTF-8-Standardcodierung.
Solaris	Informieren Sie den Autor der Applikation, dass die an die Applikation übergebenen Parameter im UTF-8-Format codiert werden müssen.

Weitere Informationen zum Verwenden einer benutzerdefinierten Befehlszeile beim Ausführen einer ausführbaren Datei bei einer Warnung finden Sie unter "Run Executable File Dialog Box" im BSM Application Administration Guide.

• Ausführbare Dateien, die für eine vorherige Version von BSM erstellt wurden, sind mit einer mehrsprachigen Version kompatibel.

Unterstützung für die mehrsprachige Benutzeroberfläche

Die BSM-Benutzeroberfläche kann in den folgenden Sprachen in Ihrem Webbrowser angezeigt werden:

Sprache	Spracheinstellung im Webbrowser
Englisch	Englisch
Französisch	Französisch (Frankreich) [fr]
Japanisch	Japanisch [ja]
Koreanisch	Koreanisch [ko]
Vereinfachtes Chinesisch	Chinesisch (China) [zh-cn]

Folgende Sprachen werden zwar von BSM unterstützt, aber nur die Run-time Service Model (RTSM)-bezogenen Seiten werden in diesen Sprachen dargestellt.

Sprache	Spracheinstellung im Webbrowser
Niederländisch	Niederländisch (Niederlande) [nl]
Deutsch	Deutsch (Deutschland) [de]
Portugiesisch	Portugiesisch (Brasilien) [pt-br]
Russisch	Russisch [ru]
Spanisch	Spanisch [es]
Italienisch	Italienisch (Italien) [it]

Mithilfe der Spracheinstellungsoption in Ihrem Browser können Sie festlegen, wie BSM angezeigt werden soll. Die Spracheinstellung wirkt sich nur auf den lokalen Computer (den Clientcomputer) aus, nicht auf den BSM-Computer oder auf andere Benutzer, die auf denselben BSM-Computer zugreifen.

So konfigurieren und verwenden Sie BSM in einer bestimmten Sprache:

- Installieren Sie die Schriftarten der gewünschten Sprache auf Ihrem lokalen Computer, sofern diese nicht bereits installiert sind. Wenn Sie eine Sprache in Ihrem Webbrowser wählen, deren Schriftarten nicht installiert sind, zeigt BSM Quadrate statt Zeichen an.
- 2. Wenn Sie bei BSM angemeldet sind, müssen Sie sich zunächst abmelden. Klicken Sie oben im BSM-Fenster auf **Abmelden**.
 - Schließen Sie alle geöffneten Browserfenster, oder löschen Sie den Cache (sofern BSM im Internet Explorer ausgeführt wird).
- 3. Wenn BSM im Internet Explorer ausgeführt wird, wählen Sie im Webbrowser auf Ihrem lokalen

Computer die Sprache aus, in der BSM angezeigt werden soll (Extras > Internetoptionen).

- a. Klicken Sie auf die Schaltfläche **Sprachen**, und wählen Sie im Dialogfeld **Spracheinstellung** die Sprache aus, in der BSM angezeigt werden soll.
- b. Wenn die gewünschte Sprache nicht im Dialogfeld angezeigt wird, müssen Sie auf Hinzufügen klicken, um die Liste der Sprachen anzuzeigen. Wählen Sie die hinzuzufügende Sprache aus, und klicken Sie auf OK.
- c. Klicken Sie auf **Nach oben**, um die ausgewählte Sprache in die erste Zeile zu verschieben.
- d. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
- e. Zeigen Sie das BSM-Anmeldefenster an.
- f. Klicken Sie im Internet Explorer-Menü auf Ansicht > Aktualisieren. BSM wird aktualisiert, und die Benutzeroberfläche wird in der ausgewählten Sprache angezeigt.

Hinweis: Weitere Informationen zum Anzeigen von Webseiten in Internet Explorer, die in einer anderen Sprache verfasst sind, finden Sie unter Anpassen der Anzeige von Webseiten (http://support.microsoft.com/kb/306872/en-us).

- 4. Wenn Sie BSM in Firefox verwenden, konfigurieren Sie den Webbrowser auf Ihrem lokalen Computer folgendermaßen:
 - a. Wählen Sie **Extras > Einstellungen > Erweitert** aus. Klicken Sie auf die Schaltfläche zum Bearbeiten der Sprache. Das Dialogfeld **Sprachen** wird geöffnet.
 - b. Wählen Sie die Sprache aus, in der BSM angezeigt werden soll.
 - Ist die gewünschte Sprache nicht im Dialogfeld enthalten, erweitern Sie die Liste **Wählen** Sie eine Sprache zum Hinzufügen aus..., wählen Sie die Sprache aus, und klicken Sie auf Hinzufügen.
 - Klicken Sie auf Nach oben, um die ausgewählte Sprache in die erste Zeile zu verschieben.
 - d. Klicken Sie auf **OK**, um die Einstellungen zu speichern. Klicken Sie auf **OK**, um das Dialogfeld **Sprache** zu schließen.

Hinweise und Einschränkungen

- Es gibt keine Sprachpaketinstallation. Alle übersetzten Sprachen sind in die mehrsprachige Benutzeroberfläche (Multilingual User Interface, MLU) von BSM integriert.
- Eingegebene Daten behalten ihre ursprüngliche Sprache bei, auch wenn die Sprache des Webbrowsers geändert wird. Eine Änderung der Sprache des Webbrowsers auf Ihrem lokalen Computer wirkt sich nicht auf die Sprache von Daten aus, die von Benutzern eingegeben wurden.
- Sie k\u00f6nnen kein Package bereitstellen, wenn sich das Servergebietsschema vom Client-Gebietsschema unterscheidet und der Package-Name nichtlateinische Zeichen enth\u00e4lt.
 Weitere Informationen finden Sie unter "Package Manager" im RTSM Administration Guide.
- Sie können kein Package erstellen, das Ressourcen (z. B. Ansichten und TQLs) mit

nichtlateinischen Zeichen im Namen enthält, wenn sich das Servergebietsschema vom Client-Gebietsschema unterscheidet. Weitere Informationen finden Sie unter "Package Creation and Deployment in a Non-English Locale" im RTSM Administration Guide.

- In Modeling Studio k\u00f6nnen Sie keine neue Ansicht erstellen, wenn der Name der Ansicht mehr als 18 japanische Zeichen enth\u00e4lt. Weitere Informationen zum Erstellen neuer Ansichten finden Sie unter "Modeling Studio" im Modellierungshandbuch.
- In der Standortverwaltung werden alle geographischen Standorte unabhängig von der Sprache der Benutzeroberfläche auf Englisch angezeigt. Logische Standorte können in einer beliebigen ausgewählten Sprache benannt werden und bleiben in dieser Sprache, auch wenn die Sprache der Benutzeroberfläche später geändert wird.
- Die HTML-Seite mit dem BSM-Serverstatus wird nur auf Englisch angezeigt. Sie steht nicht in anderen Sprachen zur Verfügung. Details finden Sie unter "Nach der Bereitstellung" im BSM-Installationshandbuch.

Kapitel 12

BSM-Protokolle

Hinweis: Dieses Kapitel ist nicht für HP Software-as-a-Service-Kunden relevant.

BSM zeichnet die Verfahren und Aktionen, die von den verschiedenen Komponenten durchgeführt werden, in Protokolldateien auf. Protokolldateien haben den Zweck, den HP Software-Unterstützung unterstützen, falls BSM nicht wie erwartet ausgeführt werden kann.

Der standardmäßige Schweregradschwellenwert für Protokolldateien ist je nach Protokoll unterschiedlich, ist aber meistens auf **Warnung** oder **Fehler** eingestellt. Eine Definition dieser Protokollebenen finden Sie unter "Protokolle – Schweregrade " auf Seite 144.

Sie können die Protokolldateien mit einem beliebigen Texteditor anzeigen.

Speicherorte der Protokolldateien

Die meisten Protokolldateien befinden sich im Verzeichnis <**HPBSM-Stammverzeichnis>**\log und in Unterverzeichnissen, die nach Komponenten organisiert sind.

Die Protokolldateieigenschaften sind in Dateien im folgenden Verzeichnis und seinen Unterverzeichnissen definiert: <h >HPBSM-Stammverzeichnis>\conf\core\Tools\log4j.

Speicherorte der Protokolldateien in einer verteilten Umgebung

In Installationen mit einem Computer oder in kompakten Installationen befinden sich alle BSM-Server und ihre Protokolle auf demselben Computer. Im Falle einer verteilten Bereitstellung der Server auf mehreren Computern werden Protokolle für einen bestimmten Server im Allgemeinen auf dem Computer gespeichert, auf dem der Server installiert ist. Falls Sie jedoch Protokolle prüfen müssen, sollten Sie dies auf allen Computern tun.

Beim Vergleich von Protokollen auf Clientcomputern mit denen auf den BSM-Servercomputern beachten Sie, dass das in einem Protokoll aufgezeichnete Datum und die Uhrzeit von dem Computer stammen, auf dem das Protokoll erstellt wurde. Falls also ein Zeitunterschied zwischen Server- und Clientcomputer vorliegt, wird dasselbe Ereignis von beiden jeweils mit unterschiedlichem Zeitstempel erfasst.

Protokolle – Schweregrade

Jedes Protokoll ist so eingestellt, dass die von ihm erfassten Informationen einem bestimmten Schweregrad-Schwellenwert entsprechen. Weil die verschiedenen Protokolle dazu dienen, verschiedene Informationen zu erfassen, ist jedes bei der Protokollierung auf die entsprechende Standardebene eingestellt. Weitere Informationen zum Ändern der Protokollebene finden Sie unter "Ändern der Protokollebenen" auf Seite 147.

Die typischen Protokollebenen werden nachfolgend aufgeführt, von der am engsten bis zu der am weitesten gefassten Ebene:

- **Fehler.** Das Protokoll erfasst nur Ereignisse, die sich negativ auf die unmittelbare Ausführung von BSM auswirken. Wenn es zu einem Fehler kommt, können Sie überprüfen, ob Fehlermeldungen protokolliert wurden und deren Inhalt prüfen, um die Quelle des Fehlers ausfindig zu machen.
- Warnung. Das Protokoll beinhaltet neben Ereignissen auf Fehlerebene Probleme, die BSM derzeit kompensieren kann sowie Vorfälle, die registriert werden sollten, um zukünftige Fehler zu verhindern.
- Info. Das Protokoll erfasst alle Aktivitäten. Meistens handelt es sich um wenig hilfreiche Routineinformationen und die Protokolldatei ist sehr schnell gefüllt.
- **Debugging.** Diese Ebene wird von HP Software-Unterstützung für die Fehlerbehebung verwendet.

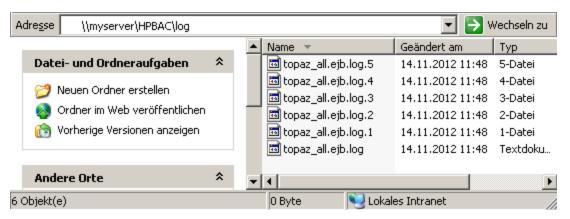
Hinweis: Die Namen der verschiedenen Protokollebenen können je nach Server und Verfahren leicht variieren. So kann **Info** auch **Immer protokolliert** oder **Ablauf** heißen.

Protokolldateigröße und automatische Archivierung

Für jeden Protokolldateityp wird ein Größenlimit festgelegt. Sobald eine Datei dieses Limit erreicht, wird sie umbenannt und als Protokoll archiviert. Dann wird eine neue aktive Protokolldatei erstellt.

Bei vielen Protokollen kann die Anzahl archivierter Protokolldateien konfiguriert werden. Sobald eine Datei ihr Größenlimit erreicht, wird sie mit der nummerierten Erweiterung 1 umbenannt. Wenn aktuell ein archiviertes Protokoll mit der Erweiterung 1 vorliegt, wird dieses mit der Erweiterung 2 umbenannt, log.2 wird log.3 usw., bis die älteste archivierte Protokolldatei (deren Nummer die maximale Anzahl zu speichernder Dateien angibt) dauerhaft gelöscht wird.

Die folgende Abbildung zeigt als Beispiel eine Protokolldatei namens **topaz_all.ejb.log** mitsamt ihren archivierten Kopien:



Die maximale Dateigröße sowie die Anzahl archivierter Protokolldateien sind in den Protokolleigenschaftsdateien in **<HPBSM-Stammverzeichnis >\conf\core\Tools\log4j** definiert. Beispiel:

def.file.max.size=2000KB def.files.backup.count=10

JBoss- und Tomcat-Protokolle

Im folgenden Verzeichnis **<HPBSM-Stammverzeichnis>\log** sind die JBoss- und Tomcat-Protokolldateien enthalten:

- **jboss_boot.log.** Protokolliert Startaktivitäten wie das Ausführen des JBoss-Prozesses, die Bereitstellung und den Startstatus sowie die Anzahl der belegten Ports.
- jboss_server.log. Protokolliert alle JBoss-Aktivitäten wie JBoss-Meldungen, Bereitstellung und Startstatus.
- jboss_tomcat.log. Protokolliert die Tomcat-Meldungen.

Hinweis: Sie können die JMX-Konsole unter http://<HPBSM-Server>:8080/jmx-console anzeigen.

Ändern der Protokollebenen

In dieser Aufgabe und dem verbundenen Prozessdiagramm wird die Einrichtung eines Systems für die Bereitstellung von Warnungen für Empfänger beschrieben.

Möglicherweise werden Sie vom HP Software-Unterstützung aufgefordert, den Schwellenwert für den Schweregrad in einem Protokoll, beispielsweise auf die Debug-Ebene, zu ändern.

So ändern Sie den Schwellenwert für den Schweregrad:

- Öffnen Sie die Datei mit Protokolleigenschaften in einem Texteditor. Die Protokolldateieigenschaften sind in Dateien im folgenden Verzeichnis definiert: <HPBSM-Stammverzeichnis>\conf\core\Tools\log4j.
- 2. Suchen Sie den Parameter loglevel. Beispiel:

loglevel=ERROR

3. Ändern Sie die Ebene wie gewünscht. Beispiel:

loglevel=DEBUG

4. Speichern Sie die Datei.

Aktivieren der Debugablaufprotokollierung für ein Ereignis

Die Debugablaufprotokollierung für ein Ereignis kann durch Festlegen des benutzerdefinierten Attributs __TRACE__ aktiviert werden. Es kann einen beliebigen Wert aufweisen. Dadurch werden Protokolle für die Flussablaufverfolgung auf der Ebene INFO für dieses Ereignis erstellt.

Die Festlegung erfolgt auf dem HPOM-Server oder dem Agent, der das Ereignis sendet. Das Attribut kann auch zu einem späteren Zeitpunkt dem Ereignis hinzugefügt werden. Wenn dieses benutzerdefinierte Attribut für ein Ereignis festgelegt wird, wird die Ablaufverfolgungsausgabe für dieses Ereignis in den Ablaufprotokollen angezeigt:

- BSM-Datenverarbeitungsserver: log/opr-backend/opr-flowtrace-backend.log
- BSM-Gateway-Server: log/opr-gateway/opr-flowtrace-gateway.log

Standardmäßig ist die Protokollierungsebene für die Ereignisfluss-Ablaufverfolgung auf INFO festgelegt. Nur Ereignisse, für die das benutzerdefinierte Attribut __TRACE__ festgelegt ist, werden in den Protokolldateien für die Flussablaufverfolgung erfasst. Um die Flussablaufverfolgung für alle Ereignisse zu aktivieren, legen Sie die Protokollebene für die Flussablaufverfolgung auf DEBUG fest.

Protokollierungsadministrator

Dieses Werkzeug ermöglicht es Ihnen, den in BSM-Protokollen angezeigten Detaillierungsgrad vorübergehend zu ändern und benutzerdefinierte Protokolle zu erstellen. Verwenden Sie zum Öffnen des BSM-Protokollierungsadministrators folgende URL:

http://<BSM-Gateway-Server>/topaz/logAdminBsm.jsp

Kapitel 13

Portverwendung

In diesem Abschnitt wird beschrieben, wie die von BSM verwendeten Ports konfiguriert werden.

Manuelles Ändern von Ports

Dieser Abschnitt enhält Informationen zum manuellen Ändern der verschiedenen Ports. Das Verfahren ist für jeden Port anders.

Manuelles Ändern von Port 80

Port 80 wird vom BSM-Webserver verwendet. Zum Ändern dieses Ports müssen Sie andere Komponenten auf dem BSM-Server neu konfigurieren und BSM neu starten.

- 1. Ändern der Einstellungen des virtuellen Gateway-Servers

 - b. Ändern Sie den URL des virtuellen Gateway-Servers für Applikationsbenutzer in http://<Servername>:<Neuer Port>.
 - c. Ändern Sie den URL des virtuellen Gateway-Servers für Datenerfassungsinstanzen in http://<Servername>:<Neuer Port>.
- 2. Ändern der Einstellungen des direkten Gateway-Servers
 - ändern Sie in derselben Tabelle den URL des direkten Gateway-Servers für Applikationsbenutzer, sodass dieser den neuen Port enthält.
 - b. Ändern Sie den URL des direkten Gateway-Servers für Datenerfassungsinstanzen, sodass dieser den neuen Port enthält.
- 3. Ändern der Einstellungen des lokalen virtuellen Gateway-Servers
 - ändern Sie in derselben Tabelle die URL des lokalen virtuellen Gateway-Servers für Applikationsbenutzer, sodass dieser den neuen Port enthält.
 - b. Ändern Sie die URL des lokalen virtuellen Gateway-Servers für Datenerfassungsinstanzen, sodass dieser den neuen Port enthält.
- 4. Ändern der URL zum Öffnen von BSM
 - a. Stellen Sie eine Remoteverbindung zum BSM-Gateway-Server her und wählen Sie Start >
 Alle Programme > HP Business Service Management.
 - b. Klicken Sie mit der rechten Maustaste auf **HP Business Service Management öffnen** und wählen Sie **Eigenschaften**.
 - c. Ändern Sie auf der Registerkarte **Webdokument** das Feld **URL** wie folgt: **http://<Gateway Server>:<Neuer Port>/topaz**.
- 5. Ändern der Webservereinstellungen

Ändern Sie die Webservereinstellungen. Dieses Verfahren variiert je nach Windows-Version und Webservertyp. Sie sollten alle auf dem BSM-Gateway-Server durchgeführt werden. Nachfolgend finden Sie Beispiele für Windows Server 2008 mit drei verschiedenen Webservern:

Für IIS 6.0 mit Windows Server 2008:

- a. Klicken Sie im Internetdienste-Manager von Microsoft IIS mit der rechten Maustaste auf Standardwebsite und wählen Sie Eigenschaften
- b. Ändern Sie auf der Registerkarte **Website** das Feld **TCP-Port** wie folgt:

Für IIS 7.x mit Windows Server 2008:

- a. Öffnen Sie das Tool **Computerverwaltung** von Microsoft, indem Sie mit der rechten Maustaste auf **Arbeitsplatz** klicken und **Verwalten** auswählen.
- b. Blenden Sie Rollen > Webserver ein und wählen Sie Internet-Informationsdienste.
- c. Im rechten Bereich können Sie den IIS-Manager sehen. Blenden Sie im linken Teil dieses Bereichs (Verbindungen) die Verbindung des aktuellen Computers und den Knoten Sites ein.
- d. Klicken Sie mit der rechten Maustaste auf **Standardwebsite** und klicken Sie dann auf **Bindungen bearbeiten**.
- e. Wählen Sie die Verbindung aus, die Port 80 abhört, und klicken Sie auf **Bearbeiten**, um den Wert auf den neuen Port zu ändern.

Für Apache mit Windows Server 2008:

- a. Öffnen Sie die Datei **SSM-Gateway-StammverzeichnisWebServerconfhttpd.conf** in einem Texteditor.
- b. Wechseln Sie zu der Zeile, die mit **Listen** beginnt, und ändern Sie den Portwert nach Bedarf.
- Wechseln Sie zu der Zeile, die mit ServerName beginnt, und ändern Sie den Portwert nach Bedarf.
- 6. Neustarten aller BSM-Server und Aktualisieren der Datenerfassungen

Starten Sie alle BSM-Server neu und aktualisieren Sie alle Datenerfassungen, die vor dem Ändern des Ports konfiguriert wurden (z. B. RUM, BPM, SiteScope). Ändern Sie die Adresse des Gateway-Servers in der jeweiligen Datenerfassung wie folgt, um den neuen Port zu berücksichtigen: **BSM-Gateway>:<Neuer Port>**.

Manuelles Ändern der Ports 1433 und 1522

Diese Ports steuern die Kommunikation zwischen BSM- und Datenbankservern von HP.

1. Ändern Sie den Management-Datenbank-Port.

Führen Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration aus. Wechseln Sie zu dem Bildschirm, auf dem der Management-Datenbank-Port angegeben ist, und ändern Sie diesen nach Bedarf. Weitere Informationen zum Dienstprogramm für die Setup- und Datenbankkonfiguration finden Sie im BSM-Installationshandbuch.

Hinweis: Sie können dieses Verfahren auch wie folgt manuell durchführen: Öffnen Sie auf allen BSM-Servern (Gateway und DPS) **<BSM-Basisverzeichnis>\conf\TopazInfra.ini** in einem Texteditor und ändern Sie die Eigenschaft **dbPort** nach Bedarf.

2. Ändern Sie den Profildatenbank-Port.

Navigieren Sie zu **Admin > Plattform > Setup und Verwaltung > Profildatenbanken verwalten** und klicken Sie auf die Schaltfläche **Datenbankeigenschaften bearbeiten**, damit der neue Port in der gewünschten Datenbankkonfiguration berücksichtigt wird.

3. Starten Sie alle BSM-Server neu.

Eingehender BSM-Datenverkehr

Hinweis: Bei den hier aufgeführten Ports handelt es sich um die von BSM verwendeten Ports. Wenn Sie eine Portzuweisung ändern müssen, sollten Sie sich unbedingt zuerst an den HP Software-Unterstützung wenden.

Es gibt zwei Kategorien von eingehendem BSM-Datenverkehr:

Interner Datenverkehr

Der interne Datenverkehr ist der Datenverkehr zwischen zwei BSM-Servern. In der folgenden Tabelle sind die Ports aufgeführt, die für die Übertragung von Daten zwischen zwei BSM-Servern verwendet werden:

Portnummer	BSM-Server, die den Port abhören	Portverwendung
4444	Gateway-Server, Server für die Datenverarbeitung	RMI-Kanal (Remote Method Invocation, Remote- Methodenaufruf) zwischen BSM-Servern
4445	Gateway-Server, Server für die Datenverarbeitung	RMI-Kanal zwischen BSM-Servem
9389	Gateway-Server	Lokale TCP-LDAP-Verbindung für die Kommunikation zwischen Gateway-Servern in einer verteilten Bereitstellungsumgebung
2506	Server für die Datenverarbeitung	Busdomänen-Manager für die Verbindung zwischen dem Server für die Datenverarbeitung und dem Gateway- Server
2507	Gateway-Server, Server für die Datenverarbeitung	Hauptbusprozesse für die Verbindung zwischen BSM- Servern
383	Gateway-Server, Server für die Datenverarbeitung	Ereignisse die von Operations Manager bei der Operations Management-Applikation eingehen

Externer Datenverkehr

Externer Datenverkehr ist der Datenverkehr, der von einem Client, bei dem es sich nicht um einen BSM-Server handelt, auf einen der BSM-Server gelangt. In der folgenden Tabelle sind die Ports aufgeführt, die für die Übertragung von Daten von einem externen BSM-Clientcomputer an einen BSM-Server verwendet werden:

Portnummer	BSM-Server, die den Port abhören	Portverwendung
80/443	Gateway-Server	80. HTTP/S-Kanal für die Applikationen auf dem Gateway-Server
		443. Port für den Reverse-Proxy

Ausgehender BSM-Datenverkehr

Hinweis: Bei den hier aufgeführten Ports handelt es sich um die von BSM verwendeten Ports. Wenn Sie eine Portzuweisung ändern müssen, sollten Sie sich unbedingt zuerst an den HP Software-Unterstützung wenden.

In der folgenden Tabelle sind die Ports aufgeführt, die von BSM-Servern für Verbindungen mit externen Servern (keine BSM-Server) verwendet werden:

Portnummer	BSM-Server, die eine Verbindung mit dem Port herstellen	Portverwendung
25	Gateway-Server, Server für die Datenverarbeitung	SMTP-Kanal für die Verbindung zwischen BSM-Servern und dem SMTP-E-Mail-Server
123	Gateway-Server	NTP-Kanal für die Verbindung zwischen dem Gateway- Server und dem NTP-Server
161	Server für die Datenverarbeitung	SNMP-Kanal für die Verbindung zwischen dem Server für die Datenverarbeitung und dem SNMP-Manager
389	Gateway-Server	Verbindung zwischen dem Gateway-Server und dem LDAP-Server für die Authentifizierung (optional). Weitere Informationen finden Sie unter "Authentifizierungsstrategien" auf Seite 385.
1433	Gateway-Server, Server für die Datenverarbeitung	Verbindung zwischen den BSM-Servern und dem Server mit Microsoft SQL Server. Dies ist der Standardport. Dieser Port kann während der Installation oder später geändert werden.
1434	Gateway-Server, Server für die Datenverarbeitung	Verbindung zwischen den BSM-Servern und dem Server mit Microsoft SQL-Browser-Dienst. Dieser Port wird nur verwendet, wenn eine benannte Instanz genutzt wird.
1521	Gateway-Server, Server für die Datenverarbeitung	Verbindung zwischen den BSM-Servern und dem Server mit dem Oracle-Server. Dies ist der Standardport. Dieser Port kann während der Installation oder später geändert werden.
80/443	Gateway-Server	80. HTTP/S-Kanal für die Verbindung zwischen dem Gateway-Server und der Datenerfassung für Remote-Verwaltungsaufgaben 443. Port für den Reverse-Proxy

Lokaler BSM-Datenverkehr

In der folgenden Tabelle sind die Ports aufgeführt, die für die Kommunikation zwischen Komponenten auf allen BSM-Servercomputern verwendet werden.

Hinweis: Bei den hier aufgeführten Ports handelt es sich um die von BSM verwendeten Ports. Wenn Sie eine Portzuweisung ändern müssen, sollten Sie sich unbedingt zuerst an den HP Software-Unterstützung wenden.

Portnummer	BSM-Server, die eine Verbindung mit dem Port herstellen	Portverwendung
1098	Gateway-Server, Server für die Datenverarbeitung	RMI (Remote Method Invocation)-Verwaltungskanal, der von JBoss Application Server verwendet wird
1099	Gateway-Server, Server für die Datenverarbeitung	Benennungsdienst, der von JBoss Application Server verwendet wird
4504	Gateway-Server	Lokale TCP-LDAP-Verbindung, die vom Gateway- Server verwendet wird
5001	Gateway-Server	Verbindung zwischen VuGen und dem zentralen Repository-Dienst
8009	Gateway-Server, Server für die Datenverarbeitung	Tomcat AJP13-Connector
8010	Gateway-Server, Server für die Datenverarbeitung	Tomcat AJP13 für WDE-Connector
8080	Gateway-Server, Server für die Datenverarbeitung	HTTP-Kanal für Komponenten auf demselben Computer
8083	Gateway-Server, Server für die Datenverarbeitung	Dynamisches Laden von RMI-Klassen
8093	Gateway-Server, Server für die Datenverarbeitung	TCP JMS OIL/2 und UIL für JBoss Application Server
11020	Gateway-Server, Server für die Datenverarbeitung	RMI-Verwaltungskanal für den BSM-Dienst

Portnummer	BSM-Server, die eine Verbindung mit dem Port herstellen	Portverwendung
11021	Gateway-Server, Server für die Datenverarbeitung	HTTP-Kanal für den BSM-Dienst
21212	Server für die Datenverarbeitung	HTTP-Kanal für den RTSM-Prozess
21301	Server für die Datenverarbeitung	RMI-Kommunikation von Backend- zu EPI-Server- Verwaltungsdiensten
21302	Gateway-Server	RMI-Kommunikation von der Konsolenwebapplikation zur Verwaltungswebapplikation
21303	Gateway-Server	RMI-Kommunikation von der Konsolenwebapplikation zum Skriptserver für die benutzerdefinierte Aktion, der auf demselben Host ausgeführt wird
29601	Gateway-Server, Server für die Datenverarbeitung	RMI-Verwaltungskanal für JBoss Application Server
29602	Gateway-Server, Server für die Datenverarbeitung	RMI-Verwaltungskanal für die Busprozesse
29603	Gateway-Server	RMI-Verwaltungskanal für den DB-Ladeprozess
29604	Gateway-Server	RMI-Verwaltungskanal für den WDE-Prozess (Web Data Entry, Webdatenerfassung)
29608	Server für die Datenverarbeitung	RMI-Verwaltungskanal für den Offline-BLE-Prozess
29610	Server für die Datenverarbeitung	RMI-Verwaltungskanal für das Partitionieren und Löschen
29612	Gateway-Server, Server für die Datenverarbeitung	RMI-Verwaltungskanal für den RTSM-Prozess
29616	Gateway-Server	RMI-Verwaltungskanal für den Scheduler-Prozess
29620	Server für die Datenverarbeitung	RMI-Verwaltungskanal für das BPI-Repository
29622	Server für die Datenverarbeitung	RMI-Verwaltungskanal für den Back-End-Prozess von Operations Manager
29628	Server für die Datenverarbeitung	RMI für Skriptausführung für Pipelineverarbeitung in OMi

Portnummer	BSM-Server, die eine Verbindung mit dem Port herstellen	Portverwendung
29629	Gateway-Server	RMI für die Skriptausführung für anpassbare Kontextmenüs im Ereignisbrowser von OMi
29630	Server für die Datenverarbeitung	RMI
29700	Server für die Datenverarbeitung	RMI-Port für Online-BLE-Prozesse
29711, 29712, 29713, 29714	Server für die Datenverarbeitung	RMI-Port für Online-BLE-Prozesse
29720	Server für die Datenverarbeitung	RMI-Port für Online-BLE-Prozesse
29800	Server für die Datenverarbeitung	HTTP-Port für Online-BLE-Prozesse
29807	Gateway-Server, Server für die Datenverarbeitung	Herunterfahren der Hauptbusprozesse
29811, 29812, 29813	Server für die Datenverarbeitung	HTTP-Port für Online-BLE-Prozesse
29820	Server für die Datenverarbeitung	HTTP-Port für Online-BLE-Prozesse
29903	Gateway-Server	HTTP-Kanal für den DB-Ladeprozess
29904	Gateway-Server	HTTP-Kanal für den WDE-Prozess (Web Data Entry, Webdatenerfassung)
29908	Server für die Datenverarbeitung	HTTP-Kanal für den Offline-BLE-Prozess
29910	Server für die Datenverarbeitung	HTTP-Kanal für das Partitionieren und Löschen
29916	Gateway-Server	HTTP-Kanal für den Scheduler-Prozess
29922	Server für die Datenverarbeitung	HTTP-Kanal für den Back-End-Prozess von Operations Manager
29928	Server für die Datenverarbeitung	HTTP-Port für Skriptausführung für Pipelineverarbeitung in OMi

Portnummer	BSM-Server, die eine Verbindung mit dem Port herstellen	Portverwendung
29929	Gateway-Server	HTTP-Port für die Skriptausführung für anpassbare Kontextmenüs im Ereignisbrowser von OMi
29930	Server für die Datenverarbeitung	НТТР
30020	Server für die Datenverarbeitung	HTTP-Port für Onlineprozesse der Engine für die Geschäftslogik
31000- 31999; 32000-32999	Gateway-Server, Server für die Datenverarbeitung	Der BSM-Dienst verwendet den ersten verfügbaren Port der einzelnen Bereiche
Dynamische Ports	Gateway-Server, Server für die Datenverarbeitung	Einige dynamische Ports werden für Kanäle zwischen Komponenten verwendet

Kapitel 14

Empfehlungen zur Dateisicherung

BSM-Verzeichnisse, die wichtige Konfigurations- und Datendateien enthalten, sollten vorbeugend täglich gesichert werden.

In der folgenden Tabelle sind die BSM-Verzeichnisse angegeben, die solche Dateien enthalten und deshalb gesichert werden sollten. Alle Verzeichnisse befinden sich im <h >HPBSM-Stammverzeichnis>.

Ressource	Kommentare
\HPBSM\BLE	Konfiguration der Geschäftsregeln. Führen Sie eine Sicherung durch, wenn Geschäftsregeln erstellt wurden.
\HPBSM\conf	Verschiedene BSM-Konfigurationsdateien.
\HPBSM\dat	Verschiedene BSM-Konfigurationsdateien.
\HPBSM\dbverify\conf	Konfigurationsdateien für dbverify . Dieses Verzeichnis muss nicht gesichert werden, wenn dbverify nicht ausgeführt wurde.
\HPBSM\EJBContainer\bin	Konfigurationsdateien für die Skripts, mit denen BSM ausgeführt wird, und Umgebungseinstellungen.
\HPBSM\bin	Binäre BSM-Dateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.
\HPBSM\lib	BSM-Bibliotheksdateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.
\HPBSM\AppServer\GDE	Konfigurationsdateien für die Generic Reporting Engine, die zum Abrufen von Daten für Reports verwendet wird.
\HPBSM\odb\conf	RTSM-Hauptverzeichnis für die Konfiguration
\HPBSM\odb\lib	RTSM-Bibliotheksdateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.

Ressource	Kommentare
\HPBSM\odb\classes	RTSM-Patch-Dateien. Sicherung, wenn Patches hinzugefügt wurden.
\HPBSM\odb\runtime\fcmdb	RTSM-Adapterdateien.
\HPBSM_postinstall	Konfigurationsdateien für Verfahren nach der Installation.
\HPBSM\opr\bin	Binäre Operations Management-Dateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.
\HPBSM\opr\lib	Operations Management-Bibliotheksdateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.
\HPBSM\opr\webapps	BSM-Webapplikationsdateien. Führen Sie eine Sicherung durch, wenn Änderungen an den Standardeinstellungen der Installation vorgenommen wurden.
\HPBSM\opr\newconfig	Verschiedene BSM-Konfigurationsdateien und - Bibliotheken.
\HPBSM\AppServer\webapps\site.war\WEB-INF\sam\hi-mapping-monitors.xml	Benutzerdefinierte EMS-Monitortypen. Sichern, wenn kundenspezifischen EMS-SiteScope-Monitore konfiguriert wurden.

Teil 3

Daten-Enrichment

Kapitel 15

Standortverwaltung

Die Standortverwaltung wird zum Definieren von geografischen und logischen Standort-CIs verwendet. Darüber hinaus werden ihnen IP-Adressen zugewiesen. Standort-CIs können mit anderen CIs verbunden werden. Sie werden beispielsweise verwendet, um einen Standort mit einem Business Process Monitor (BPM)-Agenten oder mit einer Seite zu verbinden, die automatisch von Real User Monitor (RUM) ermittelt wird.

Öffnen der Standortverwaltung:

Wählen Sie Admin > Plattform > Standorte.

Weitere Informationen

Standortverwaltung - Übersicht

Sie haben folgende Möglichkeiten:

- Öffnen Sie die Standortverwaltung über die End User Management-Verwaltung (Admin > End User Management > Einstellungen > Business Process Monitor-Einstellungen > BPM-Agenten). Klicken Sie auf , um das Dialogfeld zum Ändern des Agentenstandorts zu öffnen.
- Zeigen Sie die Standort-CIs im IT Universe Manager an (Admin > RTSM-Verwaltung > Modellieren > IT Universe Manager). Zum Anzeigen der Standort-CIs wählen Sie die Ansicht Locations (Standorte) aus.

Die Standortverwaltung steht Benutzern zur Verfügung, die über die vorab definierten Berechtigungen **Administrator** oder **Systemmodifikation** verfügen. Berechtigungen werden unter **Admin > Plattform > Benutzer und Berechtigungen** konfiguriert.

Standortdetails und -beschreibungen

Standortentität. Eine Entität, die einen Ort in der Welt beschreibt. Es kann sich um einen geografischen Standort, wie ein Land oder eine Stadt, oder um einen logischen Standort, wie ein Gebäude, handeln. Die Standortentität kann mit Geräten und logischen CIs verbunden werden, die Endbenutzer oder Rechenzentren repräsentieren.

Geografischer Standort. Ein absoluter Standort auf der Erde, der aus einer vordefinierten Liste von Städten/Staaten/Ländern ausgewählt wird und dem bestimmte geografische Koordinaten zugeordnet werden.

Logischer Standort. Ein benutzerdefinierter virtueller Standort, der nicht unbedingt einem reellen Standort entsprechen muss. Wenn Sie einem logischen Standort geografische Koordinaten zuweisen, können diese Koordinaten geändert oder gelöscht werden.

Hinweis: Alle geografischen Standorte werden unabhängig von der Sprache der Benutzeroberfläche auf Englisch angezeigt. Logische Standorte können in einer beliebigen ausgewählten Sprache benannt werden und bleiben in dieser Sprache, auch wenn die Sprache der Benutzeroberfläche später geändert wird.

Hierarchie. Standorte können unterhalb von anderen Standorten verschachtelt werden, um so eine hierarchische Struktur mit maximal sieben Ebenen unter dem Stamm zu erstellen.

Geografische Koordinaten. Längen- und Breitengrade (in Dezimalschreibweise). Die Koordinaten werden einzelnen Standorten zugewiesen.

Standardcontainer. Der übergeordnete Standort für alle Standorte, die automatisch von Real User Monitor (RUM) ermittelt werden. Standardmäßig ist **Welt** der Standardcontainer (der Stamm in der Standortstruktur), es kann jedoch ein beliebiger Standort aus der Struktur als Standardcontainer festgelegt werden.

IP-Bereiche. Jedem Standort können mehrere IP-Bereiche zugeordnet werden. Ein IP-Bereich ist ein Bereich von IP-Adressen, die zur Verwendung durch Geräte in einem bestimmten geografischen Bereich vorgesehen sind.

Aufgaben

Auffüllen der Standortverwaltung

Die Standortverwaltung kann auf mehrere Weise mit Standorten aufgefüllt werden.

Verwenden der Standortverwaltung in der Plattformverwaltung. Weitere Informationen zur Benutzeroberfläche finden Sie "Seite "Standortverwaltung" auf Seite 171.

Massenupload aus einer XML-Datei. BSM ermöglicht Ihnen das Erstellen und Definieren von Standort-CIs mithilfe einer XML-Datei außerhalb der Benutzeroberfläche. Der Massenupload ist eine Alternative zur Verwendung der Benutzeroberfläche und besser geeignet, um eine großen Anzahl von Standorten zu definieren.

Weitere Informationen finden Sie "Erstellen und Verwenden der XML-Datei" unten.

Verwenden von Real User Monitor (RUM). Wenn RUM auf eine IP-Adresse trifft, deren Standort unbekannt ist, wird diese IP-Adresse für die Standort-Discovery an die Standortverwaltung weitergegeben. Die Standortverwaltung sucht dann im Hexasoft IP2Location-Repository nach einem geografischen Standort, der mit der jeweiligen IP-Adresse übereinstimmt. Wird eine Übereinstimmung gefunden, werden in der Standortverwaltung neue Standorte für die IP-Adresse erstellt. Abhängig von den Informationen im IP-Adressen-Repository können maximal drei Standorte (Land, Bundesstaat und Stadt) für jede IP-Adresse erstellt werden.

Hinweis: Wenn End User Management (EUM) nach einer Deaktivierung wieder aktiviert wird, kann es einige Stunden dauern, bis die automatische Discovery von Standorten wieder funktioniert. In diesem Zeitraum werden die Informationen für die Zuordnung von IP-Adressen zu Standorten in die Datenbank geladen.

Erstellen und Verwenden der XML-Datei

Sie können Ihre eigene Standorthierarchie definieren, indem Sie eine XML-Datei erstellen und sie über eine Java Management Extensions (JMX)-Konsole laden. (Details zum Zugreifen auf die JMX und Verwenden der JMX finden Sie unter "Verwenden der JMX-Konsole" auf Seite 25.)

Die XML-Datei kann in einem beliebigen Werkzeug, das Text unterstützt, erzeugt und bearbeitet werden. Sie können die Datei von Grund auf neu erstellen oder sie auf einer XML-Datei basieren, die von BSM in der JMX-Konsole erstellt wird und bereits die Tags, Elemente und Attribute für die Massenupload-XML-Datei enthält.

Details zur XML-Datei

Eine Referenz mit Informationen zu allen XML-Tags, Elementen und Attributen, die in der Datei für den Massenupload enthalten sein können, finden Sie "XML-Tag-Referenz" auf Seite 180.

Jede XML-Datei für den Massenupload muss mit den folgenden Angaben beginnen:

- <?xml version="1.0" encoding="UTF-8" ?> Diese Informationen sagen aus, dass es sich um eine XML-Datei mit einer UTF-8-Zeichencodierung handelt.
- <!DOCTYPE locations_manager SYSTEM "./locations.dtd"> Dies ist die Dokumenttyp-Deklaration. Die Datei locations.dtd befindet sich im Ordner HPBSM/conf/locations. Der Pfad zur locations.dtd muss relativ zum Speicherort der XML-Datei angegeben werden, und muss möglicherweise aktualisiert werden. Wenn die XML-Datei im gleichen Speicherort wie die

locations.dtd gespeichert ist, ist kein Pfad notwendig.

Die XML-Datei wird mit der Datei **locations.dtd** auf Gültigkeit überprüft. Wenn die XML-Struktur nicht korrekt ist, wird eine SAXParseException-Meldung ausgegeben, und die Operation schlägt fehl. Wenn in der DOCTYPE-Zeile nicht korrekt auf den Pfad der **locations.dtd** verwiesen wird, schlägt die Gültigkeitsüberprüfung und die gesamte Operation fehl.

Hinweis: Durch das Füllen der Standortverwaltung über XML werden alle Standorte gelöscht, die zuvor in der Standortverwaltung definiert wurden.

XML-Beispieldatei

In diesem Beispiel möchte der Kunde 1 eine XML-Datei hochladen, um folgende Standorthierarchie in der Standortverwaltung zu erstellen: Der erste Standort in Los Angeles enthält geographische Koordinaten, ISP-Adressbereiche und ISPs. Die Standorte 2 und 3 sind unter dem ersten Standort (Los Angeles) verschachtelt, und 2a und 2b befinden sich unter 2. Standort 4 befindet sich in der Hierarchie auf gleicher Ebene wie Los Angeles.

Welt

- Los Angeles; latitude 34.0396, longitude -118.2661; ISPv4 address range 4.38.41.136 to 4.38.80.152 (ISP = Level 3 Communications); ISPv6 address range 2002:0C19:8B00:0000:0000:0000:0000:0000 to 2002:0C19:B28F:0000:0000:0000:0000
 (ISP = AT_T WorldNet Services)
- location 2
 - location 2a
 - location 2b
- location_3
- location_4

Hinweis: Der Stammstandort **Welt** muss nicht hinzugefügt werden.

Der Inhalt der XML-Datei, die zum Hochladen dieser Hierarchie verwendet wurde, lautet wie folgt:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE locations manager SYSTEM "conf/locations/locations.dtd">
<locations manager>
    <customer hierarchy customer id="1">
        <locations list>
            <location location name="Los Angeles">
                <latitude>34.0396</latitude>
                <longitude>-118.2661</longitude>
                <ip ranges>
                    <ip range>
                        <start ip>4.38.41.136/start ip>
                        <end ip>4.38.80.152</end ip>
                        <isp>Level 3 Communications</isp>
                    </ip range>
                    <ip range ip v6="true">
                        <start
```

```
ip>2002:0C19:8B00:0000:0000:0000:0000</start ip>
                        <end
ip>2002:0C19:B28F:0000:0000:0000:0000</end ip>
                       <isp>AT T WorldNet Services</isp>
                    </ip range>
                </ip ranges>
                <locations list>
                    <location location name="location 2">
                        <locations list>
                            <location location name="location 2a" />
                            <location location name="location 2b" />
                        </locations list>
                    </location>
                    <location location name="location 3" />
                </locations list>
            </location>
           <location location name="location 4" />
       </locations list>
    </customer hierarchy>
</locations manager>
```

Informationen zu den XML-Elementen und -Attributen finden Sie "XML-Tag-Referenz" auf Seite 180.

Auffüllen der Standortverwaltung

Die Standortverwaltung kann auf mehrere Arten mit Standort-CIs aufgefüllt werden. Sie haben folgende Möglichkeiten:

- "Erstellen von Standorten über die Benutzeroberfläche"
- "Auffüllen der Standortverwaltung mithilfe einer XML-Datei"

Erstellen von Standorten über die Benutzeroberfläche

Verwenden Sie die Benutzeroberfläche der Standortverwaltung zum Erstellen, Bearbeiten und Verwalten von Standorten sowie dazu, ihnen IP-Bereiche zuzuweisen. Weitere Informationen zur Benutzeroberfläche finden Sie "Seite "Standortverwaltung" auf Seite 171.

Auffüllen der Standortverwaltung mithilfe einer XML-Datei

Laden Sie Standort-CIs mithilfe einer XML-Datei außerhalb der Benutzeroberfläche in die Standortverwaltung hoch. Der Massenupload ist eine Alternative zur Verwendung der Benutzeroberfläche und besser geeignet, um die Standortverwaltung mit einer großen Anzahl von Standorten zu füllen.

Weitere Informationen zu dieser Aufgabe finden Sie "Aktualisieren von Standorten mithilfe von Massenuploads" unten.

Aktualisieren von Standorten mithilfe von Massenuploads

In dieser Aufgabe wird beschrieben, wie eine XML-Datei geladen wird, eine bestehende Standorthierarchie mithilfe von XML geändert wird und die Ergebnisse angezeigt werden.

So erstellen und ändern Sie eine XML-Datei für den Upload von Standorten:

1. Erstellen Sie eine XML-Datei ohne IDs für die Standorte mithilfe der folgenden Methoden:

Erstellen Sie die Datei mit einem beliebigen Werkzeug, das Text unterstützt. Speichern Sie die erstellte XML-Datei in einem Netzerwerkspeicherort, auf den über den BSM-Server zugegriffen werden kann. Weitere Informationen finden Sie "Erstellen und Verwenden der XML-Datei" auf Seite 166. Weitere Informationen zu den XML-Dateielementen und -attributen finden Sie "XML-Tag-Referenz" auf Seite 180.

Exportieren Sie die aktuelle Hierarchie als XML unter Verwendung der JMX-Konsole, wie weiter unten beschrieben.

- 2. Öffnen Sie die JMX-Konsole auf diesem Computer. (Ausführliche Anweisungen finden Sie unter "Verwenden der JMX-Konsole" auf Seite 25.)
- 3. Wählen Sie im Abschnitt BSM-Plattform den Eintrag service=Locations Manager aus.
- 4. Wenn Sie eine XML-Datei aus dem aktuellen Verzeichnis erstellen, verwenden Sie die Methode **convertLocationsHierarchyToXML** zum Eingeben der folgenden Werte:

customerId. Standardmäßig wird 1 für die **customerID** verwendet. Wenn Sie HP SaaS-Kunde sind, verwenden Sie Ihre HP SaaS-Kunden-ID.

target path. Der Speicherort, an dem die XML-Datei gespeichert werden soll.

- 5. Suchen und bearbeiten Sie die gerade gespeicherte XML-Datei:
 - a. Überprüfen Sie die Liste der bestehenden Standorte auf ihre Richtigkeit. Der Stammstandort **Welt** ist nicht in dieser XML-Datei vorhanden.
 - b. Zum Hinzufügen eines neuen Standorts darf keine ID definiert werden.
 - c. Zum Ändern eines Standorts ändern Sie die Felder, jedoch nicht die tatsächliche ID.
 - d. Zum Löschen eines Standorts löschen Sie alle Details aus der XML-Datei.
 - e. Zum Ändern der Position eines Standorts in der Hierarchie verschieben Sie den Standort mit der tatsächlichen ID auf eine andere Position in der XML-Datei.
 - f. Speichern Sie die erstellte XML-Datei in einem Netzerwerkspeicherort, auf den über den BSM-Server zugegriffen werden kann.

Tipps: Speichern Sie die XML-Datei in demselben Verzeichnis wie die Datei **locations.dtd**, sodass Sie nicht auf einen anderen Pfad in der Zeile der Dokumenttyp-Deklaration der XML-Datei verweisen müssen. Die Datei **locations.dtd** befindet sich im Verzeichnis **<HPBSM-Stammverzeichnis>\conf\locations**.

- 6. Für den Upload der bearbeiteten XML-Datei aktivieren Sie in JMX service=Locations Manager die Methode buildLocationsHierarchyFromXML.
 - a. Geben Sie in **xmlFilePath** den Pfad für den Speicherort ein, in dem Sie die XML-Datei gespeichert haben.
 - b. Wählen Sie im Parameter saveInFile den Wert True, um die bestehende Standorthierarchie in der Datei < HPBSM-Stammverzeichnis > \conf\locations \current_locations \higher hierarchy.xml zu speichern.

Hinweise:

- 1. Die XML-Datei muss den oben aufgeführten Regeln entsprechen. Wird eine der Regeln verletzt, wird **buildLocationsHierarchyFromXML** abgebrochen, bevor Änderungen am Standortmodell durchgeführt werden:
- Zwei Standorte auf derselben Hierarchieebene (mit demselben übergeordneten Element) dürfen nicht denselben Namen verwenden. Ein Standort direkt unter customer_hierarchy (d. h. direkt unter dem Stammstandort Welt) und ein Standort an einer anderen Stelle der Hierarchie dürfen nicht denselben Namen verwenden, es sein denn, eine Instanz bezieht sich auf einen geografischen Standort und die andere auf einen logischen Standort; oder sie beziehen sich auf verschiedene Typen von geografischen Standorten (Land, Staat oder Stadt) wie beispielsweise Mexiko und Mexiko-Stadt oder der Staat New York und die Stadt New York.
- Es kann eine Hierarchie mit maximal sieben Ebenen definiert werden.
- Standorte dürfen nicht dieselbe ID verwenden.
- Alle Standort-ID-Werte in der XML-Datei müssen einem bestehenden Standort mit dieser ID entsprechen.
- Überlappende IP-Bereiche sind nicht zulässig.
- 2. Durch das Speichern der bestehenden Hierarchie in einer Datei wird möglicherweise mehr Zeit für das Laden der neuen XML-Datei benötigt.
- 7. Die Standorte wurden nun in die Standortverwaltung geladen. Sie können über die Standortstruktur in der Benutzeroberfläche und über die JMX-Konsole angezeigt werden.

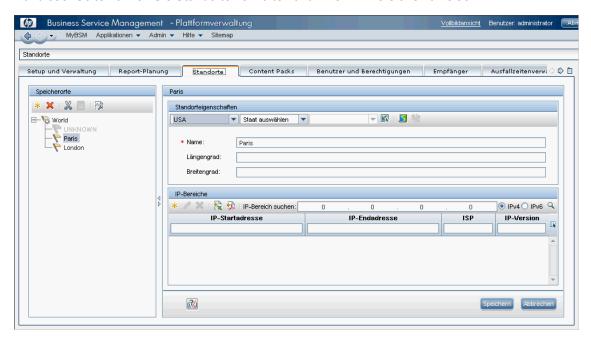
So zeigen Sie die Standorte über die JMX-Konsole an:

- Suchen Sie unter service=Locations Manager die Methode getAllLocations.
- Geben Sie die jeweilige Kunden-ID ein. Standardmäßig wird 1 für die **customerID** verwendet. Wenn Sie HP SaaS-Kunde sind, verwenden Sie Ihre HP SaaS-Kunden-ID.
- Aktivieren Sie die Methode und überprüfen Sie, dass alle Standorte, einschließlich des Stammstandorts Welt, aufgeführt werden.

Beschreibung der Benutzeroberfläche

Seite "Standortverwaltung"

Auf dieser Seite können Sie Standorte verwalten und ihnen IP-Bereiche zuweisen.

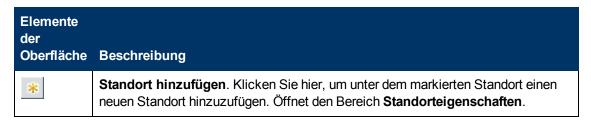


Zugriff	Wählen Sie Admin > Plattform > Standorte .
Relevante Aufgaben	"Auffüllen der Standortverwaltung" auf Seite 168
Siehe auch	"Standortverwaltung - Übersicht" auf Seite 165

• Bereich "Standorte" - Linker Ausschnitt

Im Bereich **Standorte** im linken Ausschnitt der Seite **Standorte** können Sie Standorte hinzufügen, löschen und verschieben und einen Standort als Standardcontainer festlegen. Standorte werden in einer Struktur mit maximal sieben Hierarchieebenen angezeigt, wobei der Stamm (die Nullebene) **Welt** heißt.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben. Sie können auch über ein Kontextmenü auf diese Aktionen zugreifen, indem Sie mit der rechten Maustaste auf den Bereich **Standorte** im linken Ausschnitt klicken.



Elemente der	
	Beschreibung
×	Standort löschen . Klicken Sie hier, um einen Standort und seine untergeordneten Standorte zu löschen.
	Das Fenster Bestätigung wird geöffnet, in dem Sie gefragt werden, ob Sie den Standort wirklich löschen wollen. Außerdem erhalten Sie die Warnung, dass der Standort möglicherweise von anderen BSM-Komponenten genutzt wird und Sie diese Aktion nicht rückgängig machen können.
	Wenn Sie einen Standort löschen, können alle ihm oder seinen untergeordneten Standorten zugewiesenen IP-Bereiche an den übergeordneten Standort verschoben werden. Aktivieren Sie dazu das Kontrollkästchen IP-Bereiche zu übergeordnetem Standort verschieben im Fenster Bestätigung.
*	Standort ausschneiden. Klicken Sie hier, um einen Standort auszuschneiden. Der Standort wird in die Zwischenablage kopiert und kann dann unter einem anderen Element in der Standortstruktur eingefügt werden.
	Hinweis: Wird ein Standort ausgeschnitten, so bleibt er – ausgegraut – an der früheren Stelle in der Struktur sichtbar, bis er an anderer Position eingefügt wurde. Wenn Sie die Auswahl eines ausgeschnittenen Standorts vor dem Einfügen an anderer Stelle rückgängig und diesen an seine ursprüngliche Position zurückbringen wollen, klicken Sie erneut auf Standort ausschneiden .
	Standort einfügen. Nur verfügbar, wenn ein Standort ausgeschnitten wurde und der Benutzer zu einem anderen Teil der Struktur navigiert ist.
	Hinweis: Standorte können unterhalb von anderen Standorten eingefügt werden, um so eine hierarchische Struktur mit maximal sieben Ebenen unter dem Stamm zu erstellen. Es ist nicht zulässig, untergeordneten Elementen eines Standorts dieselben Namen zuzuweisen. Ein Standort unter "Welt" und ein Standort an einer anderen Stelle der Hierarchie dürfen nicht denselben Namen verwenden, es sein denn, eine Instanz bezieht sich auf einen geografischen Standort und die andere auf einen logischen Standort; oder sie beziehen sich auf verschiedene Typen von geografischen Standorten (Land, Staat oder Stadt) wie beispielsweise Mexiko und Mexiko-Stadt oder der Staat New York und die Stadt New York.
	Als Standardcontainer festlegen. Klicken Sie hier, um einen bestimmten Standort als Standardcontainer festzulegen. Dabei handelt es sich um den übergeordneten Standort für alle automatisch ermittelten Standorte.
	Weitere Informationen finden Sie "Standortverwaltung - Übersicht" auf Seite 165.

• Bereich "Standorteigenschaften"

Im Bereich **Standorteigenschaften** können Sie einen geografischen Standort und dessen Koordinaten anhand einer vordefinierten Liste aus Ländern und Gebieten, Staaten und Städten festlegen oder einen logischen Standort benennen und dessen geografische Koordinaten festlegen. Durch das Definieren eines Standorts als geografischer Standort kann die Discovery dem Standort automatisch ermittelte IP-Adressen zuweisen. Zum Definieren eines Standorts als geografischer

Standort wählen Sie das entsprechende Land, den Staat und die Stadt aus (Sie können auch nur ein Land, Land und Staat oder Land und Stadt auswählen) und klicken Sie auf

Hinweis: Der geografische Standort kann nur aus einer vordefinierten Liste festgelegt werden. Wenn Sie den Namen eines Standorts manuell eingeben, wird dieser als logischer Standort erstellt.

Elemente der Oberfläche	Beschreibung
<land oder<br="">Region>/<bundesstaat>/<stadt></stadt></bundesstaat></land>	In der ersten und dritten Dropdown-Liste können Sie ein Land/eine Region und eine Stadt auswählen. Wenn die USA als Land ausgewählt werden, steht auch die mittlere Dropdown-Liste zur Verfügung, in der ein bestimmter Bundesstaat ausgewählt werden kann.
Q	Geografischen Standort festlegen. Klicken Sie hier, um die geografischen Koordinaten (Längengrad und Breitengrad) des ausgewählten Landes bzw. des Staats oder der Stadt zu suchen und den Namen und die Koordinaten automatisch in die entsprechenden Felder unter Standorteigenschaften einzugeben, um den Standort so als geografischen Standort zu definieren.
	Standortkoordinaten aus Karte auswählen. Klicken Sie hier, um das Dialogfeld Karte anzuzeigen, in dem Sie die geografischen Koordinaten beliebiger Standorte auswählen können.
	Wenn bereits geographische Koordinaten in die Felder Längengrad und Breitengrad eingegeben wurden, werden sie automatisch an das Dialogfeld Karte übergeben, das dann eine Stecknadel für diesen Standort erstellt.
	Weitere Informationen finden Sie "Dialogfeld 'Karte'" auf Seite 177.
*	Koordinaten vom nächsten übergeordneten Element abrufen. Klicken Sie hier, um die geografischen Koordinaten des nächsten übergeordneten Standorts mit Koordinaten an den ausgewählten Standort zu kopieren.

Elemente der Oberfläche	Beschreibung
Name	Geben Sie den Namen des Standorts in das Textfeld Name ein.
	Hinweise:
	Das Namensfeld ist erforderlich. Es ist nicht zulässig, untergeordneten Elementen eines Standorts dieselben Namen zuzuweisen. Ein Standort unter Welt und ein Standort an einer anderen Stelle der Hierarchie dürfen nicht denselben Namen verwenden, es sein denn, eine Instanz bezieht sich auf einen geografischen Standort und die andere auf einen logischen Standort; oder sie beziehen sich auf verschiedene Typen von geografischen Standorten (Land, Staat oder Stadt) wie beispielsweise Mexiko und Mexiko-Stadt oder der Staat New York und die Stadt New York. Das Zuweisen desselben Namens an verschiedene Standorte unter verschiedenen übergeordneten Standorten ist zulässig. In diesem Fall wird jedoch ein kleines Warnsymbol angezeigt, um darauf hinzuweisen, dass der Namen bereits für einen anderen Standort in der Struktur definiert ist und ggf. geändert werden sollte.
	Wenn Sie den Namen eines geografischen Standorts ändern, wird dessen Verknüpfung mit dem
	ursprünglichen geografischen Standort beibehalten.
Längengrad/Breitengrad	Geben Sie den Längengrad und den Breitengrad des Standorts in die entsprechenden Textfelder ein.
	Wenn Sie einen Standort aus der vordefinierten Dropdownliste mit Ländern, (Bundes-)Staaten und Städten oder aus dem Dialogfeld Karte auswählen, werden die Felder für Längengrad und Breitengrad automatisch ausgefüllt.

• Bereich "IP-Bereiche"

Sie können den Bereich **IP-Bereiche** verwenden, um einem Standort IP-Breiche zuzuweisen. Real User Monitor (RUM) verwendet diese Bereiche dann, um bestimmten Standorten neu ermittelte Seiten und andere CIs zuzuweisen.

Die Tabelle mit IP-Bereichen kann Tausende von Seiten enthalten. Zum Anzeigen der Tabelle in einer Datei können Sie diese im Excel- oder Adobe Acrobat-Format (PDF) exportieren.

Elemente der Oberfläche	Beschreibung
*	Neuer IP-Bereich . Klicken Sie hier, um einen neuen IP-Bereich zu erstellen. Öffnet das Dialogfeld Neuer IP-Bereich .
	Hinweis: Ein IP-Bereich kann jeweils nur einem Standort zugewiesen werden.
	Wenn Sie einen IP-Bereich zuweisen, der mit einem übergeordneten IP-Bereich überlappt, wird eine Meldung mit der Warnung angezeigt, dass der IP-Bereich durch diese Aktion aus übergeordneten Standort entfernt wird. (Es wird nur der sich überlappende Bereich entfernt und der übergeordnete IP-Bereich entsprechend angepasst.) Klicken Sie auf Von übergeordnetem Standort entfernen, um den überlappenden IP-Bereich aus dem übergeordneten Element zu entfernen und ihn dem ausgewählten Standort zuzuweisen, oder klicken Sie auf Abbrechen.
	Wenn Sie einen IP-Bereich zuweisen wollen, der mit einem Bereich überlappt, der bereits einem anderen (nicht übergeordneten) Standort zugewiesen wurde, wird eine Fehlermeldung angezeigt und Sie müssen einen anderen IP-Bereich auswählen.
0	IP-Bereich bearbeiten . Klicken Sie hier, um einen ausgewählten IP-Bereich zu bearbeiten. Öffnet das Dialogfeld IP-Bereich bearbeiten .
×	IP-Bereich löschen. Klicken Sie hier, um einen oder mehrere ausgewählte IP-Bereiche zu löschen.
	Nach Excel exportieren. Klicken Sie hier, um IP-Bereichsinformationen für den ausgewählten Standort in eine Excel-Kalkulationstabelle zu exportieren.
9	In PDF exportieren. Klicken Sie hier, um IP-Bereichsinformationen für den ausgewählten Standort in eine Adobe Acrobat-Datei zu exportieren.
	Sichtbare Spalten ändern. Klicken Sie hier, um auszuwählen, welche Spalten mit IP-Bereichsinformationen im Bereich IP-Bereiche angezeigt werden. Das Dialogfeld Sichtbare Spalten ändern wird angezeigt.
	Hinweis: Nicht auf dem Bildschirm angezeigte Spalten werden auch nicht in Excel- oder Adobe Acrobat-Dateien (PDF) exportiert.

Elemente der Oberfläche	Beschreibung	
IP-Bereich	So finden Sie einen vorhandenen Bereich mit einer bestimmten IP-Adresse:	
suchen	Wählen Sie das entsprechende Optionsfeld aus:	
	■ IPv4 (Internet Protocol Version 4) für IP-Adressen aus vier Zahlen, jeweils von 0 bis 255, in punktierter Dezimalschreibweise	
	 IPv6 (Internet Protocol Version 6) für IP-Adressen aus acht Hexadezimalzahlen, jeweils von 0 bis FFFF, in kommagetrennter Schreibweise 	
	Geben Sie die IP-Adresse in das Feld IP-Bereich suchen ein.	
	3. Klicken Sie auf .	
	Das System markiert den Bereich, in dem sich die IP-Adresse befindet.	
	Hinweis: Hierbei wird nur nach dem IP-Bereich im aktuell ausgewählten Standort gesucht.	
IP- Startadresse/IP- Endadresse, ISP, IP-Version	Um die IP-Bereiche nach einer bestimmten Textzeichenfolge in den oberen und unteren IP-Bereichslimits, ISP-Namen oder IP-Versionen zu filtern, geben Sie die Zeichenfolge in die Felder IP-Startadresse, IP-Endadresse, ISP oder IP-Version ein.	
	Diese Felder können miteinander kombiniert werden. Sie können ein Sternchen (*) als Platzhalterzeichen verwenden, um ein oder mehrere Zeichen darzustellen.	
	Beispiel:	
	Geben Sie zum Filtern nach IPv6-Adressen "6" in das Feld IP-Version ein.	
	Geben Sie zum Filtern nach IPv4-Adressbereichen, deren oberes Limit auf 0 endet, "* . * . * . 0" in das Feld IP-Startadresse ein.	

Dialogfeld 'Neuer IP-Bereich/IP-Bereich bearbeiten'

Zugriff	Wählen Sie Admin > Plattform > Standorte und klicken Sie auf unter IP-Bereiche
---------	--

Elemente der Oberfläche	Beschreibung
IP-Version	Wählen Sie IPv4 oder IPv6 , um Folgendes auszuwählen:
	Internet Protocol Version 4 (für IP-Adressen aus vier Zahlen, jeweils von 0 bis 255, in punktierter Dezimalschreibweise)
	Internet Protocol Version 6 (für IP-Adressen aus acht Hexadezimalzahlen, jeweils von 0 bis FFFF, in kommagetrennter Schreibweise)
IP- Startadresse/IP-	Verwenden Sie die Felder IP-Startadresse und IP-Endadresse , um den IP-Adressbereich für den Standort festzulegen.
Endadresse	Bei IPv4 wird bei der Eingabe einer IP-Adresse im Feld IP-Startadresse automatisch eine entsprechende, auf 255 endende Adresse in das Feld IP-Endadresse eingegeben. Die Werte in beiden Feldern können in zulässige Werte (0-255) geändert werden, die Adresse im Feld IP-Endadresse muss jedoch gleich oder höher sein als die Adresse im Feld IP-Startadresse.
	Hinweis: Der IPv4-Bereich darf 50.000.000 IP-Adressen nicht überschreiten.
	Bei IPv6 wird bei der Eingabe einer IP-Adresse im Feld IP-Startadresse automatisch dieselbe Adresse in das Feld IP-Endadresse eingegeben. Die Werte in beiden Feldern können in zulässige Werte (0-FFFF) geändert werden und die Adresse im Feld IP-Endadresse kann höher, gleich oder niedriger sein als die Adresse im Feld IP-Startadresse.
ISP	Geben Sie im Feld ISP den Internet-Service-Provider an.

Dialogfeld 'Karte'

In diesem Dialogfeld können Sie die geographischen Koordinaten von Standorten auswählen.

Hinweis: Benutzer, die nicht mit dem Internet verbunden sind, sehen eine andere Version dieser Karte.



Zugriff	Klicken Sie im Bereich Standorteigenschaften der Seite Standorte auf
Wichtiger Hinweis	Wenn bereits geographische Koordinaten in die Felder Längengrad und Breitengrad eingegeben wurden, werden sie automatisch an das Dialogfeld Karte übergeben, das dann eine Stecknadel für diesen Standort erstellt.
Relevante Aufgaben	"Auffüllen der Standortverwaltung" auf Seite 168.
Siehe auch	"Seite "Standortverwaltung"" auf Seite 171.

Elemente der Oberfläche	Beschreibung
•	Vergrößern . Klicken Sie hierauf, um die Karte zu vergrößern.
	Hinweis: Dieses Symbol befindet sich auf der Symbolleiste. Ein anderes Vergrößern -Symbol mit identischer Funktion wird auf der Karte selbst angezeigt.

Elemente der Oberfläche	Beschreibung
Q	Verkleinern . Klicken Sie hierauf, um die Karte zu verkleinern.
	Hinweis: Dieses Symbol befindet sich auf der Symbolleiste. Ein anderes Verkleinern -Symbol mit identischer Funktion wird auf der Karte selbst angezeigt.
Ω	Zurücksetzen. Wenn Sie die Karte an bestimmten Koordinaten geöffnet haben und dann woanders hinschwenken, können Sie die Karte durch Klicken auf Zurücksetzen wieder auf die Startkoordinaten zentrieren.
Optionsfelder "Ziehen/Markieren"	Wählen Sie Markieren , und verschieben Sie die Stecknadel an einen anderen Standort in der Karte, indem Sie auf diesen Standort klicken. Durch Doppelklicken wird die Stecknadel verschoben und die Karte an diesem Standort vergrößert.
	Wählen Sie Ziehen , um die Karte zu ziehen.
<land oder<br="">Region>/<bundesstaat>/<stadt></stadt></bundesstaat></land>	In der ersten und dritten Dropdown-Liste können Sie ein Land/eine Region und eine Stadt auswählen. Wenn die USA als Land ausgewählt werden, steht auch die mittlere Dropdown-Liste zur Verfügung, in der ein bestimmter Bundesstaat ausgewählt werden kann.
Q	Standort auf Karte finden. Klicken Sie hierauf, um das Land/die Region und die Stadt, das bzw. die Sie ausgewählt haben, auf der Karte zu finden.
	In eine Richtung schwenken. Klicken Sie auf dieses Steuerelement, halten Sie die Maustaste gedrückt, und ziehen Sie, um die Karte zu schwenken.
Straßenansicht	Klicken Sie hierauf, um eine Straßenkarte der Welt anzuzeigen.
Luftbild	Klicken Sie hierauf, um ein fotografisches Luftbild der Welt anzuzeigen.
Vogelperspektive	Die Vogelperspektive ist deaktiviert.
Label	Klicken Sie in der Luftbildanzeige hierauf, um Label ein- oder auszublenden. In der Straßenansicht ist dies deaktiviert.
Koordinaten eingeben	Klicken Sie hierauf, um die Koordinaten des markierten Standorts automatisch in die Felder Längengrad und Breitengrad des Bereichs Standorteigenschaften zu kopieren.

XML-Tag-Referenz

In den nachstehenden Tabellen werden sämtliche Elemente und Attribute aufgelistet, die in der Massenupload-XML-Datei verwendet werden.

• Tabelle der Elemente

Element	Beschreibung	Attribute
locations_ manager	Anfangselement eines Blocks, der Daten der Standortverwaltung enthält.	
customer_ hierarchy	Anfangselement in einer Hierarchie von Standorten für einen bestimmten Kunden.	customer_ id
locations_ list	Anfangselement in einer Liste von Standorten.	
Standort	Anfangselement in einem Block, der Attribute für einen bestimmten Standort definiert.	location_ name
latitude	Breitengrad des Standorts in Grad.	
longitude	Längengrad des Standorts in Grad.	
ip_ranges	Anfangselement in einer Liste von IP-Adressen für einen bestimmten Standort.	
ip_range	Anfangselement in einem Block, der Attribute für einen bestimmten Bereich von IP-Adressen definiert.	ip_v6
start_ip	Unteres Limit des Bereichs einer IP-Adresse.	
	IP-Adressenbereiche können das IPv4- oder IPv6-Format aufweisen. In der Standortverwaltung werden die folgenden Notationsformate unterstützt:	
	IPv4 – 4-Byte-Zahlen	
	IPv4 – Zeichenfolge im x.x.x.x-Format	
	IPv6 – 16-Byte-Zahlen	
	IPv6 – Zeichenfolge im x:x:x:x:x:x:x-Format	
	IPv6 – regulärer IPv6-Ausdruck	
end_ip	Oberes Limit des Bereichs einer IP-Adresse. Informationen zu unterstützten IPv4- und IPv6-Notationsformaten finden Sie unter "start_ip" weiter oben.	
	Hinweis: Der IPv4-Bereich darf 50.000.000 IP-Adressen nicht überschreiten.	
isp	Der IDP-Name für den Bereich	

• Tabelle der Attribute

Attribut	Übergeordnetes Element	Beschreibung	Beispiel
customer_ id	customer_ hierarchy	Zahl. Eindeutig und obligatorisch. Die ID-Nummer des Kunden, für den eine Standorthierarchie erstellt wird.	customer_ hierarchy customer_ id="1">
location_ name	Standort	Zeichenfolge. Obligatorisch. Nicht eindeutig (mehrere Standorte können denselben Namen aufweisen, sofern sie nicht gleichgeordnet sind). Name eines bestimmten Standorts.	<location location_ name="Los Angeles"></location
ip_v6	ip_range	Boolescher Wert. ="true", wenn die IP-Adressen für einen bestimmten Bereich im IPv6-Format vorliegen. Andernfalls weisen sie das IPv4-Format auf.	<ip_range ip_ v6="true"></ip_range

• Tabelle der implizierten Attribute

Die folgenden Attribute werden exportiert, wenn die aktuelle Hierarchie als XML exportiert wird, sie sind jedoch nicht erforderlich, wenn neue Standorte in der XML definiert werden. Beim Aktualisieren eines bestehenden Standorts in XML müssen diese Attribute beibehalten werden:

Attribut	Übergeordnetes Element	Beschreibung
original_geo_ location_id	Standort	Wird zur Identifizierung des geografischen Standorts verwendet.
location_type	Standort	Mögliche Werte: • "Nicht definiert" (Standard) • "Land" • "Staat" • "Stadt"
location_id	Standort	Die tatsächliche ID eines bestehenden Standorts

Beispiel:

<location_name="UNKNOWN" location_type="undefined" location_ id="47a3711c334fd8577858c6da60b3e0e6" original_geo_location_id="Unknown_Unknown">

Kapitel 16

Content Packs

Bei den Content Packs handelt es sich um Informationen, die von BSM verwendet werden, um die Objekte oder Konfigurationselemente (Configuration Items, CIs) zu beschreiben und zu erweitern, die die in der IT-Umgebung überwachten Elemente darstellen. Bei den Objekten kann es sich z. B. um Netzwerkhardware, Betriebssysteme, Applikationen, Services oder Benutzer handeln.

Der Inhalt für einen bestimmten Verwaltungsbereich kann in einem speziellen Content Pack enthalten sein. Ein Content Pack kann eine vollständige Baseline Ihrer gesamten Inhalte oder eines Teils Ihrer Inhalte enthalten – die Regeln, Zuordnungen, Indikatoren und Zuweisungen, die Sie definieren und konfigurieren, um die Benutzer bei der Verwaltung der IT-Umgebung zu unterstützen. Content Packs dienen auch dem Austausch angepasster Daten zwischen Instanzen von BSM, z. B. in Test- und Produktionsumgebungen.

Zur Verwaltung der Pakete mit Inhaltsdaten können Sie den Content Packs Manager verwenden. Er ermöglicht das Erstellen eines Content Packs, das Speichern in einer Datei, das Installieren oder Aktualisieren von Inhalten, das Hochladen von Inhalten aus einer installierten Instanz von BSM in eine andere und Verwenden der Export- und Importfunktionen.

BSM enthält eine Reihe von Content Packs, z. B. für Smart Plug-Ins (SPIs), die Sie in der Standardkonfiguration verwenden oder, falls erforderlich, an die Anforderungen Ihrer Umgebung anpassen können. Solcher Inhalt wird in der Regel als **Vordefiniert** aufgeführt und kann geändert werden (**Vordefiniert (angepasst)**). Der geänderte Inhalt kann auf die vordefinierten Werte zurückgesetzt werden.

Mit dem Content Packs Manager können Sie die folgenden Aufgaben ausführen:

- Definieren von Inhalten eines Content Packs und Speichern der Definition. Details finden Sie unter "Definieren von Content Packs" auf Seite 187.
- Verwalten von Abhängigkeiten zwischen Content Packs. Details finden Sie unter "Abhängigkeiten in Content Packs" auf Seite 188.
- Exportieren eines Content Packs (Definition und Inhalte) und der von ihm referenzierten Daten in eine Datei (ein so genanntes Content Pack). Details finden Sie unter "Exportieren von Content Packs" auf Seite 191.
- Importieren eines Content Packs (Definition und Inhalte) und der von ihm referenzierten Daten. Details finden Sie unter "Importieren von Content Packs" auf Seite 192.

Hinweis: Sie können den Zugriff auf den Content Packs Manager mithilfe von Berechtigungen gewähren und einschränken. Berechtigungen zum Verwenden des Content Packs Manager finden Sie unter **Admin > Plattform > Benutzer und Berechtigungen**.

Nachdem Sie den Benutzer ausgewählt haben, für den Sie die Content Manager-Berechtigungen ändern möchten, wählen Sie die Registerkarte **Berechtigungen** im rechten Ausschnitt aus. Der Ausschnitt **Kontext** wird angezeigt. Wählen Sie Operationenverwaltung-Kontext > Verwaltungsbenutzeroberflächen > Content Packs aus.

Inhaltstypen

Für Inhaltstypen werden folgende Begriffe verwendet:

Vordefinierter Inhalt

Bei vordefiniertem Inhalt handelt es sich in der Regel um von HP oder HP-Partnern bereitgestellten Inhalt, der für die Erstkonfiguration einer BSM-Installation verwendet wird. Nach der Installation eines vordefinierten Content Packs können Sie diese anfänglichen Artefakte ändern, sodass sie den Anforderungen Ihrer Umgebung und Verwaltungsaufgaben entsprechen. Alle geänderten vordefinierten Artefakte werden als **Vordefiniert (angepasst)** gekennzeichnet. Es ist nicht möglich, vordefinierte Artefakte zu entfernen, Sie können aber angepasste Artefakte wieder auf die ursprünglichen "vordefinierten" Werte zurücksetzen.

Benutzerdefinierter Inhalt

Bei benutzerdefiniertem Inhalt handelt es sich um Inhalt, der vom Kunden erstellt, z. B. zum Verwalten einer benutzerdefinierten, internen Applikation, und als **Benutzerdefiniert** gekennzeichnet wird.

Angepasster Inhalt

Geänderte vordefinierte Artefakte werden als **Vordefiniert (angepasst)** gekennzeichnet. Sie können angepasste Artefakte wieder auf die ursprünglichen "vordefinierten" Werte zurücksetzen.

Content Pack-Typen

Für Content Pack-Typen werden folgende Begriffe verwendet:

Vordefiniertes Content Pack

Bei vordefinierten Content Packs handelt es sich in der Regel um von HP oder HP-Partnern bereitgestellte Sammlungen von vordefiniertem Inhalt, der für die Erstkonfiguration einer BSM-Installation verwendet wird.

Nach der Installation eines vordefinierten Content Packs können Sie diese anfänglichen Artefakte ändern, sodass sie den Anforderungen Ihrer Umgebung und Verwaltungsaufgaben entsprechen. Alle geänderten vordefinierten Artefakte werden als **Vordefiniert (angepasst)** gekennzeichnet. Es ist nicht möglich, vordefinierte Artefakte zu entfernen, Sie können aber angepasste Artefakte wieder auf die ursprünglichen "vordefinierten" Werte zurücksetzen.

Bei Importieren des Inhalts vordefinierter Content Packs wird der Inhalt als **Vordefiniert** gekennzeichnet.

- Vordefinierte Content Packs müssen eindeutige Inhalte enthalten. Die Inhalte von vordefinierten Content Packs dürfen daher nicht identisch sein. Dies wird beim Export geprüft und ggf. in einer Fehlermeldung mitgeteilt.
- Vordefinierte Content Packs dürfen keine Inhalte enthalten, auf die verwiesen wird.
- Vordefinierte Content Packs können nicht geändert oder direkt gelöscht werden (im Gegensatz zu Artefakten, die geändert werden können). Wenn Sie Änderungen an einem

vordefinierten Content Pack vornehmen möchten, müssen Sie eine neue Version erstellen. Beim Import einer neuen vordefinierten Content Pack-Version wird die alte Version überschrieben.

Hinweis: Um ein vordefiniertes Content Pack zu ändern, wählen Sie **Eine neue Version der ausgewählten Content Pack-Definition erstellen** aus, und geben Sie eine neue Versionsnummer an. Weitere Informationen finden Sie unter "Erstellen einer neuen Version einer vordefinierten Content Pack-Definition" auf Seite 193.

Ein vordefiniertes Content Pack kann nur im Modus Content Pack-Entwicklung gelöscht werden. (Dieser wird unter Infrastruktureinstellungen: Operationenverwaltung - Content Manager - Einstellungen aktiviert).

Benutzerdefiniertes Content Pack

Bei benutzerdefinierten Content Packs handelt es sich um Sammlungen von Inhalt, der in der Regel vom BSM-Benutzer erstellt wird, z. B. zum Verwalten einer benutzerdefinierten, internen Applikation.

Bei Importieren des Inhalts benutzerdefinierter Content Packs wird der Inhalt als **Benutzerdefiniert** gekennzeichnet.

Die Inhalte benutzerdefinierter Content Packs dürfen mit den Inhalten anderer benutzerdefinierter oder vordefinierter Content Packs übereinstimmen.

Content Pack-Definitionen

Content Pack-Definitionen erfüllen zwei Zwecke:

- der Erstellung von Content Packs und der Artefakte, auf die sie verweisen, und
- der Beschreibung des vordefinierten Inhalts des Systems, der als Bestand an vordefiniertem Inhalt verwendet werden kann.

Eine Content Pack-Definition wird anhand ihres Namens und ihrer Version identifiziert. In einem System können nicht zwei Content Pack-Definitionen mit demselben Namen und derselben Version vorhanden sein. Eine Definition kann durch Angabe eines anderen Namens oder einer anderen Version dupliziert werden. Eine neue oder duplizierte Content Pack-Definition wird als benutzerdefinierte Definition gekennzeichnet.

Nur eine Content Pack-Definition mit einem Namen kann vordefiniert werden. Wenn ein Content Pack mit vordefinierten Inhalt basierend auf einer Content Pack-Definition mit demselben Namen importiert wird, wird die vorhandene Definition durch die zugehörige Definition ersetzt.

Vordefinierte Content Packs mit vordefiniertem Inhalt von HP werden während der BSM-Produktinstallation importiert. Sie können die vordefinierten Artefakte ändern, die dann als **Vordefiniert (angepasst)** gekennzeichnet sind. Angepasste Artefakte können auch wieder auf die ursprünglichen vordefinierten Werte zurückgesetzt, nicht aber gelöscht werden.

Exportieren und Importieren von Content Packs

Sie können eine Content Pack-Definition und darin enthaltenen Inhalt exportieren. Es gibt zwei Modi:

Modus "Normal"

Inhalt von exportierten Content Packs wird als **Benutzerdefiniert** gekennzeichnet.

Modus "Content Pack-Entwicklung"

Beim Exportieren eines Content Packs können Sie dessen Inhalt als **Vordefiniert** oder **Benutzerdefiniert** festlegen. Dabei spielt es keine Rolle, ob die als Grundlage für den Export verwendete Content Pack-Definition vordefiniert oder benutzerdefiniert ist.

Der Modus Content Pack-Entwicklung wird unter Operationenverwaltung - Content Manager - Infrastruktureinstellungen aktiviert.

Achtung: Es wird nicht empfohlen, neue Versionen vordefinierter Content Packs zu erstellen, für die Sie nicht zuständig sind, da dies in der Zukunft zu Upgrade-Fehlern führen kann.

Beim Importieren eines Content Packs ist der Inhalt abhängig vom Export des Content Packs vordefiniert oder benutzerdefiniert.

Oberflächen des Content Packs Manager

Der Content Packs Manager verfügt über folgende Oberflächen:

BSM - Content Packs-Benutzeroberfläche

Sie können den BSM Content Packs Manager über die folgenden Menüoptionen starten:

Admin > Plattform > Content Packs

Admin > Operationenverwaltung > Setup > Content Packs

Es sind zwei Modi zum Arbeiten mit Content Packs verfügbar:

- Normal Nur benutzerdefinierte Content Packs können geändert und exportiert werden.
- Content Pack-Entwicklung Beim Exportieren einer Content Pack-Definition können Sie angeben, ob sie vordefiniert oder benutzerdefiniert ist. Content Pack-Definitionen können geändert werden. Vordefinierte Content Pack-Definitionen können nicht geändert werden und müssen ggf. durch eine aktualisierte Version ersetzt werden.

Achtung: Es wird nicht empfohlen, neue Versionen vordefinierter Content Packs zu erstellen, für die Sie nicht zuständig sind, da dies in der Zukunft zu Upgrade-Fehlern führen kann.

Der Modus Content Pack-Entwicklung kann in der Einstellung Infrastruktur aktiviert werden:

Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen > Applikationen, verwenden Sie die Liste, um den Verwaltungskontext auf Operationenverwaltung festzulegen, und legen Sie den Eintrag Content Pack-Entwicklung aktivieren unter Operationenverwaltung - Content Manager - Einstellungen auf true fest.

Weitere Informationen finden Sie unter "Content Packs Manager-Benutzeroberfläche" auf Seite 202.

ContentManager-Befehlszeilenschnittstelle

Die Funktionen des Content-Pack-Managers können auch über die **ContentManager**-Befehlszeilenschnittstelle aufgerufen werden. Die **ContentManager**-Befehlszeilenschnittstelle lässt sich direkt, über eine Shell oder remote (z. B. über ein Skript) aufrufen.

Weitere Informationen finden Sie unter "Befehlszeilenschnittstelle für den Content Pack Manager" auf Seite 214.

Hinweis: Über die **ContentManager**-Befehlszeilenschnittstelle lassen sich keine Content Pack-Definitionen erstellen.

• ContentAutoUpload-Befehlszeilenschnittstelle

Währen der BSM-Installation werden alle vordefinierten Content Pack-Definitionsdateien automatisch vom Content Pack-Standardspeicherort auf dem Datenverarbeitungsserver hochgeladen:

<BSM-Stammverzeichnis>/conf/opr/content/<locale>

Mit ContentAutoUpload haben Sie folgende Möglichkeiten:

- erneutes Auslösen des Uploads vom Content Pack-Standardspeicherort
- Angeben eines anderen Ordners, von dem Content Packs hochgeladen werden sollen

Weitere Informationen finden Sie unter "Befehlszeilenschnittstelle für das automatische Hochladen von Content Packs" auf Seite 217.

Definieren von Content Packs

Eine Content Pack-Definition enthält eine Liste der Daten und der zwischen ihnen bestehenden Beziehungen, die einem Content Pack hinzugefügt werden sollen, das Sie in eine andere BSM-Installation exportieren können.

Hinweis: Die Content Pack-Definition selbst enthält keine CI-Typen. Verwenden Sie zum Austauschen von CI-Typen die Funktionen im Run-time Service Model (RTSM)

Im Bereich **Content Pack-Definitionen** können Sie die Content Pack-Definitionen anzeigen und verwalten. Sie können zum Beispiel die folgenden Aktionen durchführen:

- Erstellen, Ändern und Speichern einer Content Pack-Definition
- Löschen einer Content Pack-Definition
- Exportieren oder Importieren einer vorhandenen Definition mitsamt der Daten, auf die sie verweist

Das Erstellen eines Content Packs erfolgt in zwei Schritten. Zunächst erstellen Sie die Content Pack-Definition im Content Manager, um diese anschließend zum Exportieren des ausgewählten Inhalts in eine Content Pack-Datei zu verwenden.

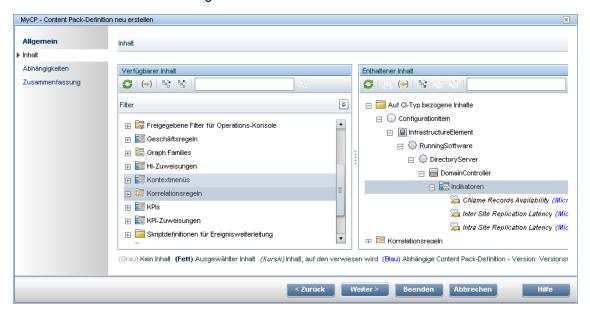
Abhängigkeiten in Content Packs

Einige Inhalte in BSM sind Teil einer Hierarchie, die mit anderen Inhalten in Zusammenhang stehen und davon abhängig sein können. Wenn Sie Inhalt zur Einbeziehung in ein Content Pack auswählen, muss der abhängige Inhalt ebenfalls eingebunden werden, entweder als Teil desselben Content Packs oder durch den Verweis von einem anderen Content Pack, das ebenfalls hochgeladen wird. Wenn Sie beispielsweise eine KPI-Zuweisung hinzufügen, müssen auch alle für diese KPI-Zuweisung erforderlichen Indikatoren, KPIs, Menüs und Regeln hinzugefügt werden.

Automatisches Einschließen abhängiger Inhalte

Wenn Sie Inhalt mit abhängigem Inhalt auswählen und der abhängige Inhalt nicht Teil eines anderen Content Packs ist, wird der abhängige Inhalt automatisch mit dem Inhalt, der ihn benötigt, in die Content Pack-Definition eingeschlossen.

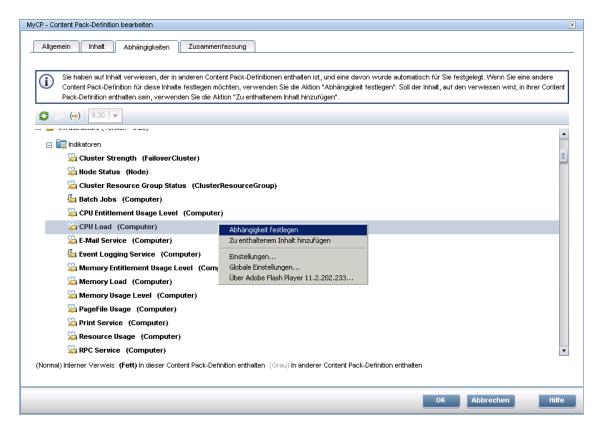
Beispiel: Die Korrelationsregel **DB-Verbindungsstatus für BB** erfordert zwei Indikatoren: den BB-Komponenten-Indikator **DB-Verbindungsstatus für BB** und den Datenbankindikator **Datenbankserverstatus**. Wenn Sie die Korrelationsregel **DB-Verbindungsstatus für BB** in einer Content Pack-Definition einschließen und die Indikatoren **DB-Verbindungsstatus für BB** und **Datenbankserverstatus** nicht in anderen Content Packs enthalten sind, werden sie automatisch in diese Content Pack-Definition eingeschlossen.



Festlegen der Abhängigkeit

Ist abhängiger Inhalt in mehreren Content Packs enthalten, können Sie wählen, auf welches Content Pack verwiesen werden soll. Dabei handelt es sich um das Festlegen der Abhängigkeit.

Wenn die Content Packs A und B beispielsweise beide den Indikator CPU-Auslastung haben und Sie die Korrelationsregel Datenbank wirkt sich auf WebApp aus (die von CPU-Auslastung abhängig ist) zur Einbeziehung in Content Pack C auswählen, können Sie die Abhängigkeit in Content Pack C so festlegen, dass sie entweder in Content Pack A oder B auf CPU-Auslastung verweist.



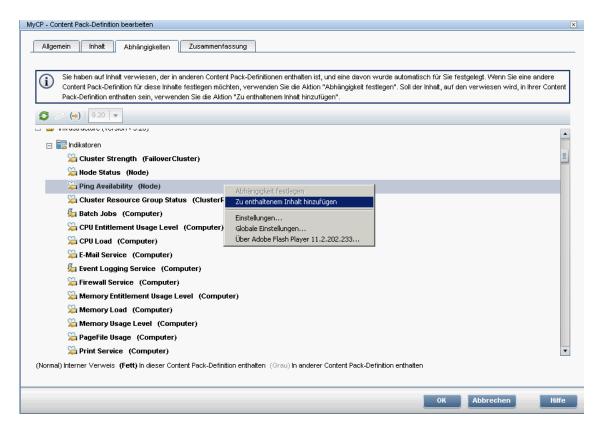
Verweisen auf abhängigen Inhalt, der in einem anderen Content Pack enthalten ist

Ist abhängiger Inhalt bereits in einem anderen Content Pack enthalten, verweist das neue Content Pack standardmäßig auf die Einbeziehung im anderen Content Pack, statt den Inhalt ebenfalls einzubeziehen. Auf der Seite **Abhängigkeiten** können Sie diesen jedoch auch dem im neuen Content Pack enthaltenen Inhalt hinzufügen.

Wenn Content Pack-Definition A beispielsweise den Indikator **Ping-Verfügbarkeit** enthält und Sie jetzt die Korrelationsregel **Datenbank wirkt sich auf WebApp aus** (die abhängig ist von **Ping-Verfügbarkeit**) zur Einbeziehung in Content Pack B auswählen, verweist Content Pack B auf die Einbeziehung von **Ping-Verfügbarkeit** in Content Pack A.

Auf der Seite mit den Abhängigkeiten von Content Pack B ist **Ping-Verfügbarkeit** fett formatiert unter Content Pack A aufgeführt. Die Abhängigkeit wird automatisch festgelegt. Um **Ping-Verfügbarkeit** in Content Pack B einzubeziehen (und somit in beide Content Packs), wählen Sie den Indikator aus, und klicken Sie auf **Zu enthaltenem Inhalt hinzufügen**.

Hinweis: Es wird nicht empfohlen, Inhalt in mehrere Content Packs einzuschließen. Es empfiehlt sich, Abhängigkeiten zwischen Content Packs festzulegen.



Löschen eines Content Packs, auf das verwiesen wird

Wenn Sie ein Content Pack mit abhängigem Inhalt, auf das verwiesen wird, löschen, wird der abhängige Inhalt automatisch der Definition des Content Packs hinzufügt, das davon abhängig ist.

Wenn Content Pack B beispielsweise die Korrelationsregel **Datenbank wirkt sich auf WebApp aus** enthält und auf den abhängigen Indikator **TS erweitern** in Content Pack A verweist und Sie Content Pack A löschen, wird **TS erweitern** automatisch Content Pack B hinzugefügt.

Hinweis: Sie werden über eine Popup-Meldung gewarnt, wenn Sie ein Content Pack mit abhängigem Inhalt löschen, auf das verwiesen wird.

Löschen von Content Packs, auf die verwiesen wird und für die die Abhängigkeit festgelegt wurde

Wenn Sie ein Content Pack löschen, auf das verwiesen wird und für das die Abhängigkeit festgelegt wurde, wird der abhängige Inhalt automatisch der Definition des Content Packs hinzufügt, das davon abhängig ist. Sie können die Abhängigkeit manuell auf ein anderes Content Pack ändern, doch wird dies nicht automatisch festgelegt.

Wenn die Content Packs A und B beispielsweise beide den Indikator **TS erweitern** enthalten und Content Pack C die Korrelationsregel **Datenbank wirkt sich auf WebApp aus** (die abhängig ist von **TS erweitern**) enthält und eine Abhängigkeit mit dem Verweis auf **TS erweitern** in Content Pack A hat und Sie Content Pack A dann löschen, wird **TS erweitern** automatisch Content Pack C hinzugefügt. Sie können die Abhängigkeit dann auf **TS erweitern** in Content Pack B festlegen, doch erfolgt diese nicht automatisch.

Exportieren von Content Packs

Mithilfe des Content Packs Manager können Sie Konfigurationsdaten in eine Datei exportieren. Das Content Pack enthält die Verweise auf Konfigurationsdaten und die Daten, auf die verwiesen wird.

Die Konfigurationsdaten in einem Content Pack verweisen auf Konfigurationselemente, die im Runtime Service Model (RTSM) gespeichert sind, das von dem System verwendet wird, aus dem das Content Pack exportiert wurde. Wenn die Konfigurationselemente nicht in dem RTSM vorhanden sind, das von dem System verwendet wird, in das Sie das Content Pack importieren wollen, können die Konfigurationsdaten im Content Pack nicht funktionieren.

Tipp: Verwenden Sie die vom RTSM bereitgestellten Features zum Exportieren und Importieren von Konfigurationselementen.

Weitere Informationen zum Exportieren von Content Packs finden Sie unter "Erstellen und Verwalten von Content Packs" auf Seite 193.

Importieren von Content Packs

Beim Importieren eines Content Packs überschreiben Sie vorhandene Daten in der Regel und fügen etwaige neue Daten hinzu. Beim Importieren eines vordefinierten Content Packs wird nur vordefinierter Inhalt mit neuen Daten überschrieben. Angepasster Inhalt bleibt unverändert. Beim Importieren eines benutzerdefinierten Content Packs werden die vorhandenen Daten immer überschrieben.

Wenn Sie den Importvorgang testen wollen, ohne die aufgelisteten Daten jedoch tatsächlich zu importieren, können Sie die Funktion **Testen** verwenden. Die Funktion **Testen** ist eine hilfreiche Methode, um unaufgelöste Abhängigkeiten (z. B. mit unbekannten CI-Typen) in der importierten Content Pack-Definition aufzulisten.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen und Verwalten von Content Packs" auf der nächsten Seite. Weitere Informationen zur Benutzeroberfläche und den im Importvorgang verfügbaren Optionen finden Sie unter "Dialogfeld "Content Pack importieren" auf Seite 213.

Erstellen und Verwalten von Content Packs

In den folgenden Schritten wird das Erstellen, Exportieren und Importieren von Content Packs beschrieben.

Erstellen und Bearbeiten von Content Pack-Definitionen

So erstellen und bearbeiten Sie eine Content Pack-Definition:

- 1. Öffnen Sie den Content Packs Manager: Admin > Plattform > Content Packs.
 - Zum Erstellen einer neuen Content Pack-Definition klicken Sie auf die Schaltfläche
 Der Assistent zum Erstellen einer neuen Content Pack-Definition wird geöffnet.
 - Zum Bearbeiten einer vorhandenen Content Pack-Definition wählen Sie diese aus und klicken Sie auf
 Das Dialogfeld Content Pack-Definition bearbeiten wird geöffnet.
- 2. Die Felder **Anzeigename**, **Name** und **Version** auf der Seite **Allgemein** des Assistenten bzw. der Registerkarte **Allgemein** des Dialogfelds sind erforderlich.
 - Die Kombination aus **Name** und **Version** muss eindeutig sein.
 - Das Feld **Name** darf maximal 255 Zeichen lang sein. Das erste Zeichen muss ein Buchstabe (A-Z, a-z) oder ein Unterstrich (_) sein. Alle weiteren Zeichen können Buchstaben, Zahlen oder Unterstriche sein. Leerzeichen am Anfang oder am Ende sind nicht erlaubt. Beim Exportieren des Content Packs ist dies der Standarddateiname für die Datei, wobei **OMi Content Pack** als Präfix verwendet wird.
 - Anzeigename ist der in der Liste Content Pack-Definitionen angezeigte Name, der nicht eindeutig sein muss. Maximal 255 Zeichen sind in diesem Feld zulässig.
 - Version ist ein freies Textfeld. Verwenden Sie Version in Kombination mit Anzeigename, um die Revisionskontrolle für Ihre Content Packs zu verwalten.
- 3. Folgen Sie den weiteren Seiten des Assistenten oder bearbeiten Sie die Registerkarten des Dialogfelds, um Inhalt auszuwählen, Abhängigkeiten festzulegen und eine Übersicht des Inhalts Ihrer Content Pack-Definition und evenuell aufgetretener Probleme anzuzeigen.

Weitere Informationen zur Benutzeroberfläche und allen verfügbaren Optionen finden Sie unter "Assistent zum Erstellen einer neuen Content Pack-Definition" auf Seite 205.

Erstellen einer neuen Version einer vordefinierten Content Pack-Definition

So erstellen Sie eine neue Version einer vordefinierten Content Pack-Definition:

1. Stellen Sie sicher, dass die Einstellung Content Pack-Entwicklung aktivieren aktiviert ist:

Achtung: Es wird nicht empfohlen, neue Versionen vordefinierter Content Packs zu erstellen, für die Sie nicht zuständig sind, da dies in der Zukunft zu Upgrade-Fehlern führen kann.

- a. Öffnen Sie **Infrastruktureinstellungen** in der Plattformverwaltung:
 - Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen
- b. Wählen Sie Applikationen aus und setzen Sie den Verwaltungskontext unter Verwendung

der Liste auf Operationenverwaltung.

- c. Aktivieren Sie die Einstellung **Content Pack-Entwicklung aktivieren** im Content Manager-Bereich.
- Öffnen Sie den Content Packs Manager: Admin > Plattform > Content Packs, und wählen Sie die vordefinierte Content Pack-Definition aus, für die Sie eine neue Version erstellen möchten.
- 3. Klicken Sie auf die Schaltfläche , um das Dialogfeld Neue Version für eine Content Pack-Definition erstellen zu öffnen.
- 4. Ändern Sie die Versionsnummer des Content Packs, und klicken Sie auf **OK**.
 - Die neue Version dieses Content Packs wird als benutzerdefiniertes Content Pack gespeichert.
- 5. Öffnen Sie die neue Version der Content Pack-Definition, nehmen Sie die erforderlichen Änderungen vor, und speichern Sie die Änderungen.

Weitere Informationen zur Benutzeroberfläche und allen verfügbaren Optionen finden Sie unter "Assistent zum Erstellen einer neuen Content Pack-Definition" auf Seite 205.

Exportieren von Content Packs

So exportieren Sie ein Content Pack:

- 1. Öffnen Sie den Content Packs Manager: Admin > Plattform > Content Packs
- 2. Wählen Sie im Bereich **Content Pack-Definitionen** das Content Pack aus, das Sie exportieren wollen.
- 3. Um das ausgewählte Content Pack in eine Datei zu exportieren, klicken Sie auf die Schaltfläche , wählen Sie den Speicherort aus, an dem das Content Pack gespeichert werden soll, und klicken Sie auf **Speichern**.

Tipp: Standardmäßig speichert BSM das Content Pack im Dateisystem des Systems, auf dem Sie den Content Packs Manager ausführen. Wenn Sie die Datei an einem anderen Speicherort speichern wollen, stellen Sie sicher, dass Sie Zugriff auf diesen Speicherort haben. Der Standarddateityp ist ZIP.

Exportieren vordefinierter Content Packs

So exportieren Sie ein vordefiniertes Content Pack:

1. Stellen Sie sicher, dass die Einstellung Content Pack-Entwicklung aktivieren aktiviert ist:

Achtung: Es wird nicht empfohlen, neue Versionen vordefinierter Content Packs zu erstellen, für die Sie nicht zuständig sind, da dies in der Zukunft zu Upgrade-Fehlern führen kann.

a. Öffnen Sie Infrastruktureinstellungen in der Plattformverwaltung:

Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen

b. Wählen Sie Applikationen aus und setzen Sie den Verwaltungskontext unter Verwendung

der Liste auf Operationenverwaltung.

- c. Aktivieren Sie die Einstellung **Content Pack-Entwicklung aktivieren** im Content Manager-Bereich.
- Öffnen Sie den Content Packs Manager: Admin > Plattform > Content Packs
 Wählen Sie im Bereich Content Pack-Definitionen das Content Pack aus, das Sie exportieren wollen.
- 3. Um das ausgewählte Content Pack in eine Datei zu exportieren, wählen Sie Content PackDefinitionen und Inhalt exportieren (vordefiniert) aus, klicken Sie auf die Schaltfläche geben Sie den Speicherort an, an dem das Content Pack gespeichert werden soll, und klicken Sie auf Speichern.

Tipp: Standardmäßig speichert BSM das Content Pack im Dateisystem des Systems, auf dem Sie den Content Packs Manager ausführen. Wenn Sie die Datei an einem anderen Speicherort speichern wollen, stellen Sie sicher, dass Sie Zugriff auf diesen Speicherort haben. Der Standarddateityp ist ZIP.

Importieren von Content Packs

So importieren Sie ein Content Pack:

Hinweis: In SaaS-Installationen können vordefinierte Content Packs nur von einem SaaS-Admin (Superuser) importiert werden.

- 1. Öffnen Sie den Content Packs Manager: Admin > Plattform > Content Packs
 - Klicken Sie auf die Schaltfläche im Bereich Content Pack-Definitionen, um das Dialogfeld Content Pack importieren zu öffnen.
- 2. Verwenden Sie die Schaltfläche **Durchsuchen (...)** im Dialogfeld **Content Pack importieren**, um das zu importierende Content Pack zu suchen. Content Packs liegen normalerweise im ZIP-Format vor. Es können aber auch Content Packs im XML-Format importiert werden.

Der Standardspeicherort für Content Packs lautet:

<HPBSM-Stammverzeichnis>conf\opr\content\<Gebietsschema>

In einer verteilten Umgebung befindet sich das Verzeichnis auf dem Datenverarbeitungsserver.

Hinweis: Standardmäßig sucht BSM Content Packs im Dateisystem des Systems, auf dem Sie die Browsersitzung starten. Wird der Browser auf einem Remotesystem ausgeführt, müssen Sie zum Dateisystem des BSM-Hosts navigieren.

3. *Optional:* Sie können **Testen** auswählen, um den Importvorgang im Testmodus auszuführen. Im Testmodus wird kein Commit der Änderungen durchgeführt und Sie können sehen, ob Probleme vorliegen, bevor Sie den eigentlichen Importvorgang durchführen.

Hinweis: Vorhandene Elemente mit identischer ID werden in der Regel überschrieben.

Beim Importieren eines vordefinierten Content Packs wird nur vordefinierter Inhalt mit neuen Daten überschrieben. Angepasster Inhalt bleibt unverändert. Beim Importieren eines benutzerdefinierten Content Packs werden die vorhandenen Daten immer überschrieben.

Nicht aufgelöste Referenzen (z. B. zu bekannten CI-Typen) sind in der importierten Definition nicht zulässig.

4. Klicken Sie auf **Importieren**, um den Import- oder Testvorgang zu starten.

Hinweis: Sie können keinen Importvorgang starten, wenn bereits ein Importvorgang ausgeführt wird.

Weitere Informationen zum Dialogfeld **Content Pack importieren** finden Sie unter "Dialogfeld "Content Pack importieren" auf Seite 213.

Prüfliste für das Veröffentlichen von Content Packs

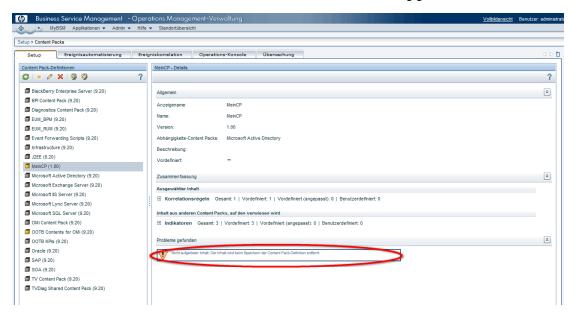
Führen Sie vor dem Veröffentlichen eines neu entwickelten Content Packs folgende Überprüfungen auf einem System aus, auf dem alle verfügbaren Content Packs (zumindest alle OOTB-Content Packs) sowie Ihr Content Pack importiert sind.

Anhand dieser Überprüfungen wird der Besitz der Inhaltsartefakte eindeutig ersichtlich, was bei Upgrades und bei der Entwicklung neuer Content Packs äußerst hilfreich ist.

Vom Content Manager gefundene Probleme

Wählen Sie im Content Manager die Content Pack-Definition aus, und prüfen Sie, ob im unteren Bereich des Ausschnitts **Details** der Bereich **Probleme gefunden** angezeigt wird.

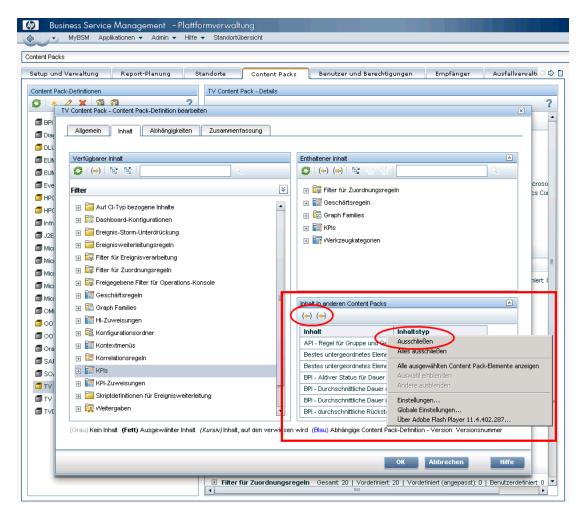
In diesem Abschnitt werden normalerweise Inkonsistenzen zwischen Ihrer Content Pack-Definition und dem verfügbaren Inhalt gemeldet. Sie müssen die gemeldeten Probleme beheben, bevor Sie das Content Pack exportieren. Beispiel: Die Content Pack-Definition verweist auf Inhalt oder anhängigen Inhalt, der im System nicht vorhanden ist. Entweder müssen Sie den Inhalt, auf den verwiesen wird, oder die Abhängigkeit aus der Content Pack-Definition entfernen oder sicherstellen, dass der Inhalt, auf den verwiesen wird, oder die Abhängigkeit "installiert" ist.



Überprüfen auf Inhalt in anderen Content Packs

Öffnen Sie die Content Pack-Definition zum Bearbeiten im Content Manager, und wählen Sie die Registerkarte Inhalt aus. Überprüfen Sie, ob ein Abschnitt namens Inhalt in anderen Content Packs (unten im Ausschnitt Enthaltener Inhalt) angezeigt wird.

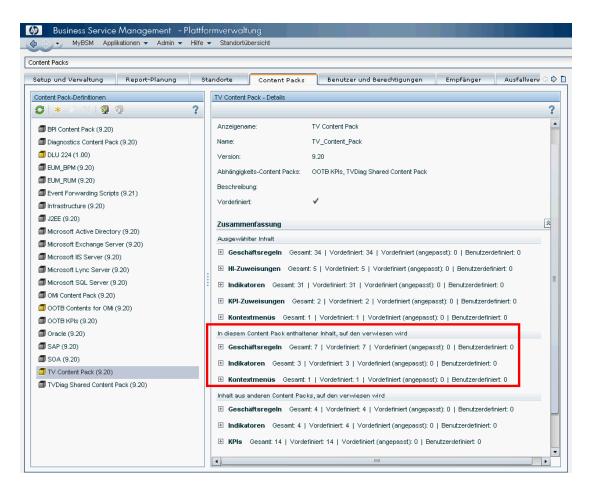
Prüfen Sie im Abschnitt Inhalt in anderen Content Packs die einzelnen Inhaltsartefakte, und stellen Sie fest, ob Sie wirklich der Besitzer des jeweiligen Inhaltsartefakts sind. Wenn Sie nicht der Besitzer sind, schließen Sie das Inhaltsartefakt aus der Content Pack-Definition aus, und legen Sie eine Abhängigkeit zum entsprechenden Content Pack fest. Sie können auch den Besitzer der anderen Content Packs kontaktieren und diesen bitten, das Inhaltsartefakt aus seiner Content Pack-Definition auszuschließen.



Überprüfen auf in diesem Content Pack enthaltenen Inhalt, auf den verwiesen wird

Wählen Sie im Content Manager die Content Pack-Definition aus, und prüfen Sie, ob im Ausschnitt **Details** der Bereich **In diesem Content Pack enthaltener Inhalt, auf den verwiesen wird** angezeigt wird.

Es wird nicht empfohlen, im eigenen Content Pack Inhalt zu haben, auf den verwiesen wird, da dies ein Hinweis darauf ist, dass der Besitz solchen Inhalts nicht eindeutig ist. Wenn Sie der Besitzer sind, schließen Sie den Inhalt, auf den verwiesen wird, in Ihre Content Pack-Definition ein. Wenn nicht, legen Sie eine Abhängigkeit zu der Content Pack-Definition fest, in dessen Besitz sich der Inhalt befindet, auf den verwiesen wird.

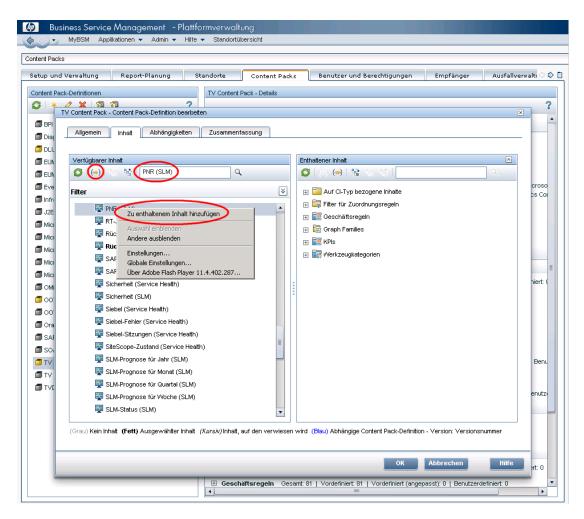


Einschließen des Inhalts, auf den verwiesen wird, in die eigene Content Pack-Definition

Öffnen Sie die Content Pack-Definition zum Bearbeiten im Content Manager, und wählen Sie die Registerkarte **Inhalt** aus.

Suchen Sie nach dem Inhalt, auf den verwiesen wird, und schließen Sie ihn in Ihre Content Pack-Definition ein.

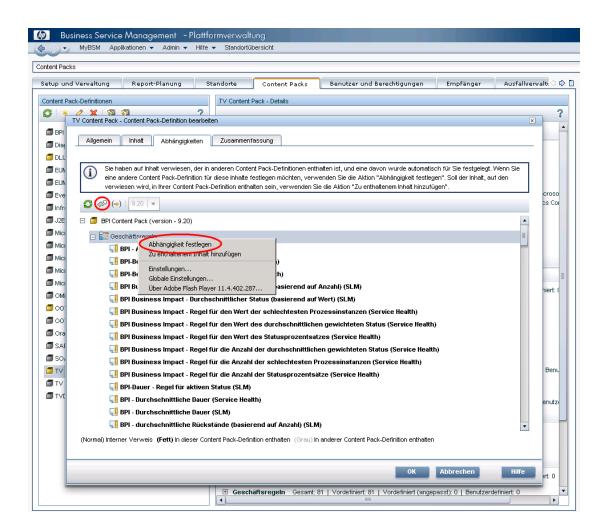
Stellen Sie sicher, dass Sie die oben beschriebenen Schritte ausgeführt haben.



Festlegen einer Abhängigkeit

Öffnen Sie Ihre Content Pack-Definition zum Bearbeiten im Content Manager, und wählen Sie die Registerkarte **Abhängigkeiten** aus.

Prüfen Sie alle Inhaltsartefakte, die in normaler Schrift angezeigt werden. Wählen Sie das Content Pack aus, in dessen Besitz das Artefakt ist, auf das verwiesen wird, und legen Sie die Abhängigkeit zu diesem fest. Ziel ist es, dass keine Inhaltsartefakte in normaler Schrift auf der Registerkarte **Abhängigkeiten** angezeigt werden.



Content Packs Manager-Benutzeroberfläche

Seite "Content Packs"

In diesem Bereich können Sie Content Pack-Definitionen verwalten. In einer Content Pack-Definition werden die im Content Pack enthaltenen Elemente beschrieben. Ein Content Pack enthält eine Baseline der Konfigurationsdaten und andere Elemente, die Sie für die Verwaltung der Ressourcen in der mit BSM überwachten IT-Umgebung definiert haben. Im Content Packs Manager wird eine Liste der bekannten Content Pack-Definitionen angezeigt.

Zugriff	Führen Sie einen der folgenden Schritte aus:	
	Admin > Plattform > Content Packs	
	Admin > Operationenverwaltung > Setup > Content Packs	
Wichtiger Hinweis	In BSM können Aktionen entweder über Schaltflächen oder über Menüelemente ausgeführt werden. Für die Schaltflächen im Ausschnitt Content Pack- Definitionen gibt es daher auch entsprechende Optionen in Kontextmenüs.	
Relevante Aufgaben	"Erstellen und Verwalten von Content Packs" auf Seite 193	
Siehe auch	" Content Packs" auf Seite 182	

Ausschnitt "Definitionen"

Im Ausschnitt **Content Pack-Definitionen** wird eine Liste aller Content Pack-Definitionen angezeigt, die für Ihre Umgebung zur Verfügung stehen.

Die Elemente der Benutzeroberfläche werden in der folgenden Tabelle aufgeführt.

Elemente der Oberfläche	Beschreibung
S	Aktualisieren. Aktualisiert den Inhalt der angezeigten Liste. Verwenden Sie dieses Element, wenn während der Arbeit neue Inhalte verfügbar werden oder wenn Sie neue Inhalte heraufgeladen haben (z. B. über die Befehlszeilenschnittstelle).
*	Neues Element. Öffnet den Assistenten zum Erstellen einer neuen Content Pack- Definition. Details zum Assistenten finden Sie unter "Assistent zum Erstellen einer neuen Content Pack-Definition" auf Seite 205.

Elemente der	
Oberfläche	Beschreibung
	Eine neue Version der ausgewählten Content Pack-Definition erstellen. Öffnet das Dialogfeld Neue Version für eine Content Pack-Definition erstellen, in dem Sie eine neue Version der ausgewählten Content Pack-Definition erstellen können.
	Sie können auch auf einen Abschnitt im Ausschnitt Details doppelklicken, um die entsprechende Registerkarte im Dialogfeld Neue Version für eine Content Pack-Definition erstellen oder die Content Pack-Definition im Ausschnitt Definitionen zu öffnen. (Dies gilt nicht bei nicht vordefinierten Content Packs.)
	Weitere Informationen finden Sie unter "Erstellen einer neuen Version einer vordefinierten Content Pack-Definition" auf Seite 193.
0	Element bearbeiten. Öffnet das Dialogfeld zum Bearbeiten der Content Pack-Definition, in dem Sie den Namen, die Version, die Beschreibung, den Inhalt und die Abhängigkeiten für das ausgewählte Content Pack bearbeiten können. Dieses Dialogfeld enthält die gleichen Bildschirme wie der Assistent zum Erstellen einer neuen Content Pack-Definition, allerdings im Registerkartenformat.
	Sie können auch auf einen Abschnitt im Ausschnitt Details doppelklicken, um die entsprechende Registerkarte im Dialogfeld Content Pack-Definition bearbeiten oder die Content Pack-Definition im Ausschnitt Definitionen zu öffnen. (Dies gilt nicht bei vordefinierten Content Packs.)
	Weitere Informationen finden Sie unter "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205.
×	Element löschen. Löscht die ausgewählte Content Pack-Definition (aber keinen referenzierten Inhalt wie Indikatoren und KPIs) aus der Liste der angezeigten Definitionen.
2	Content Pack-Definitionen und Inhalt importieren. Öffnet das Dialogfeld Content Pack importieren, in dem Sie eine Datei angeben oder zu dieser navigieren können, die die zu importierenden Definitionsdetails enthält.
	Sie können den Import zunächst im Testmodus ausführen, bei dem keine Änderungen vorgenommen werden. Nicht aufgelöste Referenzen (z. B. zu bekannten CI-Typen) sind in der importierten Definition nicht zulässig. Weitere Informationen finden Sie unter "Dialogfeld "Content Pack importieren"" auf Seite 213.

Elemente der Oberfläche	Beschreibung
a	Content Pack-Definitionen und Inhalt exportieren. Öffnet das Dialogfeld Speicherort für Download auswählen, in dem Sie einen Dateispeicherort angeben oder zu diesem navigieren können, in den Sie die Definitionsdetails exportieren möchten.
	Content Pack-Definitionen und Inhalt exportieren (vordefiniert). Öffnet das Dialogfeld Speicherort für Download auswählen, in dem Sie einen Dateispeicherort angeben oder zu diesem navigieren können, in den Sie die Definitionsdetails als vordefiniertes Content Pack exportieren möchten.

Ausschnitt "Details"

Im Ausschnitt **Details** befinden sich allgemeine Informationen zu den Eigenschaften der ausgewählten Content Pack-Definition und eine kurze Zusammenfassung der Inhalte der Content Pack-Definition und eventuell gefundener Probleme.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Allgemein	Zeigt den Namen, den Anzeigenamen, die Version, abhängige Content Packs, eine Beschreibung der ausgewählten Content Pack-Definition und ihren Ursprung (ob sie vordefiniert ist) an.

Elemente der Oberfläche	Beschreibung
Übersicht	Zeigt eine Übersicht über den Inhalt der ausgewählten Content Pack-Definition an. Diese Übersicht ist in die folgenden Unterbereiche aufgeteilt. Jeder Unterbereich enthält eine Inhaltsliste und für jedes Element in der Liste werden folgende Informationen angezeigt:
	Gesamtanzahl der Artefakte
	Anzahl der vordefinierten Artefakte
	Anzahl der vordefinierten (benutzerdefinierten) Artefakte
	Anzahl der benutzerdefinierten Artefakte
	Wenn Sie die Inhaltsgruppe einblenden, werden die in dieser Gruppe enthaltenen Artefakte, der CI-Typ des Artefakts und der Ursprung des Artefakts (Vordefiniert, Vordefiniert (Benutzerdefiniert), Benutzerdefiniert) angezeigt.
	Ausgewählter Inhalt. Zeigt gruppiert nach Inhaltstyp eine Liste des Inhalts an, der in der ausgewählten Content Pack-Definition enthalten ist.
	 In diesem Content Pack enthaltener Inhalt, auf den verwiesen wird. Zeigt gruppiert nach Inhaltstyp eine Liste des referenzierten Inhalts an, der in diesem Content Pack enthalten ist.
	 Inhalt aus anderen Content Packs, auf den verwiesen wird. Zeigt gruppiert nach Inhaltstyp eine Liste des abhängigen Inhalts an, auf den in anderen Content Packs verwiesen wird.
Probleme gefunden	Zeigt Informationen zu vorliegenden Problemen an, wie nicht aufgelöste Abhängigkeiten (Inhalte, die in der ausgewählten Content Pack-Definition enthalten sind, aber in BSM nicht mehr vorhanden sind), die in der ausgewählten Content Pack-Definition festgestellt wurden.

Assistent zum Erstellen einer neuen Content Pack- Definition

Dieser Assistent ermöglicht Ihnen das Erstellen einer neuen Content Pack-Definition. Sie können einen Namen, die Version und Beschreibung bereitstellen, den Inhalt auswählen, Abhängigkeiten festlegen und Probleme diagnostizieren.

Zugriff	Führen Sie einen der folgenden Schritte aus:
	Admin > Plattform > Content Packs
	Admin > Operationenverwaltung > Inhalt verwalten > Content Packs
	Klicken Sie anschließend auf **.

Relevante Aufgaben	"Erstellen und Verwalten von Content Packs" auf Seite 193
Aufbau des	Dieser Assistent besteht aus folgenden Elementen:
Assistenten	"Seite "Allgemein" " unten > "Seite "Inhalt"" auf der nächsten Seite > "Seite "Abhängigkeiten"" auf Seite 211 > "Seite "Zusammenfassung"" auf Seite 212
Siehe auch	" Content Packs" auf Seite 182

Seite "Allgemein"

Auf dieser Seite des Assistenten können Sie den Anzeigenamen, den Namen, die Version und die Beschreibung für ein neues Content Package definieren.

Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent zum Erstellen einer neuen Content Pack-Definition " auf der vorherigen Seite.
	Diese Seite des Assistenten wird als Registerkarte Allgemein im Dialogfeld zum Bearbeiten der Content Pack-Definition angezeigt, das geöffnet wird, wenn Sie auf klicken.
Aufbau des Assistenten	Der "Assistent zum Erstellen einer neuen Content Pack-Definition " auf der vorherigen Seite besteht aus folgenden Elementen:
	Seite "Allgemein" > "Seite "Inhalt"" auf der nächsten Seite > "Seite "Abhängigkeiten"" auf Seite 211 > "Seite "Zusammenfassung"" auf Seite 212
Siehe auch	" Content Packs" auf Seite 182

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
ID	Keine Aktion erforderlich. Die Content Pack-ID wird bei der Erstellung des Content Packs automatisch zugewiesen.
	Hinweis: Das ID-Feld wird nur auf der Registerkarte Allgemein des Dialogfelds zum Bearbeiten der Content Pack-Definition angezeigt, und nicht auf der Seite Allgemein des Assistenten Neue Content Pack-Definition erstellen .
Anzeigename	Der Name, der in der Liste Content Pack-Definitionen angezeigt wird. Dieser Name muss nicht eindeutig sein. Er darf maximal 255 Zeichen lang sein.

Elemente der Oberfläche	Beschreibung
Name	Der Name der Content Pack-Definition, der maximal 255 Zeichen lang sein darf. Das erste Zeichen muss ein Buchstabe (A-Z, a-z) oder ein Unterstrich (_) sein. Alle weiteren Zeichen können Buchstaben, Zahlen oder Unterstriche sein. Leerzeichen am Anfang oder am Ende sind nicht erlaubt.
	Hinweis: Die Kombination aus Name und Version muss eindeutig sein.
	Beim Exportieren des Content Packs ist dies der Standarddateiname für die Datei, wobei OMi Content Pack - als Präfix verwendet wird.
Version	Erforderliches, freies Textfeld. Hiermit können Sie die Versionen Ihrer Content Packs überwachen. Maximal 255 Zeichen sind in diesem Feld zulässig.
Beschreibung	Kurze Beschreibung (beschränkt auf 1024 Zeichen) der Content Pack- Definition, die Sie dem Ausschnitt Content Pack-Definitionen hinzufügen möchten (oder dort markiert haben). Über das Feld Beschreibung können Sie andere Benutzer über den Zweck und Inhalt des Content Packs informieren.
Vordefiniert	Bei vordefiniertem Inhalt handelt es sich in der Regel um von HP oder HP-Partnern bereitgestellten Inhalt, der für die Erstkonfiguration einer BSM-Installation verwendet wird. Nach der Installation eines vordefinierten Content Packs können Sie diese anfänglichen Artefakte ändern, sodass sie den Anforderungen Ihrer Umgebung und Verwaltungsaufgaben entsprechen. Alle geänderten vordefinierten Artefakte werden als Vordefiniert (angepasst) gekennzeichnet. Es ist nicht möglich, vordefinierte Artefakte zu entfernen, Sie können aber angepasste Artefakte wieder auf die ursprünglichen "vordefinierten" Werte zurücksetzen.
	Hinweis: Wird nur im Bereich Details angezeigt.

Seite "Inhalt"

Auf dieser Assistentenseite können Sie den Inhalt auswählen, der in eine neue Content Pack-Definition aufgenommen werden soll.

Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205.
	 Diese Seite des Assistenten wird als Registerkarte Inhalt im Dialogfeld zum Bearbeiten der Content Pack-Definition angezeigt, das geöffnet wird, wenn Sie auf klicken.
Aufbau des Assistenten	Der "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205 besteht aus folgenden Elementen:
	"Seite "Allgemein" " auf der vorherigen Seite > Seite "Inhalt" > "Seite "Abhängigkeiten"" auf Seite 211 > "Seite "Zusammenfassung"" auf Seite 212
Siehe auch	" Content Packs" auf Seite 182

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
©	Aktualisieren: Aktualisiert den Inhalt der angezeigten Liste. Verwenden Sie dieses Element, wenn während der Arbeit neue Inhalte verfügbar werden oder wenn Sie neue Inhalte heraufgeladen haben (z. B. über die Befehlszeilenschnittstelle).
(→)	Zu enthaltenem Inhalt hinzufügen: Fügt die ausgewählten Elemente der Liste enthaltener Inhalte hinzu.
	Falls enthaltener Inhalt bereits in ein anderes Content Pack eingeschlossen wurde, ist er im Ausschnitt Inhalt in anderen Content Packs aufgeführt und kann problemlos aus dem Content Pack, das Sie gerade erstellen, ausgeschlossen werden. Es ist nicht erforderlich, Inhalt in mehrere Content Packs einzuschließen.
	Tipps: Beim Auswählen eines CI-Typs wird automatisch jeder zugewiesene Inhalt des CI-Typs sowie auch der jeder zugewiesene Inhalt untergeordneter CI-Typen ausgewählt. Beim Auswählen bestimmter Inhalte, z. B. einem einzelnen Indikator oder KPI, wird automatisch der Verweis auf den CI-Typ, mit dem der Inhalt verbunden ist, ausgewählt.
	Auswahl einblenden: Blendet die Liste Verfügbarer Inhalt oder Enthaltener Inhalt ein, um Elemente anzuzeigen, die zur ausgewählten Gruppe gehören.
86	Andere ausblenden: Blendet alle offenen Verzweigungen mit Ausnahme der ausgewählten Verzweigung aus.
*	Einblenden : Blendet den Ausschnitt Filtern ein, um verfügbare Filter anzuzeigen.
*	Ausblenden: Blendet den Ausschnitt Filtern aus.
±	Blendet den ausgewählten Ordner ein.
⊟	Blendet den ausgewählten Ordner aus.
(4)	Ausschließen: Entfernt die ausgewählten Elemente aus der Liste enthaltener Inhalte.
(👄)	Alles ausschließen: Entfernt alle Elemente aus der Liste enthaltener Inhalte.
않	Alle ausgewählten Content Pack-Elemente anzeigen: Blendet die Liste Enthaltener Inhalt ein, um alle zum Einschließen in das Content Pack ausgewählten Elemente anzuzeigen.

Elemente der Oberfläche	Beschreibung
Q	Inhalt durchsuchen: Verwenden Sie das Suchfeld, um Inhalt im Ausschnitt Verfügbarer Inhalt oder Enthaltener Inhalt zu suchen. Geben Sie eine
	Suchzeichenfolge in das Suchfeld ein und klicken Sie auf . Der erste Inhalt, der mit der angegebenen Zeichenfolge übereinstimmt, wird markiert. Ist der Inhalt zunächst nicht sichtbar, wird er in der Struktur
	eingeblendet. Klicken Sie erneut auf , um die nächste Instanz von Inhalt zu finden, der mit der angegebenen Zeichenfolge übereinstimmt.
	Die Suchzeichenfolge muss aus mindestens 3 Zeichen bestehen. Sobald Sie das dritte Zeichen eingegeben haben, wird die Suche automatisch gestartet und der erste Treffer wird hervorgehoben. Diese Voreinstellung bewirkt, dass keine unnötigen Suchläufe gestartet und Ressourcen blockiert werden. Namen mit weniger als drei Zeichen finden Sie, indem Sie auf die Schaltfläche klicken.
Verfügbarer	Hierarchische Liste mit dem verfügbaren Inhalt in Ihrer IT-Umgebung.
Inhalt	Tipp: Wenn Sie einer Content Pack-Definition Inhalt hinzufügen möchten, ziehen Sie diesen aus dem Ausschnitt Verfügbarer Inhalt in den Ausschnitt Enthaltener Inhalt oder markieren Sie ihn und klicken Sie auf die Schaltfläche Zu enthaltenem Inhalt hinzufügen. BSM warnt Sie bei diesem Vorgang, wenn der Inhalt bereits in anderen Content Packs vorhanden ist.
	Farbcodierung:
	Kein Inhalt: Grau
	Ausgewählter Inhalt: Fett
	Inhalt, auf den verwiesen wird: Kursiv
	Abhängige Content Pack-Definition mit Versionsnummer: Blau
Filter "Nur CI- Typen mit zugewiesenem Inhalt anzeigen"	Filtert die CI-Typ-Struktur und zeigt nur CI-Typen mit zugewiesenem Inhalt an.

Elemente der Oberfläche	Beschreibung
Enthaltener Inhalt	Liste des Inhalts, der zum Hinzufügen zu einem Content Pack ausgewählt wurde, zusammen mit jeglichem abhängigen Inhalt.
	Tipp : Wenn Sie ein Element (oder eine Gruppe von Elementen) ausschließen möchten, wählen Sie dieses bzw. diese aus und klicken Sie auf die Schaltfläche Ausschließen .
	Farbcodierung:
	Kein Inhalt: Grau
	Ausgewählter Inhalt: Fett
	Inhalt, auf den verwiesen wird: Kursiv
	Abhängige Content Pack-Definition mit Versionsnummer: Blau
Inhalt in anderen Content Packs	Ist zum Hinzufügen ausgewählter Inhalt bereits in einem anderen Content Pack enthalten, wird er hier aufgeführt, um darauf hinzuweisen, dass er aus diesem Content Pack entfernt werden kann. Es ist nicht erforderlich und auch nicht empfehlenswert, denselben Inhalt in mehrere Content Packs einzuschließen.

Kontextmenüs

BSM stellt zahlreiche Kontextmenüs bereit. Diese Kontextmenüs ermöglichen den schnellen und direkten Zugriff auf Informationen zu ausgewählten Elementen und Aktionen, die Sie für diese ausführen können.

Klicken Sie mit der rechten Maustaste auf ein Element der Benutzeroberfläche, um das Kontextmenü anzuzeigen. Die verfügbaren Informationen und die möglichen Aktionen eines Kontextmenüs hängen von dem Element, auf das Sie mit der rechten Maustaste klicken, sowie seinem Kontext ab.

Das Kontextmenü auf der Registerkarte Inhalt enthält die folgenden Elemente:

Elemente der Oberfläche	Beschreibung
Zu enthaltenem Inhalt hinzufügen	Fügt die ausgewählten Elemente der Liste enthaltener Inhalte hinzu.
Andere ausblenden	Blendet alle offenen Verzweigungen mit Ausnahme der ausgewählten Verzweigung aus.
Alle ausgewählten Content Pack-Elemente anzeigen	Blendet die Liste Enthaltener Inhalt ein, um alle zum Einschließen in das Content Pack ausgewählten Elemente anzuzeigen.
Ausschließen	Entfernt die ausgewählten Elemente aus der Liste enthaltener Inhalte.
Alles ausschließen	Entfernt alle Elemente aus der Liste enthaltener Inhalte.

Elemente der Oberfläche	Beschreibung
Auswahl einblenden	Blendet die Liste Verfügbarer Inhalt oder Enthaltener Inhalt ein, um Elemente anzuzeigen, die zur ausgewählten Gruppe gehören.

Seite "Abhängigkeiten"

Auf dieser Seite des Assistenten können Sie die Abhängigkeiten bei abhängigen Inhalten festlegen, die in mehr als einem Content Pack eingeschlossen sind.

Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205.	
	Diese Seite des Assistenten wird als Registerkarte Abhängigkeiten im Dialogfeld zum Bearbeiten der Content Pack-Definition angezeigt, das geöffnet wird, wenn Sie auf klicken.	
Aufbau des Assistenten	Der "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205 besteht aus folgenden Elementen:	
	"Seite "Allgemein" " auf Seite 206 > "Seite "Inhalt"" auf Seite 207 > Seite "Abhängigkeiten" > "Seite "Zusammenfassung"" auf der nächsten Seite	
Siehe auch	" Content Packs" auf Seite 182	
	"Abhängigkeiten in Content Packs" auf Seite 188	

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
⊘	Aktualisieren. Aktualisiert den Inhalt der angezeigten Liste der Abhängigkeiten. Verwenden Sie dieses Element, wenn während der Arbeit neue Inhalte verfügbar werden oder wenn Sie neue Inhalte heraufgeladen haben (z. B. über die Befehlszeilenschnittstelle).
**	Abhängigkeit festlegen. Ist Inhalt, auf den verwiesen wird, auch in anderen Content Pack-Definitionen enthalten, wird in einer Meldung darauf hingewiesen und eine wurde automatisch für Sie festgelegt.
	Um eine andere Content Pack-Definition für diesen Inhalt anzugeben, verwenden Sie die Aktion Abhängigkeit festlegen . Um den Inhalt, auf den verwiesen wird, in Ihre Content Pack-Definition einzuschließen, verwenden Sie die Aktion Zu enthaltenem Inhalt hinzufügen .
	Der abhängige Inhalt in dem Content Pack, auf das verwiesen wird, wird fett formatiert dargestellt. Auf diese Weise wird deutlich gemacht, dass eine Abhängigkeit festgelegt wurde.

Elemente der Oberfläche	Beschreibung
(*)	Zu enthaltenem Inhalt hinzufügen. Fügt den ausgewählten abhängigen Inhalt zur Liste mit dem Inhalt hinzu, der in diesem Content Pack eingeschlossen ist.
<farbcodierung></farbcodierung>	Farbcodierung:
	Inhalt, auf den intern verwiesen wird: Normal
	In der aktuell ausgewählten Content Pack-Definition enthaltener Inhalt: Fett
	In anderer Content Pack-Definition enthaltener Inhalt: Grau
<dropdownfeld "version"=""></dropdownfeld>	Wenn für den Inhalt, auf den verwiesen wird, mehrere Versionen eines Content Packs verfügbar sind, wird das Dropdownfeld Version aktiviert, und die ausgewählte Content Pack-Version wird angezeigt. Sie können eine andere Version auswählen und die Abhängigkeit zu dieser festlegen.

Seite "Zusammenfassung"

Diese Seite des Assistenten ermöglicht Ihnen das Anzeigen von Übersichtsinformationen zum Inhalt, zu Abhängigkeiten und zu Problemen, die in einer neuen Content Pack-Definition festgestellt wurden.

Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205.
	Diese Seite des Assistenten wird als Registerkarte Zusammenfassung im Dialogfeld zum Bearbeiten der Content Pack-Definition angezeigt, die geöffnet wird, wenn Sie auf klicken.
Aufbau des Assistenten	Der "Assistent zum Erstellen einer neuen Content Pack-Definition " auf Seite 205 besteht aus folgenden Elementen:
	"Seite "Allgemein" " auf Seite 206 > "Seite "Inhalt"" auf Seite 207 > "Seite "Abhängigkeiten"" auf der vorherigen Seite > Seite "Zusammenfassung"
Siehe auch	" Content Packs" auf Seite 182

Die Elemente der Benutzeroberfläche werden in der folgenden Tabelle beschrieben.

Die Übersichtsseite zeigt eine Übersicht über den Inhalt der ausgewählten Content Pack-Definition an. Diese Übersicht ist in die folgenden Unterbereiche aufgeteilt. Jeder Unterbereich enthält eine Inhaltsliste und für jedes Element in der Liste werden folgende Informationen angezeigt:

- Gesamtanzahl der Artefakte
- Anzahl der vordefinierten Artefakte
- Anzahl der vordefinierten (benutzerdefinierten) Artefakte
- Anzahl der benutzerdefinierten Artefakte

Wenn Sie die Inhaltsgruppe einblenden, werden die in dieser Gruppe enthaltenen Artefakte, der CI-Typ des Artefakts (sofern zutreffend) und der Ursprung des Artefakts (Vordefiniert, Vordefiniert (Benutzerdefiniert), Benutzerdefiniert) angezeigt.

Zum Beispiel wird für Indikatoren und Zuordnungsregeln auch der CI-Typ angezeigt, das heißt der Typ des Konfigurationselements, dem der Indikator zugewiesen ist (z. B.: **Applikation**, **Host** oder **Oracle-System**).

Elemente der Oberfläche	Beschreibung
Ausgewählter Inhalt	Zeigt gruppiert nach Inhaltstyp eine Liste des ausgewählten Inhalts an, der in der ausgewählten Content Pack-Definition enthalten ist.
In diesem Content Pack enthaltener Inhalt, auf den verwiesen wird	Zeigt gruppiert nach Inhaltstyp eine Liste des referenzierten Inhalts an, der in der ausgewählten Content Pack-Definition enthalten ist.
Inhalt aus anderen Content Packs, auf den verwiesen wird	Zeigt eine Liste des abhängigen Inhalts an, auf den von anderen Content Packs verwiesen wird, einschließlich Anzeigename und Version jedes referenzierten Content Packs.
Probleme gefunden	Zeigt Informationen zu vorliegenden Problemen an, wie nicht aufgelöste Abhängigkeiten (Inhalte, die in der ausgewählten Content Pack-Definition enthalten sind, aber in BSM nicht mehr vorhanden sind), die in der ausgewählten Content Pack-Definition festgestellt wurden.

Dialogfeld "Content Pack importieren"

Im Dialogfeld **Content Pack importieren** können Sie das Content Pack angeben, das Sie importieren möchten, und die Importoptionen festlegen.

Hinweis: Ein Content Pack enthält die zu importierenden Elemente. In einer Content Pack-Definition werden die im Content Pack enthaltenen Elemente aufgelistet.

Zugriff	Führen Sie einen der folgenden Schritte aus:
	Admin > Plattform > Content Packs
	Admin > Operationenverwaltung > Setup > Content Packs
	und klicken Sie dann auf 🖳
Relevante Aufgaben	"Erstellen und Verwalten von Content Packs" auf Seite 193

Das Dialogfeld **Content Pack importieren** enthält die in der folgenden Tabelle aufgeführten Elemente der Benutzeroberfläche.

Elemente der Oberfläche	Beschreibung
Content Pack-Datei	Hier können Sie zum Speicherort navigieren, an dem sich die zu importierende Content Pack-Datei befindet.
Testen	Hiermit wird ein simulierter Importvogang mit der ausgewählten Content Pack- Definition ausgeführt, aber es werden keine Änderungen an BSM übergeben.
Importieren	Startet den angegebenen Inhaltsdatenimport und schließt das Dialogfeld Content Pack importieren .

Befehlszeilenschnittstelle für den Content Pack Manager

In diesem Abschnitt werden die Optionen und Parameter der **ContentManager**-Befehlszeilenschnittstelle beschrieben.

Die **ContentManager**-Befehlszeilenschnittstelle befindet sich auf den Gateway-Servern und den Datenverarbeitungsservern unter:

<BSM-Stammverzeichnis>/bin

Hinweis: Der Benutzer, der die **ContentManager**-Befehlszeilenschnittstelle ausführt, muss über Lesezugriff auf folgende Datei verfügen:

<BSM-Stammverzeichnis>/conf/TopazInfra.ini

Syntax

ContentManager <Operation> [Connection] <Benutzeranmeldeinformationen>
[Option]

Operation (eine der folgenden):

Import-Operationen:

-import <Eingabedatei> [-test]

Export-Operationen:

-snapshot -output <Ausgabedatei>

-export <Name> -output <Ausgabedatei>

[-contentPackVersion < Version >] [-asPredefined]

Verschiedene Operationen:

-list

-delete <Name> [-contentPackVersion <Version>]

-version

Verbindungen (eine der folgenden):

-url <URL>

-server <Gateway-Server> [-port <Port>] [-ssl]

Benutzeranmeldeinformationen:

-username <Anmeldename> [-password <Kennwort>]

[-customer < Kunden-ID>]

Optionen:

-verbose

In der folgenden Tabelle finden Sie weitere Informationen über die Argumente, die vom **ContentManager**-Befehl erkannt werden:

Option	Beschreibung
-asPredefined	Kennzeichnet das exportierte Content Pack als vordefiniert.
-cpv,-contentPackVersion <version></version>	Die Versionsnummer der Content Pack-Definition
-cu-customer <kunden-< th=""><th>ID des Kunden in SaaS-Umgebung.</th></kunden-<>	ID des Kunden in SaaS-Umgebung.
ID>	Wird dieser Parameter nicht festgelegt, ist der Standardwert 1.
-d,-delete <content_pack- Name></content_pack- 	Löscht die Content Pack-Definition <content_pack-name>. Der Inhalt des Content Packs wird dadurch nicht gelöscht. Zu dem Inhalt eines Content Packs zählen Definitionen für Ereignistyp-Indikatoren, Zustandsindikatoren, Berechnungsregeln für KPIs, Regeln für die topologiebasierte Ereigniskorrelation, Werkzeugdefinitionen, Ansichtszuordnungen und Diagrammfamilien.</content_pack-name>
-e,-export <content_pack- Name></content_pack- 	Exportiert die benannte Content Pack-Definition und ihre Inhalte in die Datei, die mit der Option -output angegeben wurde.
-h,-help	Zeigt eine Übersicht der Befehlsoptionen und Exit-Mechanismen an.
-i,-import <eingabedatei></eingabedatei>	Importiert die Content Pack-Definition und ihre Inhalte aus der angegebenen Datei.
	Durch das Importieren eines benutzerdefinierten Content Packs werden die vorhandenen Objekte überschrieben. Durch das Importieren eines vordefinierten Content Packs werden alle nicht angepassten Objekte überschrieben.
-l,-list	Listet die Content Pack-Definitionen auf.
-o,-output <ausgabedatei></ausgabedatei>	Gibt den Namen der Datei an, in die bei der Export-Operation geschrieben werden soll.

Option	Beschreibung
-p,-port <port></port>	Legt die Portnummer fest. Die Standardportnummern sind '80' für HTTP und '443' für HTTPS. Diese Option kann nicht zusammen mit der Option -url angegeben werden.
-password <kennwort></kennwort>	Fordert das Kennwort des Benutzers an, der mit der Option - username angegeben wurde und dessen Konto zu Authentifizierungszwecken verwendet wird.
-server <gateway-server></gateway-server>	Legt den BSM-Ziel-Gateway-Server per Hostname oder IP-Adresse fest. Der angegebene Server muss ein BSM-Gateway-Server sein. Der Standardwert ist "{0}".
	Hinweis: Diese Option kann nicht zusammen mit der Option -url angegeben werden.
-skipCheck	Überspringt die Konsistenzprüfung des Content Packs. Bei der Konsistenzprüfung des Content Packs wird geprüft, ob sich abhängiger Inhalt, der nicht Teil eines anderen Content Packs ist, entweder im Content Pack selbst befindet oder bereits importiert wurde.
	Vorsicht: Diese Option darf nur beim Upgrade auf eine neuere Version des Content Packs verwendet werden.
-snapshot	Exportiert eine Baseline des gesamten Inhalts, die vom Content Packs Manager verwaltet werden kann.
-ssl	Legt das Protokoll auf HTTPS fest. Das Standardprotokoll ist HTTP. Diese Option kann nicht zusammen mit der Option -url angegeben werden. Wenn kein Port mit der Option -port angegeben wurde, wird im Befehl die Standardportnummer für HTTPS verwendet: 443.
-t,-test	Führt den Import im Vorschaumodus aus und zeigt sofort Ergebnisse an. Es werden keine Änderungen in der Datenbank gespeichert.
-u, -url <url></url>	Gibt die URL des BSM-Gateway-Servers an. Der Standardwert ist
	http:// <gateway-server-dns-name>:<port>/opr-admin-server</port></gateway-server-dns-name>
	Diese Option kann nicht zusammen mit der Option -server angegeben werden.
-username <anmeldename></anmeldename>	Der Name des Benutzers, dessen Konto für Authentifizierungszwecke verwendet wird.
-v, -verbose	Gibt ausführliche Informationen aus.
-version	Gibt die Versionsinformationen des Befehls aus und beendet den Vorgang.

Mit dem Befehl **ContentManager** werden die folgenden Werte angezeigt, um den Exit-Status der angeforderten Operation anzugeben:

Exit-Status	Beschreibung
0	Erfolgreich abgeschlossen
1	Angeforderte Operation nicht erfolgreich
300-399	HTTP-Umleitung (300-399)
400-499	HTTP-Clientfehler (400-499)
500-599	Interner HTTP-Serverfehler (500-599)

Die Nummern des Exit-Status (300-599) geben eine standardmäßige HTTP-Statuskategorie (und Nummer) wieder. Beispiel: Umleitung (300-399). Weitere Informationen zu einem bestimmten HTTP-Fehlerstatus, beispielsweise 307, was eine temporäre HTTP-Umleitung bedeutet, finden Sie in der öffentlich verfügbaren HTTP-Dokumentation.

Befehlszeilenschnittstelle für das automatische Hochladen von Content Packs

In diesem Abschnitt werden die Optionen und Parameter der **ContentAutoUpload**-Befehlszeilenschnittstelle beschrieben.

Die **ContentAutoUpload**-Befehlszeilenschnittstelle befindet sich auf dem Datenverarbeitungsserver unter:

<BSM-Stammverzeichnis>/bin

Hinweis: Der Benutzer, der die **ContentAutoUpload**-Befehlszeilenschnittstelle ausführt, muss über Lesezugriff auf folgende Datei verfügen:

<BSM-Stammverzeichnis>/conf/TopazInfra.ini

Verwendung

ContentAutoUpload <Operation> [Option]

Operation (eine der folgenden):

Operationen importieren:

-autoUpload [-uploadFolder <Verzeichnis>]

[-forceReload]

Verschiedene Operationen:

-version

Optionen:

-verbose

In der folgenden Tabelle finden Sie weitere Informationen über die Argumente, die vom **ContentAutoUpload**-Befehl erkannt werden:

Option	Beschreibung
-a,- autoUpload	Lädt die Content Pack-Definitionsdateien automatisch aus dem Content Pack- Standardverzeichnis auf dem Datenverarbeitungsserver hoch.
	<bsm-stammverzeichnis>/conf/opr/content/<locale>/</locale></bsm-stammverzeichnis>
	Windows: C:\HPBSM\conf\opr\content\ <locale>\</locale>
	Linux: /opt/HP/BSM/conf/opr/content/ <locale>/</locale>
	Wenn Sie Content Pack-Definitionen aus einem alternativen Verzeichnis auf dem Datenverarbeitungsserver hochladen wollen, geben Sie den Verzeichnispfad mithilfe der Option -uploadFolder < Verzeichnis> an.
	Hinweis: Wenn Sie über mehrere Datenverarbeitungsserver verfügen, müssen Sie die Content Pack-Ordner synchronisiert halten, weil es nicht möglich ist, festzulegen, von welchem Datenverarbeitungsserver Content Packs importiert werden.
	Alle vordefinierten Content Pack-Definitionsdateien im angegebenen Verzeichnis werden in der Reihenfolge ihrer Abhängigkeiten importiert. Wurde eine Content Pack-Definition bereits ins Repository hochgeladen, wird sie nicht erneut hochgeladen.
	Informationen zu Importfehlern finden Sie in der folgenden Protokolldatei:
	<bsm-stammverzeichnis>/log/EJBContainer/opr-webapp.log</bsm-stammverzeichnis>
	Windows: C:\HPBSM\log\EJBContainer\opr-webapp.log
	Linux: /opt/HP/BSM/log/EJBContainer/opr-webapp.log
-forceReload	Erzwingt das erneute Laden aller Content Packs im Standardverzeichnis (<bsm-stammverzeichnis>/conf/opr/content/<locale>/) oder im angegebenen Verzeichnis mithilfe der Option -uploadFolder <verzeichnis>. Nicht angepasster Inhalt wird überschrieben.</verzeichnis></locale></bsm-stammverzeichnis>
-h,-help	Zeigt eine Übersicht der Befehlsoptionen und Exit-Mechanismen an.
-skipCheck	Überspringt die Konsistenzprüfung des Content Packs. Bei der Konsistenzprüfung des Content Packs wird geprüft, ob sich abhängiger Inhalt, der nicht Teil eines anderen Content Packs ist, entweder im Content Pack selbst befindet oder bereits importiert wurde.
	Vorsicht: Diese Option darf nur beim Upgrade auf eine neuere Version des Content Packs verwendet werden.

Option	Beschreibung
-uploadFolder <verzeichnis></verzeichnis>	Wenn Sie Content Packs aus einem alternativen Verzeichnis hochladen wollen, geben Sie den Verzeichnispfad mithilfe der Option -uploadFolder <verzeichnis></verzeichnis> an.
	Beispiel:
	ContentAutoUpload -a -uploadFolder c:\temp
-v, -verbose	Gibt ausführliche Informationen aus.
-version	Gibt die Versionsinformationen des Befehls aus und beendet den Vorgang.

Mit dem Befehl **ContentAutoUpload** werden die folgenden Werte angezeigt, um den Exit-Status der angeforderten Operation anzugeben:

Exit- Status	Beschreibung
0	SUCCESS (Mindestens ein Content Pack wurde importiert. Es sind keine Fehler aufgetreten.)
1	FAILURE (Es wurden keine Content Packs importiert. Kompletter Fehler.)
2	FAILURE_PARTIAL (Einige Content Packs wurden importiert. Bei einigen Content Packs sind Fehler aufgetreten.)
3	NO_OPERATION (Es wurde kein neuer Inhalt für den Upload gefunden.)
4	NO_PERMISSION (Der Benutzer hat keine Berechtigung zum Ausführen dieses Werkzeugs.)
5	SYNTAX_ERROR (Es wurden falsche Befehlszeilenargumente angegeben.)

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Hinweise zur Fehlerbehebung beim Content Management, unter anderem für das Erstellen, Ändern und Aktivieren von Konfigurationselementen.

Inhalt ist nicht im Content Pack enthalten

Stellen Sie sicher, dass Sie die Aktion zum Einschließen auf der richtigen Ebene in der CI-Typ-Hierarchie durchführen, damit *alle* dem ausgewählten CI-Typ (sowie allen untergeordneten CIs) zugewiesenen Elemente gleichzeitig hinzugefügt werden.

Nicht aufgelöste Verweise auf CIs beim Importieren

Das Content Pack enthält Verweise auf Konfigurationselemente, die im Zielsystem nicht vorhanden sind. Stellen Sie sicher, dass die Optionen zum Überschreiben und Erstellen richtig angegeben sind, bevor Sie mit dem Importvorgang beginnen.

Kapitel 17

Ausfallzeitenverwaltung

Ausfallzeiten oder andere geplante Ereignisse können CI-Daten verzerren. Möglicherweise möchten Sie diese Zeiträume von der Berechnung für Ereignisse, Warnungen, Reports, Ansichten oder SLAs ausschließen. Ausfallzeiten werden basierend auf verknüpften CIs konfiguriert. Sie könnten beispielsweise ein wiederkehrendes Wartungsereignis oder Urlaub für ein bestimmtes Host-CI ausschließen, dessen physischer Host in diesem Zeitraum nicht in Betrieb sein wird.

Sie definieren und verwalten Ausfallzeiten mithilfe der Seite "Ausfallzeitenverwaltung" in der Plattformverwaltung. Mit BSM haben Sie folgende Möglichkeiten:

- Konfigurieren der Ausfallzeit für die einmalige oder wiederkehrend für die wöchentliche oder monatliche Ausführung.
- Auswählen von mehreren CIs, für die die Ausfallzeit gelten soll.

Beim Konfigurieren einer Ausfallzeit wählen Sie bestimmte Instanzen der CIs aus den verfügbaren Ansichten aus. Sie können CIs der folgenden CI-Typen für die Ausfallzeit auswählen:

- Knoten
- Ausgeführte Software
- Geschäftsprozess
- Unternehmensapplikation
- CI-Sammlung
- Infrastrukturservice
- Geschäftsservice

Aktionen für die Ausfallzeit

Sie können auswählen, welche Aktion während der Ausfallzeit für die in der Ausfallzeitenkonfiguration ausgewählten CIs durchgeführt wird. Die Ausfallzeit kann sich auf Folgendes auswirken:

- Warnungen und Ereignisse. Ereignisse werden unterdrückt und es werden weder CI-Statuswarnungen, EUM-Warnungen oder Benachrichtigungen für die mit der Ausfallzeit verknüpften CIs gesendet.
- KPIs. Dem CI zugeordnete KPIs und betroffene CIs werden nicht aktualisiert und zeigen die Ausfallzeit für das CI in Service Health an. Weitere Informationen zur Auswirkung von Ausfallzeitkonfigurationen in Service Health finden Sie unter "KPI Status Colors and Definitions" im BSM-Benutzerhandbuch.
- **Reports**. End User Management-Reports werden nicht aktualisiert und zeigen die Ausfallzeit für das CI an. Weitere Informationen zur Auswirkung von Ausfallzeitkonfigurationen auf Reports finden Sie unter "Downtime Information in Reports" im BSM-Benutzerhandbuch.
- SLAs. Ausgewählte SLAs, die mit dem CI verbunden sind, werden nicht aktualisiert. Sie

können auswählen, welche SLAs in die Ausfallzeit aufgenommen werden. Weitere Informationen zur Auswirkung von Ausfallzeitkonfigurationen auf SLAs finden Sie unter "Retroactive SLA Data Corrections" im BSM Application Administration Guide.

• Überwachen. Business Process Monitor und SiteScope stoppen die Überwachung aller mit der Ausfallzeit verbundenen CIs. Weitere Informationen zur Auswirkung von Ausfallzeitkonfigurationen auf die SiteScope-Überwachung finden Sie unter "CI Downtime" im BSM-Benutzerhandbuch.

Die Optionen, die Sie im Assistenten für die Ausfallzeit auswählen, stellen Kombinationen der oben genannten Aktionen in dieser Reihenfolge dar. Dabei umfasst jede Option die zuvor aufgelisteten Optionen. Die in BSM während der Ausfallzeit durchgeführten Aktionen hängen von der in der Ausfallzeitenkonfiguration ausgewählten Option ab.

Ereignisse in Operationenverwaltung

Wenn Sie eine Option für eine Aktion auswählen, zu der das Unterdrücken von Ereignissen für ein ausgewähltes CI in einer Ausfallzeit gehört, hängt das Ergebnis in der Operationenverwaltungs-Applikation davon ab, wie das Ausfallzeitverhalten in Operationenverwaltung konfiguriert wurde. Weitere Informationen finden Sie unter "Downtime Behavior" im BSM Application Administration Guide.

REST-Service für Ausfallzeit

Sie haben die Möglichkeit, Ausfallzeiten mithilfe eines RESTful Web Service, der auf dem Gateway-Server ausgeführt wird, abzurufen, zu erstellen und zu löschen. Weitere Informationen finden Sie unter "REST-Service für Ausfallzeit" auf Seite 225.

Erstellen und Verwalten von Ausfallzeiten für Cls

In dieser Aufgabe wird beschrieben, wie Sie Ausfallzeiten für die CIs in Ihrem System erstellen und verwalten.

1. Voraussetzungen

Planen Sie, wie sich die Ausfallzeit auf die CIs in Ihrem System auswirken soll. Bevor Sie im Assistenten arbeiten:

- Wenn Sie festlegen, für welche CIs Ausfallzeiten notwendig sind, sollten Sie die CIs berücksichtigen, die sich auf die ausgewählten CIs auswirken. In bestimmten Fällen sind diese CIs auch von der Ausfallzeit betroffen. Weitere Hintergrundinformationen zu den Auswirkungen der Ausfallzeiten finden Sie in der BSMDowntime_topology-TQL im RTSM Modeling Studio. Sie können nur CIs der folgenden CI-Typen auswählen:
 - Knoten
 - running_software
- business_process
- o business_application
- ci collection
- infrastructure_service
- o business service
- Legen Sie fest, welche Aktionen auf welche CIs angewendet werden sollen. Folgende Optionen stehen während der Ausfallzeit zur Verfügung:
 - Keine Aktion
 - Warnungen unterdrücken und Ereignisse schließen
 - Ausfallzeit für KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen
 - Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen
 - Überwachung beenden (BPM und SiteScope); Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen (wirkt sich auf alle zugehörigen SLAs aus)

2. Konfigurieren, wie Ereignisse in Operationenverwaltung behandelt werden - optional

Sie können festlegen, wie Ereignisse behandelt werden, die mit von einer Ausfallzeit betroffenen CIs verknüpft sind. Diese Festlegungen können Sie unter **Admin > Operationenverwaltung > Operationenverwaltung abstimmen > Ausfallzeitverhalten** vornehmen.

Weitere Informationen zu diesem Thema finden Sie unter "Downtime Behavior" im BSM-Benutzerhandbuch.

3. Ausführen des Assistenten zum Erstellen einer Ausfallzeit

Wechseln Sie zu **Admin > Plattform > Ausfallverwaltung** und klicken Sie auf die Schaltfläche **Neue Ausfallzeit erstellen**.

Informationen zur Benutzeroberfläche finden Sie unter "Assistent für neue Ausfallzeit" auf Seite 231.

4. Ergebnisse

Nach dem Ausführen des Assistenten werden die Details der Ausfallzeit auf der Seite **Ausfallzeitenverwaltung** angezeigt. Sie haben die Möglichkeit, die Details der Ausfallzeiten in eine .pdf-Datei oder Excel-Datei zu exportieren.

Informationen zur Benutzeroberfläche finden Sie unter "Seite "Ausfallzeitenverwaltung"" auf Seite 229.

Tipp: Um die Ausfallzeiten in der exportierten Datei auf eine bestimmte Auswahl zu begrenzen, können Sie die sichtbaren Ausfallzeiten in der Ausfallzeitenverwaltung filtern und erst dann den Export in eine .pdf-Datei oder Excel-Datei durchführen. Sie können nach einer beliebigen Kombination der folgenden Spalten filtern: Name, CIs, Status, Aktion, Planung, Nächstes Vorkommen, Geändert von, Genehmigt von, Geplant und Kategorie.

REST-Service für Ausfallzeit

Sie haben die Möglichkeit, Ausfallzeiten mithilfe eines RESTful Web Service, der auf dem Gateway-Server ausgeführt wird, abzurufen, zu aktualisieren, zu erstellen und zu löschen. Sie können HTTP-Anforderungen in Ihren Browser eingeben und Kombinationen aus HTTP-Anforderungen und XML-Befehlen in einen REST-Client. Die Dienstauthentifizierung erfolgt gemäß der Basisauthentifizierung.

Unterstützte HTTP-Anforderungen

Der REST-Service für Ausfallzeit unterstützt die folgenden HTTP-Anforderungen:

Hinweis: "CustomerID" ist außer bei HP SaaS-Kunden stets 1.

Aktion	HTTP-Befehl
Alle Ausfallzeiten abrufen	http:// <hpbsm-server>/topaz/bsmservices/customers/ [customerId]/downtimes</hpbsm-server>
Bestimmte Ausfallzeit abrufen	http:// <hpbsm-server>/topaz/bsmservices/customers/ [customerId]/downtimes/[downtimeId]</hpbsm-server>
Ausfallzeit mithilfe von HTTP PUT aktualisieren	http:// <hpbsm-server>/topaz/bsmservices/customers/ [customerId]/downtimes/[downtimeId] + XML der Ausfallzeit</hpbsm-server>
Ausfallzeit mithilfe von HTTP POST erstellen	http:// <hpbsm-server>/topaz/bsmservices/customers/ [customerId]/downtimes + XML der Ausfallzeit Hinweis: Das erfolgreiche Erstellen der Ausfallzeit führt zur Rückgabe der neu erstellten Ausfallzeit im XML-Format, einschließlich der Ausfallzeit-ID.</hpbsm-server>
Ausfallzeit mithilfe von HTTP DELETE löschen	http:// <hpbsm-server>/topaz/bsmservices/customers/ [customerId]/downtimes/[downtimeId]</hpbsm-server>

Zulässige Aktionen für die Ausfallzeit

Verwenden Sie die aufgeführten XM-Befehle für die folgenden Aktionen für die Ausfallzeit:

Aktionsbeschreibung	XML-Befehl
Keine Aktion	<action name="REMINDER"></action>
Warnungen unterdrücken und Ereignisse schließen	<action name="SUPPRESS_NOTIFICATIONS"></action>

Aktionsbeschreibung	XML-Befehl
Ausfallzeit für KPI- Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen (Überwachung fortsetzen)	<action name="ENFORCE_ON_KPI_CALCULATION"></action>
Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen (Überwachung fortsetzen)	<action name="ENFORCE_ON_REPORTS"></action>
Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen (Überwachung fortsetzen), einschließlich aller SLAs	<pre><action name="ENFORCE_ON_REPORTS"> <pre></pre></action></pre>
Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen (Überwachung fortsetzen), einschließlich bestimmter SLAs	<pre><action name="ENFORCE_ON_REPORTS"> <pre></pre></action></pre>
Aktive Überwachung beenden (BPM und SiteScope); Ausfallzeit für Reports und KPI-Berechnungen erzwingen, Warnungen unterdrücken und Ereignisse schließen	<action name="STOP_MONITORING"></action>

XML-Beispiel für Ausfallzeit

Die folgenden Felder dürfen die angegebene maximale Länge nicht überschreiten:

• Name: 200 Zeichen

• Beschreibung: 2.000 Zeichen

• Genehmigende Person: 50 Zeichen

```
<recipients>
            <recipient id="24"/>
            <recipient id="22"/>
            <recipient id="21"/>
        </recipients>
    </notification>
    <selectedCIs>
        <ci>
            <id>ac700345b47064ed4fbb476f21f95a76</id>
            <viewName>End User Monitors</viewName>
        </ci>
    </selectedCIs>
    <schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"</pre>
xsi:type="WeeklyScheduleType">
        <type>WÖCHENTLICH</type>
        <startDate>2010-06-10T15:40:00+03:00</startDate>
        <timeZone>Europa/Zürich</timeZone>
        <Tage>
            <selectedDays>MITTWOCH</selectedDays>
            <selectedDays>DONNERSTAG</selectedDays>
            <selectedDays>FREITAG</selectedDays>
            <selectedDays>SAMSTAG</selectedDays>
        </days>
        <startTimeInSecs>52800</startTimeInSecs>
        <durationInSecs>300</durationInSecs>
    </schedule>
</downtime>
```

Planung

Beachten Sie beim Festlegen des Zeitplans für Ausfallzeiten Folgendes:

- Rückwirkende Ausfallzeiten werden nicht unterstützt Folgendes ist nicht möglich:
- Erstellen einer in der Vergangenheit geplanten Ausfallzeit.
- Löschen einer Ausfallzeit, die noch nicht begonnen hat oder in der Vergangenheit aufgetreten ist
- Ändern einer Ausfallzeit, die noch nicht begonnen hat oder in der Vergangenheit aufgetreten ist.
- Das Datumsformat für "startDate/endDate" lautet: JJJJ-MM-TT'T'hh:mm:ssZ
- Bei wöchentlichen und monatlichen Ausfallzeiten sollten "startDate" und "endDate" auf Mitternacht festgelegt werden. Beispiel:
- <startDate>2010-07-24T00:00:00+03:00</startDate>
- <endDate>2010-09-04T00:00:00+03:00</endDate>

Beispiel eines Zeitplans für Ausfallzeit mit einem Vorkommen

Beispiel eines wöchentlichen Zeitplans für Ausfallzeit

Beispiel eines monatlichen Zeitplans für Ausfallzeit

Ausfallzeitverwaltung - Benutzeroberfläche

Seite "Ausfallzeitenverwaltung"

Zeigt die Liste der geplanten Ausfallzeiten für die verknüpften CIs an.

Zugriff:	Wählen Sie Admin > Plattform > Ausfallverwaltung.
Wichtiger Hinweis	 Zum Hinzufügen, Bearbeiten oder Löschen von Ausfallzeiten müssen Sie über vollständige Berechtigungen für die Ressource Ausfall verfügen. Außerdem sollten Sie über die Berechtigung Anzeigen für die Ansichten verfügen, zu denen die ausgefallenen CIs gehören. Details zu Berechtigungen finden Sie unter "Berechtigungen" auf Seite 248.
	 Die Werte auf dieser Seite sind schreibgeschützt. Um einen der Werte für eine Ausfallzeit zu bearbeiten, markieren Sie den Wert, und klicken Sie auf Bearbeiten. Der Assistent für die Ausfallzeit wird geöffnet, und Sie können den Wert auf der Seite bearbeiten, auf der er angezeigt wird.
	• Für Ausfallzeiten, die schon aufgetreten sind, sind nur folgende Felder editierbar:
	Seite Eigenschaften: alle Felder
	Seite Planung: Datum unter Ende um im Serienbereich
	Seite Benachrichtigung: Ausgewählte Empfänger
	 Jede Spalte umfasst die Optionen zum Filtern der Liste nach den Inhalten der Spalte. Sie können z. B. einen Kategorietyp in der Kategoriespalte auswählen und sehen dann nur die Ausfallzeiten, die in dieser Kategorie konfiguriert wurden. Bereits verstrichene Ausfallzeiten werden standardmäßig herausgefiltert. Klicken Sie zum Ändern dieser Einstellung auf die Filter-Schaltfläche Status, und wählen Sie Abgeschlossen.
Relevante Aufgaben	"Erstellen und Verwalten von Ausfallzeiten für CIs" auf Seite 223
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Element der Oberfläche	Beschreibung
*	Neue Ausfallzeit erstellen. Hiermit wird der Assistent Neue Ausfallzeit geöffnet, mit dem Sie eine neue Ausfallzeit konfigurieren können. Weitere Informationen finden Sie unter "Assistent für neue Ausfallzeit" auf Seite 231.

Element der Oberfläche	Beschreibung
0	Ausfallzeit bearbeiten. Hiermit wird der Assistent Ausfallzeit bearbeiten geöffnet, mit dem Sie die Konfiguration einer bestehenden Ausfallzeit bearbeiten können. Dieser Assistent umfasst die gleichen Bildschirme wie der Assistent Neue Ausfallzeit. Details finden Sie unter "Assistent für neue Ausfallzeit" auf der nächsten Seite.
	Ausfallzeit duplizieren. Hiermit werden die Einstellungen einer bestehenden Ausfallzeit für eine neue Ausfallzeit dupliziert.
×	Ausfallzeit(en) löschen. Hiermit werden ausgewählte Ausfallzeiten gelöscht. Ausfallzeiten, die jetzt aktiv sind oder in der Vergangenheit aktiv waren, können nicht gelöscht werden. Auf diese Weise soll der Verlust historischer Daten verhindert werden.
	Nach Excel exportieren. Hiermit wird die Tabelle konfigurierter Ausfallzeiten in eine Datei im Excel-Format exportiert.
1	In PDF exportieren. Hiermit wird die Tabelle konfigurierter Ausfallzeiten in eine PDF-Datei exportiert.
Aktion	Die Aktion, die während der Ausfallzeit ausgeführt werden soll. Die Aktion für die Ausfallzeit kann im Assistenten Neue Ausfallzeit konfiguriert werden. Weitere Informationen über die möglichen Aktionen finden Sie unter "Seite "Aktion" auf Seite 235.
CIs	Die mit der Ausfallzeit verknüpften CIs. Dies sind die CIs, auf die sich die Ausfallzeit auswirkt.
Geändert von	Der Benutzer, der die Ausfallzeit-Konfiguration zuletzt erstellt oder geändert hat.
Name	Der im Assistenten für die Ausfallzeit konfigurierte Name der Ausfallzeit.
Nächstes Vorkommen	Datum und Uhrzeit des nächsten Vorkommens der Ausfallzeit. Dieses Feld wirdautomatisch aktualisiert.
Planung	Zeigt Folgendes an:
	Datum, Uhrzeit, Zeitzone und Dauer
	Zeigt für sich wiederholende Ausfallzeiten außerdem an:
	Wochentag oder Monat für die wiederholte Ausführung
	Serienbereich

Element der Oberfläche	Beschreibung
Status	Zeigt den Status der Ausfallzeit an:
	Aktiv. Die Ausfallzeit für die CIs ist aktiv, und die ausgewählte Aktion wird ausgeführt.
	Inaktiv. Die Ausfallzeit ist konfiguriert, ist aber zurzeit nicht aktiv.
	Abgeschlossen. Die Ausfallzeit ist bereits verstrichen, und die konfigurierten Aktionen wurden ausgeführt.
Optionale Sp	alten
Genehmigt von	Hiermit wird angegeben, ob und von wem die Ausfallzeit genehmigt wurde.
Kategorie	Die der Ausfallzeit zugewiesene Kategorie. Folgende Optionen sind verfügbar:
	Applikationsinstallation
	Applikationswartung
	Hardwareinstallation
	Hardwarewartung
	Netzwerkwartung
	Neukonfiguration des Betriebssystems
	Sonstiges
	Sicherheitsproblem
	Sie können auch eigene angepasste Kategorien mithilfe der Infrastruktureinstellungen erstellen.
	Zum Hinzufügen einer benutzerdefinierten Ausfallzeitkategorie klicken Sie auf Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen.
	Wählen Sie Foundation aus.
	Wählen Sie Ausfall aus.
	 Ändern Sie in der Tabelle Ausfall - Allgemeine Einstellungen die Ausfallkategorien in den Namen, den Sie als angepasste Kategorie für die Ausfallzeit verwenden möchten. Der eingegebene Name wird als Option in der Liste der verfügbaren Ausfallzeitenkategorien angezeigt.
Geplant	Hiermit wird angegeben, ob die Ausfallzeit geplant ist oder nicht.

Assistent für neue Ausfallzeit

Dieser Assistent ermöglicht Ihnen das Erstellen und Bearbeiten von Ausfallzeiten für die CIs in Ihrem Modell.

Zugriff	Admin > Plattform > Ausfallzeit, klicken Sie auf die Schaltfläche Neue Ausfallzeit erstellen oder wählen Sie eine bestehende Ausfallzeit aus und klicken Sie dann auf die Schaltfläche Ausfallzeit bearbeiten.
Relevante Aufgaben	"Erstellen und Verwalten von Ausfallzeiten für CIs" auf Seite 223
Aufbau des Assistenten	Dieser Assistent für neue Ausfallzeit enthält Folgendes: "Seite "Eigenschaften" " unten > "Seite "CIs auswählen" " auf der nächsten Seite > "Seite "Planung" " auf Seite 234 > "Seite "Aktion"" auf Seite 235 > "Seite "Benachrichtigung" " auf Seite 238 > "Seite "Vorschau" " auf Seite 238
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Seite "Eigenschaften"

Auf dieser Seite des Assistenten können Sie die allgemeinen Eigenschaften für die Ausfallzeit konfigurieren.

Wichtiger Hinweis	Für Ausfallzeiten, die schon aufgetreten sind, sind alle Felder auf der Seite Eigenschaften editierbar.
Aufbau des Assistenten	Der "Assistent für neue Ausfallzeit" auf der vorherigen Seite besteht aus folgenden Elementen:
	Seite "Eigenschaften" > "Seite "CIs auswählen" " auf der nächsten Seite > "Seite "Planung" " auf Seite 234 > "Seite "Aktion"" auf Seite 235 > "Seite "Benachrichtigung" " auf Seite 238 > "Seite "Vorschau" " auf Seite 238
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Elemente der Oberfläche	Beschreibung
Name der Ausfallzeit	Darf 200 Zeichen nicht überschreiten.
Beschreibung der Ausfallzeit	Diese Beschreibung wird auch im "Downtime Information Area" im BSM-Benutzerhandbuch angezeigt.
Genehmigt von	Hier können Sie die Person oder die Abteilung angeben, die die Ausfallzeit genehmigt hat. Darf 50 Zeichen nicht überschreiten.
Geplant	Wählen Sie aus, ob diese Ausfallzeit als geplant markiert sein soll. Sie können auch ungeplante Ausfallzeiten erstellen. Dies dient nur Informationszwecken.

Elemente der Oberfläche	Beschreibung
Kategorie der Ausfallzeit	Wählen Sie eine Kategorie aus der Dropdownliste aus. Mit dieser Kategorie wird der Grund für die Ausfallzeit beschrieben.
	Sie können auch eigene angepasste Kategorien mithilfe der Infrastruktureinstellungen erstellen.
	Zum Hinzufügen einer benutzerdefinierten Ausfallzeitkategorie klicken Sie auf Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen.
	Wählen Sie Foundation aus.
	Wählen Sie Ausfall aus.
	Ändern Sie in der Tabelle Ausfall - Allgemeine Einstellungen die Ausfallkategorien in den Namen, den Sie als angepasste Kategorie für die Ausfallzeit verwenden möchten. Der eingegebene Name wird als Option in der Liste der verfügbaren Ausfallzeitenkategorien angezeigt, nachdem Sie BSM. neu gestartet haben.

Seite "Cls auswählen"

Diese Seite des Assistenten ermöglicht Ihnen das Auswählen der CIs, die von der Ausfallzeit betroffen sind.

Wichtiger Hinweis	Für Ausfallzeiten, die schon aufgetreten sind, können keine ausgewählten CIs auf dieser Seite bearbeitet werden.
Aufbau des Assistenten	Der "Assistent für neue Ausfallzeit" auf Seite 231 besteht aus folgenden Elementen:
	"Seite "Eigenschaften" " auf der vorherigen Seite > Seite "CIs auswählen" > "Seite "Planung" " auf der nächsten Seite > "Seite "Aktion"" auf Seite 235 > "Seite "Benachrichtigung" " auf Seite 238 > "Seite "Vorschau" " auf Seite 238
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Elemente der Oberfläche	Beschreibung
Verfügbare	Wählen Sie aus der Liste die Ansicht aus, die die von dieser Ausfallzeit
Cls	betroffenen CIs enthält. Sie können die Schaltfläche 🗒 verwenden, um eine Suche unter den verfügbaren Ansichten durchzuführen.
	Markieren Sie ein CI aus der Ansicht, um es in die Liste Ausgewählte CIs zu verschieben. Halten Sie die Strg-Taste gedrückt, um mehrere CIs auszuwählen
	Alle Ansichten, für die eine Anzeigeberechtigung des Benutzers vorliegt, können ausgewählt werden. Sie können nur CIs der folgenden CI-Typen auswählen:
	Knoten
	Ausgeführte Software
	Geschäftsprozess
	Unternehmensapplikation
	CI-Sammlung
	Infrastrukturservice
	Geschäftsservice
Ausgewählte Cls	Nach dem Auswählen der CIs werden diese in der Liste Ausgewählte CIs angezeigt. Um ein CI aus dem Ausfallzeitbereich zu entfernen, wählen Sie das CI unter Ausgewählte CIs aus und klicken auf den Zurückpfeil, um es wieder in die Liste Verfügbare CIs zu verschieben.

Seite "Planung"

Auf dieser Seite des Assistenten können Sie die Planung für die Ausfallzeit konfigurieren.

Wichtiger Hinweis	Eine Ausfallzeit kann nicht für die Vergangenheit geplant werden.
	Für Ausfallzeiten, die schon aufgetreten sind, ist nur das folgende Feld auf der Seite Planung editierbar.
	Ende um-Datum in Serienbereich
	Um eine wiederkehrende Ausfallzeit abzubrechen, die schon mindestens ein Mal aufgetreten ist, bearbeiten Sie die Ausfallzeit und ändern dieses Feld.
Aufbau des Assistenten	Der "Assistent für neue Ausfallzeit" auf Seite 231 besteht aus folgenden Elementen:
	"Seite "Eigenschaften" " auf Seite 232 > "Seite "CIs auswählen" " auf der vorherigen Seite > Seite "Planung" > "Seite "Aktion"" auf der nächsten Seite > "Seite "Benachrichtigung" " auf Seite 238 > "Seite "Vorschau" " auf Seite 238
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Elemente der Oberfläche	Beschreibung
Zeiteinstellung	Start. In der Dropdownliste sind Zeiteinstellungen zur vollen Stunde und zur halben Stunde enthalten. Um eine andere Tageszeit auszuwählen, wählen Sie die halbstündliche Einstellung aus, die dieser am nächsten liegt, und geben die tatsächliche Zeit für den Start ein. Für 02:10 Uhr wählen Sie beispielsweise 02:00 Uhr aus und ändern die Minuten in 02:10 Uhr.
	Ende. Sie können eine Endezeit auswählen, wobei die Dauer automatisch angepasst wird. Oder Sie wählen eine Einstellung für die Dauer aus und die Endezeit wird automatisch angepasst.
	Dauer. Beinhaltet Optionen zwischen 5 Minuten und einer Woche. Die Dauer für die Ausfallzeit muss in Inkrementen von 5 Minuten als Wert in Minuten, Stunden, Tagen oder Wochen definiert werden.
	Wird die Zeitdauer nicht angezeigt, beispielsweise 1 1/2 Stunden, geben Sie die Endezeit an, sodass die Dauer automatisch angepasst wird.
	Um einen Wert auszuwählen, der größer ist als 1 Woche, wählen Sie den Wert 1 Woche aus und geben in das Feld die korrekte Anzahl der Wochen ein.
Serien-Pattern	Wählen Sie eine der folgenden Optionen aus:
	Einmal. Die Ausfallzeit tritt nur einmal wie geplant auf und nicht mehrfach. Wählen Sie ein Kalenderdatum für das Auftreten aus.
	Wöchentlich. Wählen Sie den Wochentag für die geplante wöchentliche Serie aus.
	Monatlich. Wählen Sie einen Tag des Monats aus der Dropdownliste für die geplante monatliche Serie aus.
Serienbereich	Wenn Sie Wöchentlich oder Monatlich ausgewählt haben:
	Sie müssen ein Datum unter Start auswählen.
	Wählen Sie entweder ein Datum unter Ende um oder Kein Enddatum aus.
Zeitzone	Alle Zeitzonen werden in Bezug zur GMT angezeigt.

Seite "Aktion"

Diese Seite des Assistenten ermöglicht Ihnen das Definieren der Aktionen, die während der Ausfallzeit durchgeführt werden.

Wichtiger	Für Ausfallzeiten, die schon aufgetreten sind, sind keine Felder auf der Seite
Hinweis	Aktion editierbar.

Aufbau des Assistenten	Der "Assistent für neue Ausfallzeit" auf Seite 231 besteht aus folgenden Elementen:
	"Seite "Eigenschaften" " auf Seite 232 > "Seite "CIs auswählen" " auf Seite 233 > "Seite "Planung" " auf Seite 234 > Seite "Aktion" > "Seite "Benachrichtigung" " auf Seite 238 > "Seite "Vorschau" " auf Seite 238
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Elemente der Oberfläche	Beschreibung
Keine Aktion	Es werden keine Aktionen für verbundene CIs oder CI- Überwachung, Warnungen, Reports oder SLAs durchgeführt.
	Hinweis: Während dieser Ausfallzeit wird der Status des betroffenen CIs nicht in Ausfallzeit geändert. CI-Status-Warnungen sind so konfiguriert, dass sie ausgelöst werden, sobald das CI den Status wechselt.
Warnungen unterdrücken und Ereignisse	Es werden keine Warnungen oder zugehörige Benachrichtigungen oder Aktionen für mit der Ausfallzeit verbundene CIs gesendet.
berücksichtigen	Standardmäßig werden Ereignisse als geschlossen übermittelt. Ist OMi installiert, kann die Ereignisverarbeitung in der Ausfallzeit unter Admin > Operationenverwaltung > Operationenverwaltung abstimmen > Ausfallzeitverhalten konfiguriert werden und die Einstellung hier überschreiben.
	Die Überwachung wird fortgesetzt und Reports, Status in Service Health und SLAs werden aktualisiert.
	Hinweis: Während der Ausfallzeit kann das betroffene CI seinen Status ändern und die Statusänderung die entsprechende CI-Status-Warnung auslösen.
Ausfallzeit für KPI- Berechnungen erzwingen; Warnungen	Es werden keine KPI-Berechnungen ausgeführt und der Status in Service Health wird nicht aktualisiert. Stattdessen wird die Ausfallzeit des CIs angezeigt.
unterdrücken und Ereignisse berücksichtigen	Es werden keine Warnungen oder zugehörige Benachrichtigungen oder Aktionen für mit der Ausfallzeit verbundene CIs gesendet.
	Standardmäßig werden Ereignisse als geschlossen übermittelt. Ist OMi installiert, kann die Ereignisverarbeitung in der Ausfallzeit unter Admin > Operationenverwaltung > Operationenverwaltung abstimmen > Ausfallzeitverhalten konfiguriert werden und die Einstellung hier überschreiben.
	Reporterstellung und Überwachung werden fortgesetzt. SLAs werden aktualisiert.

Elemente der Oberfläche Beschreibung

Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse berücksichtigen

- Report-Daten werden nicht aktualisiert und die Ausfallzeit für die verbundenen CIs wird angezeigt.
- Ausgewählte SLAs werden nicht aktualisiert, wenn sie von den mit der Ausfallzeit verbundenen CIs betroffen sind.
- Es werden keine KPI-Berechnungen ausgeführt und der Status in Service Health wird nicht aktualisiert. Stattdessen wird die Ausfallzeit des CIs angezeigt.
- Es werden keine Warnungen oder zugehörige Benachrichtigungen oder Aktionen für mit der Ausfallzeit verbundene CIs gesendet.
- Standardmäßig werden Ereignisse als geschlossen übermittelt.
 Ist OMi installiert, kann die Ereignisverarbeitung in der Ausfallzeit unter Admin > Operationenverwaltung > Operationenverwaltung abstimmen > Ausfallzeitverhalten konfiguriert werden und die Einstellung hier überschreiben.
- Die Überwachung wird fortgesetzt.

Aktive Überwachung beenden (BPM & SiteScope); Ausfallzeit für Reports und KPI-Berechnungen erzwingen, Warnungen unterdrücken und Ereignisse berücksichtigen (wirkt sich auf alle zugehörigen SLAs aus)

- Die Business Process Monitor- und SiteScope-Überwachung wird beendet.
- Report-Daten werden nicht aktualisiert und die Ausfallzeit für die verbundenen CIs wird angezeigt.
- SLAs werden nicht aktualisiert, wenn sie von den mit der Ausfallzeit verbundenen CIs betroffen sind.
- Es werden keine KPI-Berechnungen ausgeführt und der Status in Service Health wird nicht aktualisiert. Stattdessen wird die Ausfallzeit des CIs angezeigt.
- Es werden keine Warnungen oder zugehörige Benachrichtigungen oder Aktionen für mit der Ausfallzeit verbundene CIs gesendet.
- Standardmäßig werden Ereignisse als geschlossen übermittelt. Ist OMi installiert, kann die Ereignisverarbeitung in der Ausfallzeit unter Admin > Operationenverwaltung > Operationenverwaltung abstimmen > Ausfallzeitverhalten konfiguriert werden und die Einstellung hier überschreiben.

Hinweis: Wenn Sie eine Ausfallzeit für ein Applikations-CI konfigurieren (dessen Daten von der BPM-Überwachung aktualisiert werden), sendet die Ausfallzeitenverwaltung zu Beginn der Ausfallzeit automatisch ein Ereignis an den BPM-Agenten. Der Agent beendet das Senden von Stichproben an BSM. Dabei werden die BPM-Stichproben unterdrückt, die mit den Transaktions-CIs übereinstimmen, bei denen des sich um untergeordnete CIs der Applikations-CIs handelt, für die die Ausfallzeit konfiguriert ist. Pro Transaktion gibt es eine Stichprobe.

Seite "Benachrichtigung"

Mit dieser Seite des Assistenten können Sie die Empfänger festlegen, die eine Benachrichtigung über die Ausfallzeit erhalten sollen. Benachrichtigungen werden per E-Mail versendet, wenn eine Ausfallzeit auftritt und sofort wenn diese beendet ist. Sie können nur Empfänger auswählen, für die eine E-Mail-Adresse definiert wurde.

Wichtiger Hinweis	Für Ausfallzeiten, die schon aufgetreten sind, können Ausgewählte Empfänger auf der Seite Benachrichtigung bearbeitet werden.
Aufbau des Assistenten	Der "Assistent für neue Ausfallzeit" auf Seite 231 besteht aus folgenden Elementen:
	"Seite "Eigenschaften" " auf Seite 232 > "Seite "CIs auswählen" " auf Seite 233 > "Seite "Planung" " auf Seite 234 > "Seite "Aktion"" auf Seite 235 > Seite "Benachrichtigung" > "Seite "Vorschau" " unten
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
*	Öffnet das Dialogfeld Neuer Empfänger , in dem ein Empfänger erstellt werden kann, der noch nicht in der Liste der verfügbaren Empfänger aufgeführt wird. Die Empfänger, die Sie erstellen, stehen als Empfänger in allen Bereichen von BSM zur Verfügung. Weitere Informationen zum Erstellen von Empfängern finden Sie unter "Konfigurieren und Verwalten von Empfängern" auf Seite 359.
Verfügbare Empfänger	Listet die verfügbaren Empfänger für die Ausfallzeitbenachrichtigung per E-Mail, SMS oder Pager auf.
Ausgewählte Empfänger	Listet die ausgewählten Empfänger für die Ausfallzeitbenachrichtigung per E- Mail, SMS oder Pager auf. Sie können eine oder alle drei Möglichkeiten der Benachrichtigung auswählen.

Seite "Vorschau"

Auf dieser Seite des Assistenten sehen Sie eine Zusammenfassung der Ausfallzeiteinstellungen.

Aufbau des Assistenten		
	"Seite "Eigenschaften" " auf Seite 232 > "Seite "CIs auswählen" " auf Seite 233 > "Seite "Planung" " auf Seite 234 > "Seite "Aktion"" auf Seite 235 > "Seite "Benachrichtigung" " > Seite 'Vorschau'	
Siehe auch	"Ausfallzeitenverwaltung" auf Seite 221	

Elemente der Oberfläche	Beschreibung
Tabelle "Vorschau"	Eine Tabelle, in der die für diese Ausfallzeit konfigurierten Werte aufgelistet werden. Sie können auf die Schaltfläche Zurück klicken, um auf die vorherige Seite zu wechseln, auf der ein Wert geändert oder gelöscht werden soll.
	Nachdem Sie auf dieser Seite auf Fertig stellen geklickt haben, wird die Ausfallzeit zum System hinzugefügt und auf der Seite Ausfallzeitenverwaltung angezeigt.

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden Maßnahmen zur Fehlerbehebung bei der Ausfallzeitenverwaltung sowie die Einschränkungen der Ausfallzeitenverwaltung beschrieben.

Bearbeiten von Ausfallzeiten

- Wenn sich der Status einer Ausfallzeit während der Bearbeitung im Assistenten für Ausfallzeiten von Inaktiv in Aktiv ändert, kann sie nicht gespeichert werden.
- Wenn Sie eine sich wiederholende Ausfallzeit verwerfen möchten, die bereits mindestens ein Mal aufgetreten ist, müssen Sie das Datum Ende um auf der Seite Planung bearbeiten.

Ausfallzeiten und Sommerzeit

In Zeitzonen mit Sommerzeit müssen die Umstellungen zwischen Winter- und Sommerzeit bei der Berechnung von Ausfallzeiten wie folgt berücksichtigt werden:

Hinweis: In den folgenden Beispielen werden die Daten und Uhrzeiten zu Grunde gelegt, die bei der Zeitumstellung in großen Teilen der USA gelten.

- 14. März 2010: Um 2:00 Uhr wird die Uhr auf 3:00 Uhr vorgestellt. Der Zeitraum zwischen 2:00 und 2:59 Uhr ist also nicht vorhanden.
- 7. November 2010: Um 2:00 Uhr wird die Uhr auf 1:00 Uhr zurückgestellt. Der Zeitraum zwischen 1:00 und 1:59 Uhr ist also zwei Mal vorhanden.

In anderen Zeitzonen wird ähnlich vorgegangen, aber das Datum und die Uhrzeiten für die Umstellung können eventuell abweichen.

Die folgenden Beispiele werden in der Tabelle "Auswirkungen von Zeitumstellungen auf geplante Ausfallzeiten – Übersicht über die Beispiele" auf Seite 243 zusammengefasst dargestellt.

Frühling (Winterzeit zu Sommerzeit)

 Wenn die Ausfallzeit vor der Zeitumstellung beginnt und am Tag nach der Umstellung endet, endet sie wie definiert, aber die Dauer ist um 1 Stunde verkürzt.

Beispiel 1:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 14. um 1:30 Uhr beginnt und am 15. um 2:40 Uhr endet. Die Dauer beträgt 1 Tag, 1 Stunde und 10 Minuten.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 14. um 1:30 Uhr und endet am 15. um 2:40. Die Dauer beträgt 1 Tag, 1 Stunde und 10 Minuten.

Sommer-/Winterzeitumstellung am 14. März 2010: Die Ausfallzeit beginnt am 14. um 1:30 Uhr und endet am 15. um 2:40, aber die Dauer beträgt 1 Tag, 0 Stunden und 10 Minuten (1 Stunde weniger als definiert).

 Wenn die Ausfallzeit vor der Zeitumstellung beginnt und am gleichen Tag, aber nach der Umstellung endet, endet sie 1 Stunde später als definiert, aber die Dauer entspricht der definierten Dauer.

Beispiel 2:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 13. um 23:00 Uhr beginnt und 5 Stunden dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 13. um 23:00 Uhr und endet am 14. um 4:00 Uhr.

Sommer-/Winterzeitumstellung am 14. März 2010: Die Ausfallzeit beginnt am 13. um 23:00 Uhr und endet am 14. um 5:00 Uhr, und die Dauer bleibt 5 Stunden.

• Wenn die Ausfallzeit eigentlich in der übersprungenen Stunde beginnen soll, wird die Startzeit automatisch um 1 Stunde verschoben, und die definierte Dauer bleibt bestehen.

Beispiel 3:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 14. um 2:30 Uhr beginnt und 2 Stunden dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 14. um 2:30 Uhr und endet am 14. um 4:30 Uhr.

Sommer-/Winterzeitumstellung am 14. März 2010: Die Ausfallzeit beginnt am 14. um 3:30 Uhr und endet am 14. um 5:30 Uhr, und die Dauer bleibt 2 Stunden.

 Wenn die Ausfallzeit eigentlich vor der Zeitumstellung beginnen und während der übersprungenen Stunde enden soll, wird die Endzeit automatisch um 1 Stunde verschoben, und die definierte Dauer bleibt bestehen.

Beispiel 4:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 13. um 1:30 Uhr beginnt und 1 Tag, 1 Stunde und 10 Minuten dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 13. um 1:30 Uhr und endet am 14. um 2:40 Uhr. Die Dauer beträgt 1 Tag, 1 Stunde und 10 Minuten.

Sommer-/Winterzeitumstellung am 14. März 2010: Die Ausfallzeit beginnt am 13. um 1:30 Uhr und endet am 14. um 3:40 Uhr. Die Dauer ist wie definiert: 1 Tag, 1 Stunde und 10 Minuten.

 Wenn die Ausfallzeit eigentlich während der übersprungenen Stunde beginnen und enden soll, findet sie eine Stunde später als definiert statt.

Beispiel 5:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 14. um 2:00 Uhr beginnt und 1 Stunde dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 14. um 2:00 Uhr und endet am 14. um 3:00 Uhr.

Sommer-/Winterzeitumstellung am 14. März 2010: Die Ausfallzeit beginnt am 14. um 3:00 Uhr und endet am 14. um 4:00 Uhr, und die Dauer bleibt wie definiert: 1 Stunde.

Herbst (Sommerzeit zu Winterzeit)

 Wenn die Ausfallzeit nach der Zeitumstellung beginnt und endet, bleiben Endzeit und Dauer wie definiert. Wenn die Ausfallzeit vor der Zeitumstellung beginnt (am Tag der Umstellung oder am Tag davor) und nach der Umstellung am gleichen Tag endet, endet sie 1 Stunde früher als definiert, aber die Dauer entspricht der definierten Dauer.

Beispiel 6:

Zwei Ausfallzeiten pro Monat, die jeweils am 7. um Mitternacht beginnen. Die Dauer der ersten Ausfallzeit beträgt 1 Stunde, die der zweiten 2 Stunden.

Keine Sommer-/Winterzeitumstellung: Die erste Ausfallzeit findet am 7. von 0:00 bis 1:00 Uhr statt (Dauer 1 Stunde) und die zweite am 7. von 0:00 bis 2:00 Uhr (Dauer 2 Stunden).

Sommerzeit-/Winterzeitumstellung am 7. November 2010: Die erste Ausfallzeit beginnt am 7. um 0:00 Uhr Sommerzeit und endet am 7. um 1:00 Uhr Sommerzeit, die Dauer beträgt 1 Stunde. Die zweite Ausfallzeit beginnt am 7. um 0:00 Uhr Sommerzeit und endet am 7. um 1:00 Uhr Winterzeit, die Dauer bleibt 2 Stunden, wie definiert.

Beispiel 7:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 7. um Mitternacht beginnt und 4 Stunden dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 7. um 0:00 Uhr und endet am 7. um 4:00 Uhr.

Sommerzeit-/Winterzeitumstellung am 7. November 2010: Die Ausfallzeit beginnt am 7. um 0:00 Uhr und endet am 7. um 3:00 Uhr, und die Dauer bleibt wie definiert: 4 Stunden.

Beispiel 8:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 6. um 20:00 Uhr beginnt und 7 Stunden dauert

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 6. um 20:00 Uhr und endet am 7. um 3:00 Uhr.

Sommerzeit-/Winterzeitumstellung am 7. November 2010: Die Ausfallzeit beginnt am 6. um 20:00 Uhr und endet am 7. um 2:00 Uhr, und die Dauer bleibt wie definiert: 7 Stunden.

 Wenn die Ausfallzeit vor der Zeitumstellung beginnt und am Tag nach der Umstellung endet, endet sie wie definiert, aber die Dauer ist 1 Stunde länger.

Beispiel 9:

Monatlich wiederkehrende Ausfallzeit, die jeweils am 7. um 0:00 Uhr (Mitternacht) beginnt und 1 Tag und 1 Stunde (25 Stunden) dauert.

Keine Sommer-/Winterzeitumstellung: Die Ausfallzeit beginnt am 7. um 0:00 Uhr und endet am 8. um 1:00 Uhr.

Sommerzeit-/Winterzeitumstellung am 7. November 2010: Die Ausfallzeit beginnt am 7. um 0:00 Uhr und endet am 8. um 1:00 Uhr, aber die Dauer beträgt 26 Stunden.

Auswirkungen von Zeitumstellungen auf geplante Ausfallzeiten – Übersicht über die Beispiele

Beispiel	Festgelegte Ausfallzeit/Ausfallzeit mit Sommer-/Winterzeitumstellung	Startzeit	Endzeit	Dauer
1	Festgelegt	am 14. um 01:30 Uhr	am 15. um 2:40 Uhr	1 Tag, 1 Stunde, 10 Minuten
	Mit Sommer-/Winterzeitumstellung	am 14. um 1:30 Uhr	am 15. um 2:40 Uhr	1 Tag, 0 Stunden, 10 Minuten
2	Festgelegt	am 13. um 23:00 Uhr	am 14. um 4:00 Uhr	5 Stunden
	Mit Sommer-/Winterzeitumstellung	am 13. um 23:00 Uhr	am 14. um 5:00 Uhr	5 Stunden
3	Festgelegt	am 14. um 2:30 Uhr	am 14. um 4:30 Uhr	2 Stunden
	Mit Sommer-/Winterzeitumstellung	am 14. um 3:30 Uhr	am 14. um 5:30 Uhr	2 Stunden
4	Festgelegt	am 13. um 1:30 Uhr	am 14. um 2:40 Uhr	1 Tag, 1 Stunde und 10 Minuten
	Mit Sommer-/Winterzeitumstellung	am 13. um 1:30 Uhr	am 14. um 3:40 Uhr	1 Tag, 1 Stunde und 10 Minuten
5	Festgelegt	am 14. um 2:00 Uhr	am 14. um 3:00 Uhr	1 Stunde
	Mit Sommer-/Winterzeitumstellung	am 14. um 3:00 Uhr	am 14. um 4:00 Uhr	1 Stunde

Beispiel	Festgelegte Ausfallzeit/Ausfallzeit mit Sommer-/Winterzeitumstellung		Startzeit	Endzeit	Dauer
6	1.	Festgelegt	am 7. um 0:00 Uhr	am 7. um 1:00 Uhr	1 Stunde
		Mit Sommer-/ Winterzeitumstellung	am 7. um 0:00 Uhr	am 7. um 1:00 Uhr	1 Stunde
	2.	Festgelegt	am 7. um 0:00 Uhr	am 7. um 2:00 Uhr	2 Stunden
		Mit Sommer-/ Winterzeitumstellung	am 7. um 0:00 Uhr	am 7. um 1:00 Uhr Winterzeit	2 Stunden
7	Festgelegt		am 7. um 0:00 Uhr	am 7. um 4:00 Uhr	4 Stunden
	Mit Sommer-/Winterzeitumstellung		am 7. um 0:00 Uhr	am 7. um 3:00 Uhr	4 Stunden
8	Festgelegt		am 6. um 20:00 Uhr	am 7. um 3:00 Uhr	7 Stunden
	Mit Sommer-/Winterzeitumstellung		am 6. um 20:00 Uhr	am 7. um 2:00 Uhr	7 Stunden
9	Festgelegt		am 7. um 0:00 Uhr	am 8. um 1:00 Uhr	25 Stunden
	Mit Sommer-/Winterzeitumstellung		am 7. um 0:00 Uhr	am 8. um 1:00 Uhr	26 Stunden

Teil 4

Benutzer, Berechtigungen und Empfänger

Kapitel 18

Benutzerverwaltung

Mithilfe der Benutzerverwaltung können Sie:

 BSM-Gruppen und -Benutzer konfigurieren. Mithilfe von Berechtigungen können Sie den Benutzerzugriff auf bestimmte Bereiche beschränken. Berechtigungen können entweder direkt oder über eine Benutzergruppe zugewiesen werden. Sie gruppieren Benutzer, um die Verwaltung von Benutzerberechtigungen zu vereinfachen. Statt immer nur einem Benutzer Zugriffsberechtigungen zuzuweisen, können Sie Benutzer gruppieren, denen dieselben Berechtigungsstufen für dieselben Ressourcen zugewiesen werden.

Sie können unterschiedliche Gruppen abhängig von dem erforderlichen Benutzerzugriff auf die unterschiedlichen Ressourcen in BSM erstellen. Beispiele für Kriterien für das Gruppieren von Benutzern in Ihrer Organisation sind:

Funktionen innerhalb der Organisation	Standorte und Regionen
Kundendienstvertreter	Benutzer, die in unterschiedlichen Vertriebsregionen arbeiten
Systemadministratoren	Benutzer basierend auf geografischem Standort
Oberes Management	Benutzer, die auf Netzwerkserver an unterschiedlichen Standorten zugreifen

In der Registerkarte **Allgemein** können Sie die Parameter eines Benutzers ändern, wie den Benutzernamen und das Kennwort. Weitere Informationen finden Sie unter "Registerkarte "Allgemein" (Benutzerverwaltung)" auf Seite 341.

Weitere Informationen zum Erstellen von Gruppen und Benutzern finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

Definieren eines Superusers. Für jede BSM-Installation wird ein Superuser definiert. Der Anmeldename des Superusers lautet admin. Das Anfangskennwort für dieses Konto wird im
Dienstprogramm für die Setup- und Datenbankkonfiguration festgelegt. Dieser ursprüngliche
Superuser wird nicht in der Benutzerliste der Benutzerverwaltung aufgelistet. Daher kann das
Kennwort dieses Benutzers nur auf der Seite Allgemeine Einstellungen im Bereich mit den
persönlichen Einstellungen (Admin > Persönliche Einstellungen) geändert werden. Details
zur Benutzeroberfläche für diese Aufgabe finden Sie unter "Seite "Benutzerkonto" auf Seite
382.

Der Superuser kann auf andere Benutzer des Systems angewendet werden. Diese Benutzer mit Superuser-Berechtigungen werden in der Benutzerverwaltung aufgelistet und können nicht geändert werden. Weitere Informationen zum Anwenden von Berechtigungen finden Sie unter "Zuweisen von Berechtigungen" auf Seite 266.

• Zuweisen eines Empfängers für einen Benutzer. Sie können einem Benutzer einen

Empfänger zuweisen. Ein Empfänger kann Warnungen und geplante Reports empfangen. Details zu Empfängern finden Sie unter "Empfängerverwaltung" auf Seite 358.

- Zuweisen von Berechtigungen zu Gruppen und Benutzern. Die Benutzeroberfläche für die Benutzerverwaltung steht nur Benutzern mit den entsprechenden Berechtigungen zur Verfügung. Die Berechtigungen eines Benutzers werden entweder von zugewiesenen Rollen geerbt oder bei der Konfiguration von Parametern einzeln zugewiesen. Details zu Berechtigungen finden Sie unter "Berechtigungen" auf der nächsten Seite.
- Festlegen der Gruppen- und Benutzerhierarchie. Sie können Benutzer zu Gruppen hinzufügen und Gruppen in anderen Gruppen verschachteln. Details finden Sie unter "Gruppen- und Benutzerhierarchie" auf Seite 254.
- Anpassen der Benutzereinstellungen. Wählen Sie die Seite aus, die Benutzern beim Aufrufen von BSM angezeigt wird. Wählen Sie außerdem die Menüelemente aus, die auf den Seiten von BSM zur Verfügung stehen. Details finden Sie unter "Anpassen der Benutzermenüs" auf Seite 256.

Berechtigungen

Sie können den in Ihrer BSM-Plattform definierten Gruppen und Benutzern Berechtigungen zuweisen und damit den Zugriff auf bestimmte Bereiche von BSM ermöglichen.

Beim Erteilen von Berechtigungen sind folgende Komponenten notwendig:

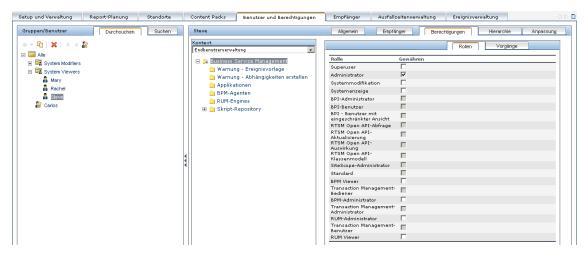
- Benutzer
- Ressource
- die Rolle oder Operation, für die die Berechtigung erteilt werden soll

Die Registerkarte **Berechtigungen** umfasst die folgenden Bereiche:

- Einen Bereich mit der Ressourcenstruktur in der Mitte der Seite, der die Kontexte, Ressourcen und Ressourceninstanzen umfasst, für die Berechtigungen zugewiesen werden können. Details finden Sie unter "Grundlegende Informationen zu Berechtigungen für Ressourcen" auf der nächsten Seite.
- Einen Bereich mit Rollen und Operationen rechts auf der Seite. Details zu Rollen finden Sie unter "Rollen" auf Seite 251. Details zu Operationen finden Sie unter "Operationen" auf Seite 252.

Außerdem ist der Ausschnitt Gruppen/Benutzer links auf der Seite kontinuierlich geöffnet.

Nachfolgend sehen Sie ein Beispiel für das Erteilen von Berechtigungen:



Weitere Informationen zum Zuweisen von Berechtigungen finden Sie unter "Zuweisen von Berechtigungen" auf Seite 266.

Hinweis:

- Wenn Sie ein Upgrade von einer früheren Version von BSM durchgeführt haben und in dieser Version bestimmte Benutzer und Sicherheitsstufen definiert waren, werden diese Benutzer und Sicherheitsstufen den neuen Rollen auf der Registerkarte Berechtigungen zugeordnet. Details finden Sie unter "Rollen" auf Seite 251.
- Sie können Benutzer und Gruppen zusammen mit den zugehörigen Rollen von einem BSM-

Computer auf einen anderen exportieren. Details erhalten Sie bei der HP Software-Unterstützung.

Grundlegende Informationen zu Berechtigungen für Ressourcen

Mit BSM können Sie Ihre Berechtigungsverwaltung optimieren, indem Sie Berechtigungen auf Ressourcenebene erteilen. Alle Ressourcen, für die Berechtigungen erteilt werden können, wurden in einer hierarchischen Struktur identifiziert und kategorisiert, die die BSM-Plattform bildet.

Die Ressourcen und Instanzen dieser Ressourcen sind in logischen Gruppierungen organisiert, die als **Kontexte** bezeichnet werden. Kontexte vereinfachen das Identifizieren und Auswählen des Bereichs der Plattform, auf den Sie Berechtigungen anwenden möchten.

Die Ressourcen werden anhand des Kontextes eingeteilt, in dem sie innerhalb der Plattform funktionieren, und nicht notwendigerweise danach, wo sie sich auf der Benutzeroberfläche befinden.

Dieser Abschnitt umfasst darüber hinaus die folgenden Themen:

- "Ressourcen und Ressourceninstanzen"
- "Richtlinien für das Arbeiten mit Ressourcen"

Ressourcen und Ressourceninstanzen

In der Berechtigungsverwaltung werden folgende Typen von Ressourcen verwendet. Jeder Typ wird in der Ressourcenstruktur durch ein anderes Symbol gekennzeichnet:

<u> </u>	Ressourcensammlung (eine Ressource, die mehrere Instanzen besitzen kann)
<u>_</u> *	Instanz einer Ressource
副	Ressourcen, die in der Berechtigungsressourcenstruktur nicht über Instanzen verfügen können

Eine Instanz einer Ressource wird nur angezeigt, wenn diese in der Plattform definiert wurde. Die Instanz einer Ressource wird in der Struktur als untergeordnetes Objekt der Ressource mit dem Namen angezeigt, mit dem sie in der Applikation definiert wurde. Wenn im System Instanzen einer Ressource definiert wurden, dient die Ressourcensammlung als übergeordnete Ressource für diese Instanzen.

Es gibt einige Ressourcen, die in der Hierarchie der Ressourcenstruktur andere Ressourcen enthalten, wie zum Beispiel die unterschiedlichen Daten-Collector-Profile. Einige dieser Typen untergeordneter Ressourcen werden nur angezeigt, wenn auf Ihrer Plattform Instanzen der Ressource definiert sind, wie zum Beispiel Monitor- und Transaktionsressourcen innerhalb einer Profilressource.

Ressourcen, die in der Berechtigungsstruktur über keine Instanzen verfügen können, werden in die folgenden Typen aufgeteilt:

 Ressourcen, die innerhalb des Systems als Funktionen oder Optionen dienen und nicht über Instanzen oder Typen verfügen.

Beispiel:

Die Ressource **Ausreißerwert** bestimmt, ob der Benutzer den Ausreißerschwellenwert bearbeiten kann. Diese Ressource besitzt keine Instanzen.

 Ressourcen, die über Instanzen verfügen. Berechtigungen können nur auf den Ressourcentyp angewendet werden und wirken sich auf alle Instanzen der Ressource aus.

Beispiel:

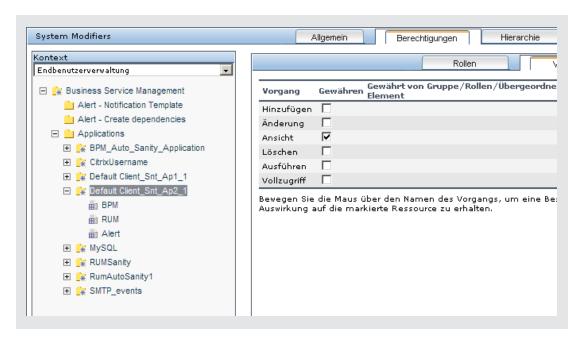
Die Ressource **Kategorie** umfasst alle in der End User Management-Verwaltung definierten Kategorien. Wenn einem Benutzer die Berechtigung **Ändern** für die Ressource **Kategorie** gewährt wurde, kann er alle im System definierten Kategorien ändern. Sie können Berechtigungen nicht für bestimmte Kategorien gewähren oder aufheben, sondern nur für Kategorien, die in der End User Management-Verwaltung definiert sind.

Beispiele für Ressourcen und Instanzen:

Ein Beispiel dafür, wie Ressourcen und Instanzen in der Berechtigungshierarchie angezeigt werden, ist die Ressourcensammlung **Applikationen** im Kontext **End User Management**. Die Ressource **Applikationen** enthält nur Instanzen, wenn im System Applikationen definiert wurden. Einige Instanzen können standardmäßig definiert sein, andere müssen vom Benutzer definiert werden. Wenn im System Applikationen definiert sind, werden diese als Instanz der Ressource **Applikationen** angezeigt.

Da BPM, RUM und Warnungen auf Ihrer Plattform pro Applikation definiert werden, werden die Ressourcen **BPM**, **RUM** und **Warnungen** unter jeder Instanz der Applikationsressource angezeigt.

Sie können Berechtigungen nur auf der Ressourcenebene für Applikationen anwenden. Auf diese Weise erhält der Benutzer Zugriff auf alle im System erstellten Applikationen. Wenn Sie den Zugriff eines Benutzers auf bestimmte Applikationen beschränken möchten, die mit seinen Aufgaben verbunden sind, können Sie Berechtigungen für diese speziellen Applikationen erteilen und auch Berechtigungen auf bestimmte Ressourcen pro Applikation gewähren oder verweigern.



Richtlinien für das Arbeiten mit Ressourcen

- Die Ressource Business Service Management bezieht sich auf alle Kontexte in BSM.
- Sie können der Ressource Business Service Management nur Rollen aber keine Operationen zuweisen. Details finden Sie unter "Rollen".
- Um die Berechtigungen einer Unterressource zu verwalten, müssen Sie dem Benutzer mindestens die Berechtigung **Anzeigen** für die übergeordnete Ressource gewähren.
- Sie gewähren die Berechtigung Hinzufügen nur für eine Ressource und nicht für die Instanz einer Ressource.
- Wenn ein Benutzer eine Instanz einer Ressource definiert oder erstellt, beispielsweise wenn er ein Profil "Geschäftsprozess' erstellt, besitzt der Benutzer die Berechtigung Vollzugriff für die Ressourceninstanz und alle untergeordneten Ressourcen.

Rollen

BSM ermöglicht es Ihnen, Berechtigungen mithilfe von Rollen für bestimmte Benutzer oder Gruppen in Ihrer Organisation zu übernehmen. Zu diesen Rollen gehört eine vorkonfigurierte Sammlung aus Ressourcen und einer Gruppe von Operationen, die zu diesen Ressourcen gehören.

Rollen sind nach Kontext organisiert, der bestimmt, welche Ressourcen und Operationen vorkonfiguriert und in den Rollen enthalten sind. Weitere Informationen dazu, welche Operation auf welche Ressource angewendet wird, finden Sie unter "Operationen" auf der nächsten Seite.

Rollen können nur auf bestimmte Ressourcen angewendet werden:

- Rollen, die Ressourcen aus verschiedenen Kontexten beinhalten, können nur auf die Business Service Management-Ressource verwendet werden. Business Service Management wird in allen Kontexten als erste Ressourcensammlung angezeigt.
- Rollen, deren Ressourcen sich alle in einem Kontext befinden, können nur auf bestimmte Ressourcen innerhalb dieses Kontexts angewendet werden.

Eine Beschreibung der einzelnen Rollen, darunter Details zu den Ressourcen, auf die Rollen angewendet werden können, finden Sie unter "Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung" auf Seite 280.

Operationen

Beachten Sie bei der Arbeit mit Operationen Folgendes:

- Alle Operationen, die auf eine Ressourcensammlung angewendet werden können, können auch auf Instanzen dieser Ressource angewendet werden. Einzige Ausnahme ist die Operation Hinzufügen, die nicht auf die Instanz einer Ressource angewendet werden kann.
- Die Operation Vollzugriff schließt automatisch alle anderen für die Ressource verfügbaren Operationen ein. Wird sie angewendet, werden die anderen Operationen automatisch ausgewählt.
- Wird die Operation Vollzugriff auf eine andere Ressource angewendet, hat der Benutzer auch die Berechtigung zum Gewähren oder Entfernen von Berechtigungen für diese Ressource oder Ressourceninstanz für andere Benutzer oder Gruppen.
- Wenn die Operation Ansicht zu den verfügbaren Operationen der Ressource gehört und Sie eine der anderen verfügbaren Operationen auswählen, wird die Operation Ansicht ebenfalls automatisch ausgewählt.

Weitere Informationen zu den in BSM verfügbaren Operationen finden Sie unter "Operationen für die Benutzerverwaltung" auf Seite 314.

Sicherheits-Officer

Der Sicherheits-Officer ist ein Benutzer, der über Sicherheitsberechtigungen zum Anzeigen sensibler Informationen im System verfügt. Der Sicherheits-Officer, bei dem es sich im Allgemeinen nicht um einen gewöhnlichen BSM-Benutzer handelt, erhält Zugriff für die Konfiguration bestimmter sensibler Report-Informationen. In Real User Monitor kann der Sicherheits-Officer Einstellungen für die Maskierung sensibler Daten konfigurieren. Weitere Informationen finden Sie unter "Sensitive Data Area" im BSM Application Administration Guide.

Im Allgemeinen greift dieser Benutzer nicht auf andere Bereiche in BSM zu.

Es kann nur ein Benutzer im System als Sicherheits-Officer zugewiesen werden. Nur ein Benutzer mit Superuser-Berechtigungen kann den Sicherheits-Officer erstmalig zuweisen. Anschließend kann nur der als Sicherheits-Officer zugewiesene Benutzer den Status des Sicherheits-Officers an einen anderen Benutzer übergeben oder sein eigenes Kennwort ändern. Der Superuser kann den Status des Sicherheits-Officers nicht mehr zuweisen.

Der Sicherheits-Officer wird durch Markieren eines Benutzers in der Benutzerverwaltungsstruktur und Klicken auf das Symbol **Sicherheits-Officer** ernannt. Details zur Benutzeroberfläche finden Sie unter "Ausschnitt "Gruppen/Benutzer"" auf Seite 352.

Kein anderer Benutzer im System kann den als Sicherheits-Officer zugewiesenen Benutzer löschen. Der Status als Sicherheits-Officer muss einem anderen Benutzer durch den aktuell als Sicherheits-Officer fungierenden Benutzer zugewiesen werden, bevor dieser Benutzer aus dem System gelöscht werden kann.

BSM-Plattformverwaltungshandbuch

Kapitel 18: Benutzerverwaltung

Für den unvorhergesehenen Fall, dass der Sicherheits-Officer nicht mehr auf das System zugreifen kann, um den Status des Sicherheits-Officers einem anderen Benutzer zuzuweisen, kann der Administrator mithilfe der JMX-Konsole den Status des Sicherheits-Officers für den Benutzer löschen. Details zur Durchführung dieser Aufgabe finden Sie unter "Entfernen des Status "Sicherheits-Officer" über die JMX-Konsole " auf Seite 270.

Gruppen- und Benutzerhierarchie

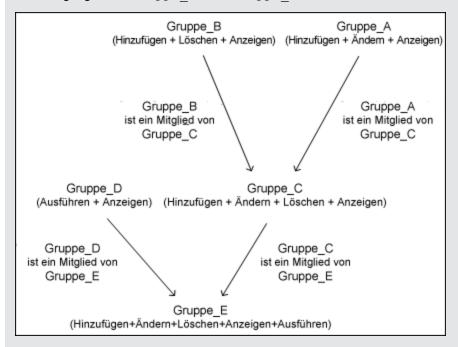
Sie können Gruppen verschachteln, um die Verwaltung von Benutzer- und Gruppenberechtigungen zu vereinfachen. Anstatt Zugriffsberechtigungen jeder Gruppe einzeln zuzuweisen, können Sie eine Gruppe verschachteln und die Berechtigungen ihrer übergeordneten Gruppe vererben.

Beachten Sie beim Verschachteln von Gruppen Folgendes:

- Eine Gruppe kann mehreren Gruppen angehören.
- Berechtigungen werden verschachtelten Gruppen auf dieselbe Weise zugewiesen wie normalen, nicht verschachtelten Gruppen. Änderungen an den Berechtigungen verschachtelter Gruppen werden bei der nächsten Anmeldung des Benutzers wirksam.
- Es besteht keine Beschränkung für die Verschachtelungsebenen von Gruppen.

Beispiel:

In dem folgenden Beispiel sind <code>Gruppe_A</code> und <code>Gruppe_B</code> verschachtelte Mitglieder von <code>Gruppe_C</code>. <code>Gruppe_C</code> erbt die kombinierten Berechtigungen beider Gruppen. <code>Gruppe_C</code> und <code>Gruppe_D</code> sind verschachtelte Mitglieder von <code>Gruppe_E</code>. <code>Gruppe_E</code> erbt die Berechtigungen direkt von <code>Gruppe_C</code> und <code>Gruppe_D</code> und erbt indirekt die Berechtigungen von <code>Gruppe_A</code> und <code>Gruppe_B</code>.



Wenn Berechtigungen zu einer verschachtelten Gruppe hinzugefügt werden oder aus dieser entfernt werden, werden die Änderungen automatisch in die Gruppe implementiert, die der Gruppe direkt übergeordnet ist. Die Weitergabe an zusätzliche übergeordnete Gruppen erfolgt ebenfalls automatisch. Wenn beispielsweise die Berechtigung Löschen aus Gruppe_B entfernt wird, erhält Gruppe_C die Berechtigungen Hinzufügen + Ändern + Anzeigen. Die Berechtigungen von Gruppe_E werden geändert in Hinzufügen + Ändern + Anzeigen + Ausführen.

Eine Schleife verschachtelter Gruppen ist nicht zulässig. Zum Beispiel: Gruppe_A ist ein Mitglied von Gruppe_B und Gruppe_B ist ein Mitglied von Gruppe_C. Gruppe_C kann nicht Mitglied von Gruppe A sein.

Hinweis: Alle Berechtigungen in dem vorherigen Beispiel beziehen sich auf dieselbe Ressource.

Details zum Einrichten verschachtelter Gruppen finden Sie unter "Konfigurieren der Gruppen- und Benutzerhierarchie" auf Seite 267.

Anpassen der Benutzermenüs

Sie können Benutzermenüs mit den folgenden Zielen anpassen:

- Auswählen des Standardkontexts, der für bestimmte Benutzer angezeigt wird, wenn sie sich bei BSM anmelden
- Festlegen der ersten Seite, die für bestimmte Benutzer in den verschiedenen Bereichen von BSM angezeigt wird
- Auswählen von Kontexten und Applikationen, die für bestimmte Benutzer ausgeblendet werden sollen
- Festlegen der Registerkarten und Optionen, die auf den Seiten in BSM zur Verfügung stehen

Durch das Anpassen der Eingangsseite, der Menüelemente und der Registerkarten kann die Benutzeroberfläche so eingestellt werden, dass nur die Bereiche von BSM angezeigt werden, die für bestimmte Benutzer relevant sind.

Ausführliche Beschreibungen zum Anpassen von Benutzermenüs finden Sie unter "Anpassen von Benutzermenüs" auf Seite 273.

Die Benutzermenüs werden auf der Registerkarte **Anpassung** angepasst. Informationen zur Benutzeroberfläche der Registerkarte **Anpassung** finden Sie unter "Registerkarte "Anpassung" (Benutzerverwaltung)" auf Seite 340.

Hinweis: Für die Applikationen Service Health und Operations Management können Sie keinen Benutzerzugriff für spezifische Seiten definieren, Sie können hier nur den Benutzerzugriff auf Applikationsebene aktivieren oder deaktivieren.

Konfigurieren von Benutzern und Berechtigungen – Workflow

In dieser Aufgabe wird die empfohlene Vorgehensweise zur Verwendung der Applikation **Benutzerverwaltung** beschrieben. Sie können Einstellungen für die Benutzerverwaltung in einer beliebigen logischen Reihenfolge konfigurieren.

Ein fallspezifisches Szenario für diese Aufgabe finden Sie unter "Konfigurieren von Benutzern und Berechtigungen – Fallspezifisches Szenario" auf Seite 259.

1. Voraussetzungen

Bevor Sie das Portal für die Benutzerverwaltung konfigurieren, sollten Sie die erforderlichen Benutzer und Gruppen sowie ihre entsprechenden Berechtigungsstufen zuordnen, bevor Sie diese in BSM definieren. Geben Sie zum Beispiel die folgenden Informationen in ein Datenblatt ein:

- Eine Liste der Benutzer, die das System verwalten, sowie die Endbenutzer, die auf Service Health und Reports zugreifen müssen. Tragen Sie die entsprechenden Benutzerinformationen zusammen, wie Benutzernamen, Anmeldenamen, Anfangskennwörter und Benutzerzeitzonen. Obwohl es nicht zum Definieren von Benutzern erforderlich ist, kann es hier hilfreich sein, auch Benutzerkontaktinformationen wie Telefonnummern sowie Pager- und E-Mail-Adressen zu erfassen. (Kontaktinformationen sind für HP Software-as-a-Service-Kunden erforderlich.)
- Wenn eine Kategorisierung der Benutzer in Modi (Operationen und Geschäft) erforderlich ist, geben Sie an, welchem Benutzermodus jeder Benutzer zugeordnet werden soll. Weitere Informationen finden Sie unter "KPIs for User Modes" im BSM Application Administration Guide.
- Wenn mehrere Benutzer ähnliche Systemberechtigungen benötigen, erstellen Sie eine Liste der Rollen und der Benutzer für jede Gruppe.
- Die Berechtigungen, die jeder Benutzer oder jede Gruppe benötigt. Um diesen Prozess zu unterstützen, zeigen Sie die Seite für die Berechtigungsverwaltung an. Diese Seite enthält Informationen zu den unterschiedlichen Kontexten und Ressourcen, für die Berechtigungen gewährt werden. Weitere Informationen finden Sie unter "Grundlegende Informationen zu Berechtigungen für Ressourcen" auf Seite 249.

2. Gruppen erstellen

Gehen Sie folgendermaßen vor, um im Bereich Gruppen/Benutzer Gruppen zu erstellen:

- a. Klicken Sie auf der Registerkarte **Durchsuchen** auf die Schaltfläche zum Erstellen von neuen Gruppen/neuen Benutzern , nachdem Sie eine vorhandene Gruppe oder die Stammgruppe ausgewählt haben.
- Wählen Sie Gruppe erstellen aus und geben Sie die Informationen für die Gruppe in das Dialogfeld Gruppe erstellen ein. Informationen zur Benutzeroberfläche finden Sie unter "Dialogfeld "Gruppe erstellen" auf Seite 339.

3. Berechtigungen zu Gruppen zuweisen

BSM bietet Ihnen die Möglichkeit, Berechtigungen für Gruppen und Benutzer auf bestimmte

Ressourcen und Instanzen der im System definierten Ressourcen anzuwenden. Details zu Aufgaben finden Sie unter "Zuweisen von Berechtigungen" auf Seite 266.

4. Benutzer erstellen

Sie erstellen Benutzer und platzieren diese anschließend in den entsprechenden Gruppen. Informationen zur Benutzeroberfläche finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

5. Konfigurieren der Benutzer- und Gruppenhierarchie

In der Registerkarte **Hierarchie** legen Sie die Benutzer- und Gruppenhierarchie fest, indem Sie Benutzer zu Gruppen hinzufügen und Gruppen in anderen Gruppen verschachteln. Details zu Aufgaben finden Sie unter "Konfigurieren der Gruppen- und Benutzerhierarchie" auf Seite 267.

6. Anpassen der Benutzereinstellungen

In der Registerkarte **Anpassung** passen Sie die Menüelemente an, die in den unterschiedlichen Kontexten für Benutzer angezeigt werden. Details zu Aufgaben finden Sie unter "Anpassen von Benutzermenüs" auf Seite 273.

7. Konfigurieren und Verwalten von Empfängern

Sie erstellen Empfänger, indem Sie eine oder mehrere Benachrichtigungsmethoden, die für Warnungsbenachrichtigungen verwendete Vorlage und einen Benachrichtigungszeitplan für den Empfang von Reports definieren. Sie erstellen Empfänger und verwalten vorhandene Empfänger auf der Seite **Empfänger**. Informationen zur Benutzeroberfläche finden Sie unter "Konfigurieren und Verwalten von Empfängern" auf Seite 359.

Konfigurieren von Benutzern und Berechtigungen – Fallspezifisches Szenario

In diesem fallspezifischen Szenario wird beschrieben, wie Sie Benutzer und Gruppen in der Benutzerverwaltung konfigurieren.

Hinweis: Eine Aufgabe für dieses Szenario finden Sie unter "Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257.

1. Zuordnen von Benutzern und Gruppen

Jane Smith ist Systemadministrator in der Firma NewSoft und möchte sowohl Benutzer und Gruppen, die auf BSM zugreifen, als auch Endbenutzer konfigurieren, die auf Service Health und Reports zugreifen sollen. Vorher benötigt sie die folgenden Informationen von den entsprechenden Mitarbeitern:

- Benutzernamen
- Anmeldenamen
- Anfangskennwörter
- Benutzerzeitzonen
- Kontaktinformationen (z. B. Telefonnummer, Pager, E-Mail-Adresse)

Hinweis: Kontaktinformationen sind nur für HP Software-as-a-Service-Kunden erforderlich.

Mithilfe dieser Informationen kann Sie dann eine Gruppe erstellen, die die Berechtigungsebene für die Systemmodifikation erhält, und eine andere Gruppe, die die Berechtigungsebene für die Systemanzeige erhält. Darüber hinaus wird einem Benutzer die Rolle des SiteScope-Administrators zugewiesen.

2. Erstellen von Gruppen

Jane gruppiert die Benutzer entsprechend der Berechtigungsebene, die ihnen zugewiesen werden soll. Sie klickt im Ausschnitt **Gruppen/Benutzer** auf die Schaltfläche zum Erstellen von neuen Gruppen/neuen Benutzern und erstellt anschließend die folgenden Gruppen:

- Systemanzeige
- Systemmodifikation

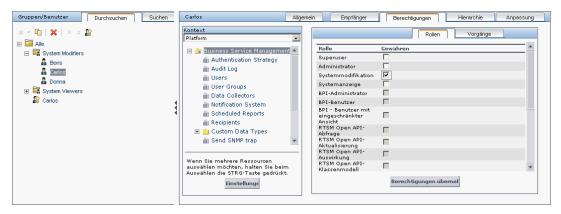
Der Ausschnitt Gruppen/Benutzer wird wie folgt angezeigt:



3. Zuweisen von Berechtigungen zu Gruppen

Nach dem Erstellen der Gruppen weist Jane ihnen die entsprechenden Berechtigungsebenen zu. Zunächst wählt Sie Systemmodifikation im Ausschnitt Gruppen/Benutzer aus, navigiert zur Registerkarte Berechtigungen im Ausschnitt mit den Informationen und wählt die Stamminstanz (Business Service Management) des jeweiligen Kontextes aus. Auf der der Registerkarte Rollen wählt sie Systemmodifikation aus und klickt anschießend auf Berechtigungen übernehmen. Anschließend wählt Sie Systemanzeige im Ausschnitt Gruppen/Benutzer aus. Sie wählt Systemanzeige auf der Registerkarte Rollen aus und klickt dann auf Berechtigungen übernehmen.

Die Ergebnisse werden auf der Registerkarte Berechtigungen wie folgt angezeigt:



4. Erstellen von Benutzern

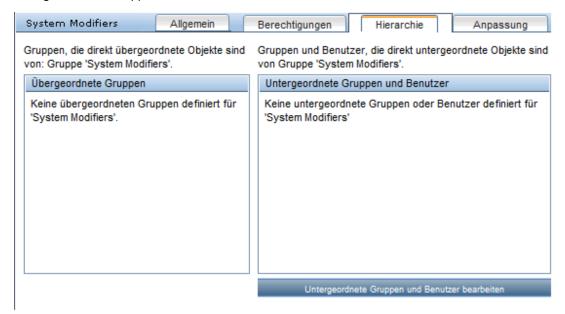
Jane muss nun Benutzer erstellen, die in den Gruppen gemäß den gewünschten Berechtigungsebenen der einzelnen Benutzer verschachtelt werden. Sie klickt auf die Schaltfläche zum Erstellen von neuen Gruppen/neuen Benutzerm im Ausschnitt Gruppen/Benutzer. Für die Stammgruppe (Alle) wählt sie Benutzer erstellen aus und legt für jeden neuen Benutzer die Einstellungen fest. Der Ausschnitt Gruppen/Benutzer wird wie folgt angezeigt:



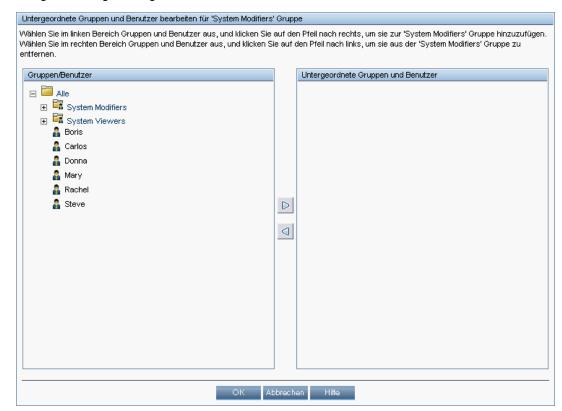
5. Konfigurieren der Benutzer- und Gruppenhierarchie

Nachdem Jane die Benutzer mit der Berechtigung für den Zugriff auf BSM erstellt hat, weist sie ihnen Berechtigungsebenen zu, indem sie die Benutzer innerhalb der jeweiligen Gruppe verschachtelt.

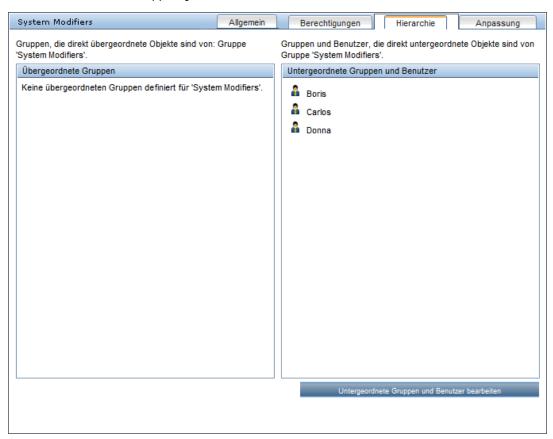
Sie wählt die Gruppe **Systemmodifikation** aus dem Ausschnitt **Gruppen/Benutzer** aus, um die jeweiligen Benutzer in dieser Gruppe zu verschachteln. Jane wählt anschließend die Registerkarte **Hierarchie** aus dem Ausschnitt mit den Informationen rechts auf der Seite aus. Die Registerkarte **Hierarchie** zeigt wie folgt an, dass die Gruppe **Systemmodifikation** keine untergeordneten Gruppen aufweist:



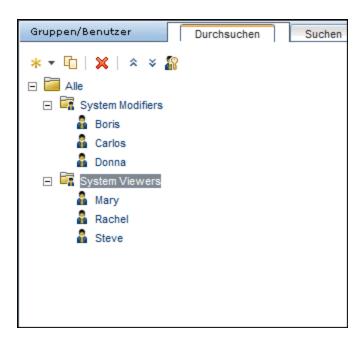
Jane klickt auf die Schaltfläche **Untergeordnete Gruppen und Benutzer bearbeiten**, um das gleichnamige Dialogfeld zu öffnen:



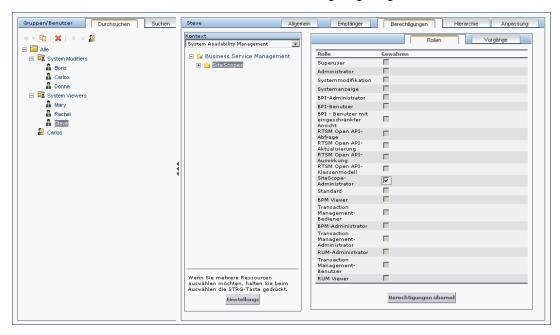
Anschließend wählt Sie die gewünschten Benutzer aus dem Ausschnitt **Gruppen/Benutzer** aus und klickt auf den Rechtspfeil, um sie in den Ausschnitt **Untergeordnete Gruppen und Benutzer** zu verschieben. Auf der Registerkarte **Hierarchie** wird wie folgt angezeigt, dass diese Benutzer in der Gruppe **Systemmodifikation** verschachtelt sind:



Nachdem die jeweiligen Benutzer mithilfe desselben Verfahrens in der Gruppe **Systemanzeige** verschachtelt wurden, wird der Ausschnitt **Gruppen/Benutzer** wie folgt angezeigt:



Da Steve die hinzugefügte Berechtigungsebene SiteScope-Administrator zugewiesen wurde, wählt Jane den Benutzernamen des Benutzers im Ausschnitt **Gruppen/Benutzer** aus, dem die hinzugefügte Berechtigungsebene SiteScope-Administrator zugewiesen werden soll, und auf der Registerkarte **Berechtigungen** wählt sie den Kontext **System Availability**Management aus. Nach dem Auswählen einer Ressource wählt sie **SiteScope-Administrator** auf der Registerkarte **Rollen** aus und klickt auf **Berechtigungen**übernehmen. Anschließend wird der Bildschirm wie folgt angezeigt:



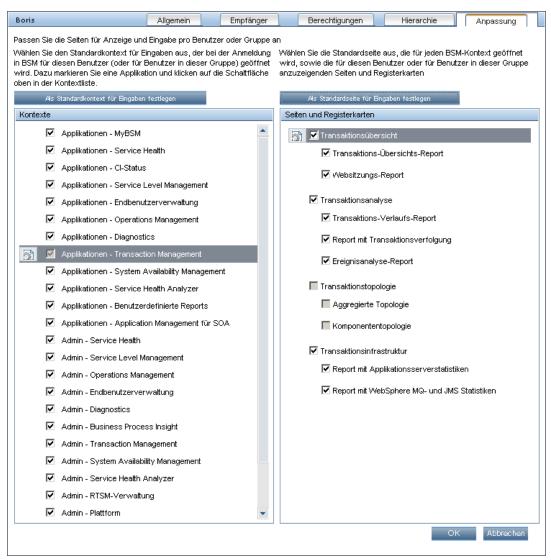
6. Anpassen der Benutzereinstellungen

Jane legt nun die Seite fest, die Benutzern beim Aufrufen von BSM angezeigt wird. Sie wählt außerdem die Menüelemente aus, die auf den Seiten von BSM zur Verfügung stehen. Nach dem Auswählen der einzelnen Benutzer klickt sie auf die Registerkarte **Anpassung** und legt

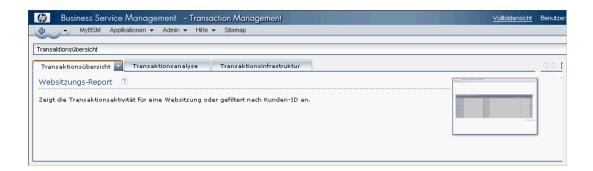
die folgenden Parameter fest:

- Den Eingangskontext, der angezeigt wird, wenn sich Benutzer bei BSM anmelden.
 Beispielsweise Admin End User Management.
- Die Seite innerhalb des Eingangskontextes, die dem Benutzer im Rahmen des ausgewählten Kontextes angezeigt wird. Beispielsweise Reports.
- Die Seiten und Registerkarten, die auf jeder BSM-Seite durch Aktivieren oder Deaktivieren der jeweiligen Kontrollkästchen angezeigt werden. So werden beispielsweise die Kontrollkästchen für die Seiten Transaktionstopologie und Vom Benutzer erstellte Reports deaktiviert, damit sie nicht bei der Benutzeranmeldung im Kontext Applikationen Transaction Management angezeigt werden.

Die konfigurierten Einstellungen werden auf der Registerkarte **Anpassung** wie folgt angezeigt:



Die folgende Anmeldeseite wird dem Benutzer gemäß den angepassten Einstellungen angezeigt:



Zuweisen von Berechtigungen

In dieser Aufgabe wird beschrieben, wie Sie die Benutzer- und Gruppenberechtigungen in der Benutzerverwaltung konfigurieren. Damit die angewendeten Berechtigungen wirksam werden, muss der Benutzer, für den die Berechtigungen gewährt oder entfernt wurden, sich bei BSM ab- und wieder anmelden.

1. Voraussetzungen

Stellen Sie sicher, dass in Ihrem System Gruppen und Benutzer konfiguriert sind. Informationen zur Benutzeroberfläche finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

2. Auswählen einer Gruppe oder eines Benutzers

Klicken Sie auf eine Gruppe oder einen Benutzer im Ausschnitt **Gruppen/Benutzer** links auf der Seite.

3. Auswählen eines Kontexts

Wählen Sie einen Kontext aus dem Listenfeld **Kontext** über der Ressourcenstruktur in der Mitte der Seite. Weitere Informationen zu den verfügbaren Kontexten finden Sie unter "Ausschnitt "Ressourcenstruktur" auf Seite 347.

4. Zuweisen einer Rolle

Berechtigungen werden mithilfe von Rollen zugewiesen. Sie weisen der ausgewählten Gruppe oder dem ausgewählten Benutzer auf der Registerkarte **Rollen** rechts auf der Seite eine Rolle zu. Weitere Informationen zu den verfügbaren Rollen finden Sie unter "Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung" auf Seite 280.

5. Zuweisen von Operationen – optional

Optional können Sie auf der Registerkarte **Operationen** einzelne Operationen zuweisen, die die Gruppe oder der Benutzer in BSM durchführen kann. Weitere Informationen zu den verfügbaren Operationen finden Sie unter "Operationen für die Benutzerverwaltung" auf Seite 314.

6. Konfigurieren von Berechtigungseinstellungen – optional

Klicken Sie optional unten in der Ressourcenstruktur auf **Einstellungen**. Das Dialogfeld **Berechtigungseinstellungen übernehmen** wird geöffnet, und Sie können die Einstellungen für die aktuelle Sitzung konfigurieren. Informationen zur Benutzeroberfläche finden Sie im Abschnitt "Ausschnitt "Ressourcenstruktur" auf Seite 347.

Konfigurieren der Gruppen- und Benutzerhierarchie

In dieser Aufgabe wird beschrieben, wie Sie die Benutzer- und Gruppenhierarchie konfigurieren. Informationen zur Benutzeroberfläche der Registerkarte **Hierarchie** finden Sie unter "Registerkarte "Hierarchie" (Benutzerverwaltung)" auf Seite 344.

1. Voraussetzungen

Stellen Sie sicher, dass Sie mindestens eine Gruppe und einen Benutzer im Abschnitt **Gruppen/Benutzer** konfiguriert haben. Informationen zur Benutzeroberfläche finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

2. Anzeigen der Gruppen- und Benutzerhierarchie

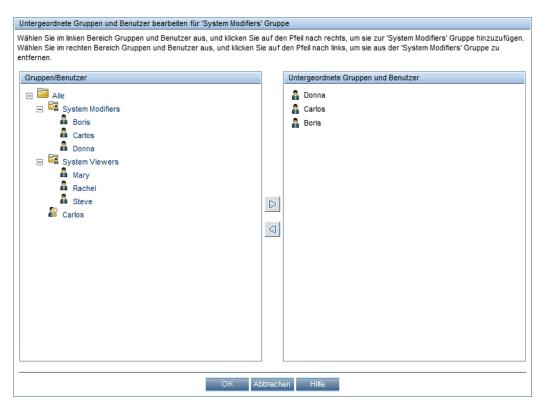
Wählen Sie eine Gruppe oder einen Benutzer im Ausschnitt **Gruppen/Benutzer** aus und wählen Sie die Registerkarte **Hierarchie** rechts auf der Seite aus, um die über- und untergeordneten Gruppen der Gruppen oder Benutzer anzuzeigen, sofern vorhanden.

3. Verschachteln von Gruppen und Benutzern

Wählen Sie eine Gruppe im Ausschnitt **Gruppen/Benutzer** und anschließend die Gruppen und Benutzer aus, die darunter verschachtelt werden sollen.

- a. Klicken Sie auf eine Gruppe oder einen Benutzer auf der Registerkarte **Durchsuchen** des Ausschnitts **Gruppen/Benutzer** auf der linken Seite des Bildschirms.
- b. Klicken Sie rechts auf dem Bildschirm auf die Registerkarte Hierarchie.
- c. Wählen Sie auf der Registerkarte Gruppen/Benutzer die Gruppe aus, die Sie verwalten möchten, und klicken Sie dann auf die Schaltfläche Untergeordnete Gruppen und Benutzer bearbeiten. Das Fenster Untergeordnete Gruppen und Benutzer bearbeiten wird geöffnet.

Im Folgenden sehen Sie das Fenster Untergeordnete Gruppen und Benutzer bearbeiten:

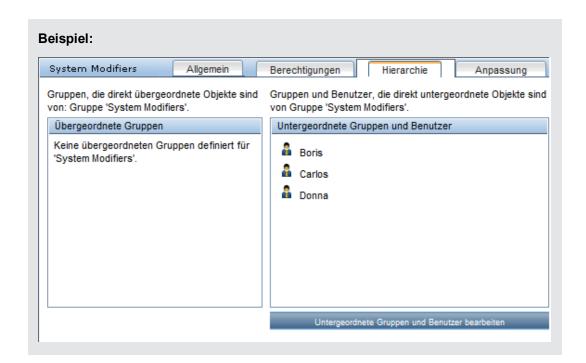


d. Weisen Sie Benutzer zu und verschachteln Sie Gruppen, indem Sie die Benutzer oder Gruppen im Ausschnitt Gruppen/Benutzer auswählen und auf den Links-Nach-Rechts-Pfeil klicken, um sie in den Ausschnitt Untergeordnete Gruppen und Benutzer zu ziehen.

Lösen Sie die Zuweisung zu Benutzern auf und entfernen Sie verschachtelte Gruppen, indem Sie die Gruppen oder Benutzer im Ausschnitt **Untergeordnete Gruppen und Benutzer** auswählen und auf den Rechts-Nach-Links-Pfeil klicken.

4. Ergebnisse

Die verschachtelten Gruppen und Benutzer werden im Ausschnitt **Untergeordnete Gruppen und Benutzer** auf der Registerkarte **Hierarchie** angezeigt.



Entfernen des Status "Sicherheits-Officer" über die JMX-Konsole

In dieser Aufgabe wird beschrieben, wie Sie den Status "Sicherheits-Officer" für einen Benutzer mithilfe der JMX-Konsole entfernen. Dies kann notwendig werden, wenn der "Sicherheits-Officer" unerwarteterweise den Status nicht selbst entfernen kann. Nachdem der "Sicherheits-Officer" einmal festgelegt wurde, kann kein anderer Benutzer diese Änderung in der Oberfläche für die Benutzerverwaltung vornehmen. Weitere Informationen zu diesem Thema finden Sie unter "Sicherheits-Officer" auf Seite 252.

So entfernen Sie einen Sicherheits-Officer:

- Geben Sie die URL der JMX-Konsole (http://<Name des Gateway- oder Datenverarbeitungsservers>:8080/jmx-console/) in einem Webbrowser ein.
- 2. Geben Sie Anmeldeinformationen für die JMX-Konsole ein. Wenn Sie diese nicht kennen, wenden Sie sich an Ihren Systemadministrator.
- Suchen Sie folgende Einträge:
 - Domänenname: Foundations
 - Service: Infrastructure Settings Manager
 - Einstellung: setCustomerSettingDefaultValue
- 4. Ändern Sie die Parameterwerte wie folgt:
 - Kontextname: Geben Sie security ein.
 - Einstellungsname: Geben Sie secured.user.login.name ein.
 - Neuer Wert: Lassen Sie dies leer.
- 5. Klicken Sie auf Aufrufen.

Exportieren und Importieren von Benutzerinformationen mit der JMX-Konsole

In dieser Aufgabe wird beschrieben, wie Sie in der JMX-Konsole Informationen zu Benutzern, Rollen und Berechtigungen von einem Quellsystem auf ein Zielsystem kopieren können. Beispielsweise kann es erforderlich sein, Benutzerinformationen aus einer vorhandenen Datenbank zu kopieren, wenn Sie eine neue BSM-Datenbank konfigurieren müssen.

Festlegen der zu exportierenden Kontexte

Sie können die Kontexte einschränken, die in den Export einbezogen werden. Eine Liste der verfügbaren Kontexte können Sie in der JMX-Konsole anzeigen:

- Geben Sie in einem Browser folgende URL ein: http://<QUELL-Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Topaz%3Aservice%3DAuthorization+Service
- 2. Geben Sie den Benutzernamen und das Kennwort für die JMX-Konsole ein.
- Klicken Sie auf der Seite JMX MBean View unterhalb von java.util.Set listAuthorizationContexts() auf die Schaltfläche Invoke. In der JMX-Konsole werden alle Kontexte in der TAS angezeigt.

So können Sie die im Export enthaltenen Kontexte einschränken:

- Öffnen Sie auf dem Quellserver die Datei HPBSM\conf\tas\exportedContexts.properties.
- Ändern Sie die Eigenschaft contexts-to-export.
 Kontexte in der Eigenschaft contexts-to-export müssen ohne Leerschritte durch Kommas getrennt werden.
- 3. Speichern Sie die Änderungen.

Exportieren

Verwenden Sie die JMX-Konsole, um eine ZIP-Datei mit XML-Dateien mit Informationen zu Benutzern, Rollen und Berechtigungen zu erstellen.

- Geben Sie in einem Browser folgende URL ein: http://<QUELL-Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export
- Klicken Sie auf der Seite JMX MBean View unter void loadExportedContexts() auf die Schaltfläche Invoke, und klicken Sie dann im Browser auf die Schaltfläche Zurück, um zur Seite JMX MBean View zurückzukehren.
- 3. Geben Sie unter **void exportAllTasEntities()** im Feld **ParamValue** einen Speicherort und einen Dateinamen für die Exportdatei auf dem Quellserver ein. Der Dateiname muss die Erweiterung ZIP aufweisen, z. B.: **C:\HPBSM\export.zip**
- 4. Klicken Sie unter void exportAllTasEntities() auf die Schaltfläche Invoke.

Übertragen

Sie müssen die Datei **export.zip** vom Quellserver auf den Zielserver kopieren.

- 1. Navigieren Sie auf dem Quellserver zu der Exportdatei, wie oben beschrieben.
- 2. Kopieren Sie die Datei auf den Zielserver.

Importieren

Importieren Sie die Benutzer, Rollen und Berechtigungen aus der ZIP-Datei auf das BSM-Zielsystem.

Achtung: Stellen Sie vor dem Importieren von Benutzer- und Gruppeninformationen sicher, dass der Zielserver keine erstellten Ressourcen, z. B. Reports, Profile und Monitore, mit Benutzerinformationen aufweist, die nicht mit den Informationen kompatibel sind, die Sie importieren möchten.

- Geben Sie in einem Browser folgende URL ein: http://<ZIEL-Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export
- 2. Geben Sie den Benutzernamen und das Kennwort für die JMX-Konsole ein.
- 3. Geben Sie unter **void importAllTasEntities()** im Feld **ParamValue** den Speicherort und den Dateinamen der Exportdatei ein, und klicken Sie dann auf die Schaltfläche **Invoke**.

Anpassen von Benutzermenüs

In dieser Aufgabe wird beschrieben, wie die Standardseite angepasst wird, die Benutzern beim Anmelden bei BSM angezeigt wird, und wie die Menüelemente ausgewählt werden, die auf den Seiten des Systems zur Verfügung stehen sollen.

Tipp: Ein fallspezifisches Szenario für diese Aufgabe finden Sie unter "Anpassen von Benutzermenüs – Fallspezifisches Szenario" auf Seite 275.

Sie können den Zugriff auf Funktionen einschränken oder Standardseiten für einzelne Benutzer oder für alle Benutzer in einer Gruppe festlegen, einschließlich aller Mitglieder in Untergruppen, die zu einer übergeordneten Gruppe gehören. Wenn Sie den Zugriff auf eine Funktion oder einen Report für eine Gruppe einschränken, kann kein Mitglied dieser Gruppe auf die Funktion zugreifen, und Sie können die Einstellung für einzelne Benutzer nicht außer Kraft setzen.

Wenn Sie einer Gruppe, für die Gruppeneinstellungen gelten, Benutzer oder Untergruppen hinzufügen, erhalten die Benutzer oder Mitglieder der Untergruppen automatisch die Zugriffseinschränkungen, die auf die Gruppe angewendet wurden.

1. Voraussetzungen

Stellen Sie sicher, dass Sie mindestens einen Benutzer im Abschnitt **Gruppen/Benutzer** konfiguriert haben. Informationen zur Benutzeroberfläche finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

2. Auswählen eines Benutzers

Wählen Sie im Ausschnitt **Gruppen/Benutzer** auf der Registerkarte **Durchsuchen** einen Benutzer bzw. eine Gruppe aus, dessen bzw. deren Seiten und Menüelemente angepasst werden sollen, und wählen Sie die Registerkarte **Anpassung** aus.

3. Zuweisen eines Standardkontextes

Wählen Sie im Ausschnitt **Kontexte** einen Kontext aus, der als standardmäßiger Eingangskontext angezeigt werden soll, wenn sich dieser Benutzer oder alle Benutzer in einer Gruppe bei BSM anmeldet bzw. anmelden, und klicken Sie auf **Als standardmäßigen Eingangskontext festlegen**. Informationen zur Benutzeroberfläche finden Sie unter "Registerkarte "Anpassung" (Benutzerverwaltung)" auf Seite 340.

4. Auswählen von Kontexten und Applikationen, die ein-/ausgeblendet werden sollen

Deaktivieren Sie im Ausschnitt **Kontexte** die Kontrollkästchen der Kontexte und Applikationen, die für den Benutzer bzw. alle Mitglieder der Gruppe nicht sichtbar sein sollen. Standardmäßig sind alle Kontexte und Applikationen ausgewählt.

5. Auswählen von Kontextseiten und Registerkarten

Aktivieren Sie im Ausschnitt **Seiten und Registerkarten** die Kontrollkästchen der Seiten und Registerkarten, die im ausgewählten Kontext für den Benutzer bzw. die Gruppe sichtbar sein sollen. Deaktivieren Sie die Kontrollkästchen der Seiten und Registerkarten, die für den Benutzer bzw. die Gruppe nicht sichtbar sein sollen.

Hinweis: Für die Applikationen Service Health und Operations Management können Sie keinen Benutzerzugriff für spezifische Seiten definieren, Sie können hier nur den Benutzerzugriff auf Applikationsebene aktivieren oder deaktivieren.

6. Zuweisen einer standardmäßigen Eingangsseite

Wählen Sie eine Seite oder Registerkarte aus, die als standardmäßige Eingangsseite für den ausgewählten Kontext verwendet werden soll, und klicken Sie auf **Als standardmäßige Eingangsseite festlegen**.

7. Ergebnisse

Die Schaltfläche **Standard für Eingang** wird neben dem standardmäßigen Eingangskontext bzw. der standardmäßigen Eingangsseite angezeigt. Die für den Benutzer sichtbaren Applikationen und Kontexte sind im Ausschnitt **Kontexte** angezeigt. Die für den Benutzer sichtbaren Seiten und Registerkarten sind im Ausschnitt **Seiten und Registerkarten** ausgewählt.

Anpassen von Benutzermenüs – Fallspezifisches Szenario

In diesem fallspezifischen Szenario wird beschrieben, wie Sie Benutzermenüs für einzelne Benutzer anpassen.

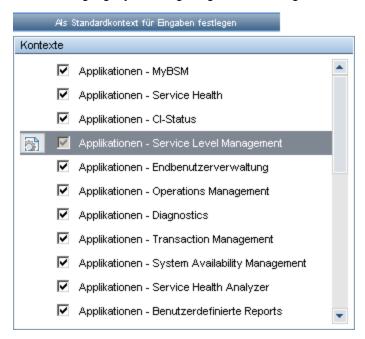
Hinweis: Eine Aufgabe für dieses Szenario finden Sie unter "Anpassen von Benutzermenüs" auf Seite 273.

1. Auswählen eines Benutzers

Marie, die Administratorin des Versicherungsunternehmens ABC, erstellt im Abschnitt **Benutzerverwaltung** von BSM mehrere Benutzer. Sie entscheidet, dass der Benutzer Karl Müller in BSM nur bestimmte Seiten und Registerkarten anzeigen darf und dass eine bestimmte Seite auf seinem Bildschirm angezeigt wird, wenn er sich bei BSM anmeldet.

2. Zuweisen eines Standardkontextes

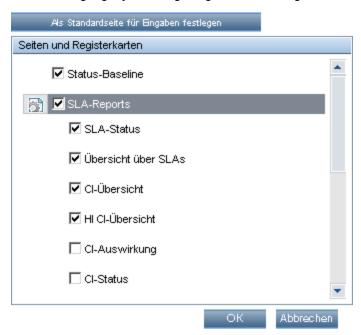
Da Karls vorwiegende Verantwortung bei ABC das Service Level Management ist, legt Marie die Seite Applikationen – Service Level Management als Standardeingangskontext fest. Marie wählt Applikationen - Service Level Management im Bereich Kontexte aus und klickt auf Als standardmäßigen Eingangskontext festlegen. Der Kontext Applikationen - Service Level Management wird als Standardeingangskontext mit dem Standardeingangssymbol angezeigt wie in der folgenden Abbildung dargestellt:



3. Auswählen von Kontextseiten und Registerkarten

Da Karl nicht berechtigt ist, Ausfall-Reports anzuzeigen, ist diese Option im Bereich **Seiten und Registerkarten** deaktiviert. Die Optionen für die verbleibenden Seiten und Registerkarten bleiben aktiviert, sodass diese angezeigt werden, wenn Karl sich bei BSM anmeldet. Da SLA-

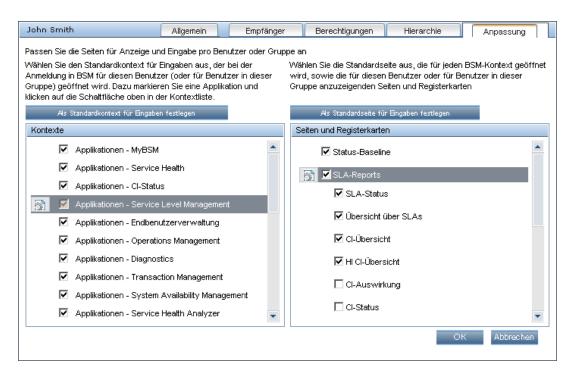
Reports für das Versicherungsunternehmen ABC höchste Priorität besitzen, legt Marie fest, dass diese Seite zuerst angezeigt wird, wenn Karl sich anmeldet. Sie wählt **SLA-Reports** im Bereich **Seiten und Registerkarten** aus und klickt anschließend auf **Als standardmäßige Eingangsseite festlegen**. **SLA-Reports** wird als Standardeingangskontext mit dem Standardeingangssymbol angezeigt, wie in der folgenden Abbildung dargestellt:



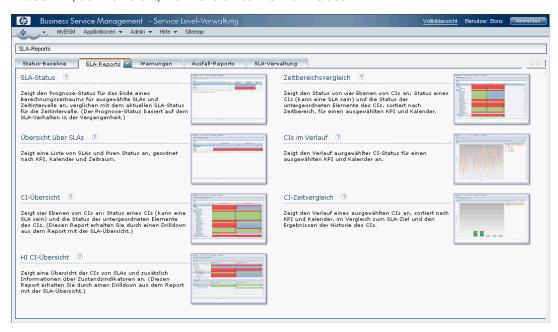
4. Ergebnisse

Der Kontext, der geöffnet wird, wenn Karl Müller sich bei BSM anmeldet, ist der Kontext **Service Level Management** im Menü **Applikationen**. Die Seite **SLA-Reports** wird geöffnet und Karl kann auch auf die Seiten **Status-Baseline**, **Warnungen** und **SLA-Verwaltung** zugreifen.

Die konfigurierte Registerkarte **Anpassung** in der Benutzerverwaltung wird wie folgt angezeigt:



Bildschirm, den Karl sieht, wenn er sich bei BSM anmeldet:



Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS

Wenn Ihr Anbieter in der Liste der Standardanbieter nicht aufgeführt ist und der Anbieter ein E-Mail-Gateway verwendet, können Sie Ihren Anbieter manuell zu BSM hinzufügen. Anschließend wird der Anbieter in der Liste aufgeführt.

Um einen Anbieter hinzuzufügen, der ein E-Mail-Gateway verwendet, geben Sie die Gateway-Informationen manuell in die Verwaltungsdatenbank ein. Wenden Sie sich an den Datenbankadministrator, wenn Sie Hilfe benötigen.

So fügen Sie einen Anbieter hinzu, der ein E-Mail-Gateway verwendet:

- 1. Öffnen Sie die Tabelle **NOTIFICATION_PROVIDERS** in der Verwaltungsdatenbank.
- Fügen Sie in der Spalte NP_NOTIFICATION_PROVIDER_NAME den Namen des Anbieters unten in der Liste ein.

Fügen Sie den Namen genau so hinzu, wie er in der Anbieterliste angezeigt werden soll, die in der Registerkarte **SMS** des Assistenten für die Empfängereigenschaften geöffnet wird. Weitere Informationen finden Sie unter "Registerkarte "SMS" auf Seite 372.

Beachten Sie die ID-Nummer, die dem Anbieter automatisch zugewiesen wird.

- Schließen Sie die Tabelle NOTIFICATION_PROVIDERS und öffnen Sie die Tabelle NOTIFPROVIDER_NOTIFTYPE.
- 4. Fügen Sie in der Spalte **NN_NOTIF_PROVIDER_ID** die ID-Nummer hinzu, die dem neuen Anbieter zugewiesen wurde.
- 5. Fügen Sie dem Anbieter in der Spalte **NN_NOTIF_TYPE_ID** einen der folgenden Benachrichtigungstypen hinzu:
 - 102 für Pager-Dienstanbieter
 - 101 für SMS-Dienstanbieter
- 6. Schließen Sie die Tabelle **NOTIFPROVIDER_NOTIFTYPE** und öffnen Sie die Tabelle **NOTIFICATION_PROVIDER_PROP**.
- 7. Fügen Sie in der Spalte **NPP_NOTIFICATION_PROVIDER_ID** die ID-Nummer hinzu, die dem neuen Anbieter zugewiesen wurde.
 - Achten Sie darauf, dass Sie die ID-Nummer in zwei aufeinanderfolgenden Zeilen hinzufügen.
- Fügen Sie in den Spalten NPP_NPROVIDER_PROP_NAME und NPP_NPROVIDER_ PROP_VALUE die folgenden neuen Eigenschaftsnamen und -werte für den Anbieter untereinander hinzu (Beispiele finden Sie in den bestehenden Einträgen):

Eigenschaftenname	Eigenschaftenwert	Beschreibung
EMAIL_SUFFIX	<e_mail_suffix></e_mail_suffix>	Das E-Mail-Suffix des Gateways. Wenn die E-Mail-Adresse des Gateways beispielsweise 12345@beispiel.com lautet, geben Sie beispiel.com als Eigenschaftenwert für EMAIL_SUFFIX an.
EMAIL_MAX_LEN	<max_länge></max_länge>	Die maximale Textlänge der E-Mail-Nachricht in Zeichen. Beispiel: 500.
		Wenn Sie diesen Wert festlegen, beachten Sie die maximale Länge, die durch den Dienstanbieter limitiert wird, sowie die Vorgaben Ihres Pagers oder Mobiltelefons.

- 9. Geben Sie in der Spalte NPP_NPROVIDER_PROP_DATATYPE_ID wie folgt einen ID-Wert an:
 - Für EMAIL_SUFFIX: 1
 - Für EMAIL_MAX_LEN: 2
- 10. Starten Sie BSM erneut.

Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung

Die folgenden Rollen können auf alle Kontexte in BSM angewendet werden. Details zu den Ressourcen, auf die Rollen angewendet werden können, finden Sie im Folgenden in der Beschreibung der einzelnen Rollen.

Details zu Rollen, die nur auf bestimmte Kontexte angewendet werden können, finden Sie unter "Rollen in der Benutzerverwaltung für verschiedene Kontexte" auf Seite 310.

Superuser

Die Rolle **Superuser** kann nur der Ressource **Business Service Management** zugewiesen werden.

Diese Rolle umfasst alle verfügbaren Operationen für alle Ressourcen in allen Kontexten. Nur ein Superuser kann einem anderen Benutzer die Rolle **Superuser** zuweisen.

Achtung: Der Standard-Superuser hat keine Berechtigungen zum Schreiben in Business Service Management aus der UCMDB WS-API. Für diesen Zweck gibt es spezifische Rollen. Details finden Sie unter "Rollen in der Benutzerverwaltung für verschiedene Kontexte" auf Seite 310 und "Rollen in der Benutzerverwaltung für verschiedene Kontexte" auf Seite 310.

Administrator

Die Rolle **Administrator** kann nur der Ressource **Business Service Management** zugewiesen werden.

Ein Administrator verfügt über eine Sammlung von Berechtigungen, die das Hinzufügen von Profilen zum System sowie das Verwalten der zu diesen Profilen gehörenden Ressourcen beinhaltet. Sobald ein Profil hinzugefügt wurde, besitzt der Administrator Berechtigungen für den Vollzugriff auf alle Ressourcen innerhalb dieser Profilinstanz.

Business Process Insight

Ressource	Zulässige Operationen
Business Process Insight-Applikation	Ansicht
Business Process Insight-Verwaltung	Vollzugriff

Diagnostics

Ressource	Zulässige Operationen
Diagnostics	Änderung
	Ansicht
	Ausführen
	Vollzugriff

End User Management

Ressource	Zulässige Operationen
Warnung - Abhängigkeiten erstellen	Änderung
Applikationen	Hinzufügen
	Ansicht
BPM-Agenten	Ansicht
RUM-Engines	Ansicht
Skript-Repository	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

MyBSM

Ressource	Zulässige Operationen
User Pages	Vollzugriff
Predefined Pages	Ansicht
User Components	Vollzugriff

MyBSM (Legacy)

Ressource	Zulässige Operationen
Module	Vollzugriff
Portlet-Definitionen	Vollzugriff

Operations Management

Ressource	Zulässige Operationen
Dem Benutzer zugewiesene Ereignisse	Bearbeiten/Auflösen
	Schließen
	Erneut öffnen
	Zuweisen zu
	Operator-Aktion starten
	Automatische Aktion starten
	Übertragungssteuerung
	Übertragene schließen
	Ereignisbeziehungen hinzufügen/entfernen
	Schweregrad ändern
	Priorität ändern
	Titel ändern
	Beschreibung ändern
	Lösung ändern
	Anmerkungen hinzufügen/löschen/aktualisieren
	Benutzerdefinierte Attribute hinzufügen/löschen/aktualisieren

Ressource	Zulässige Operationen
Dem Benutzer nicht zugewiesene	Ansicht
Ereignisse	Bearbeiten/Auflösen
	Schließen
	Erneut öffnen
	Zuweisen zu
	Operator-Aktion starten
	Automatische Aktion starten
	Übertragungssteuerung
	Übertragene schließen
	Ereignisbeziehungen hinzufügen/entfernen
	Schweregrad ändern
	Priorität ändern
	Titel ändern
	Beschreibung ändern
	Lösung ändern
	Anmerkungen hinzufügen/löschen/aktualisieren
	Benutzerdefinierte Attribute hinzufügen/löschen/aktualisieren
Zustandsindikatoren	Zurücksetzen
Verwaltungsbenutzeroberflächen	Ansicht
Werkzeugkategorien	Ausführen

Operations Orchestration-Integration

Ressource	Zulässige Operationen
Verwaltung	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
Ausführung	Ausführen
	Vollzugriff

Platform

Ressource	Zulässige Operationen
Audit Log	Ansicht
	Vollzugriff
Users	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
User Groups	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Data Collectors	Änderung
	Ansicht
Scheduled Reports	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
Recipients	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Custom Data Types	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Downtime	Ansicht
	Vollzugriff
Databases	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

RTSM

Ressource	Zulässige Operationen
Ansichten	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
RTSM	Vollzugriff
CI-Suche	Vollzugriff
Datenmodifizierung	Vollzugriff

Ressource	Zulässige Operationen
Zugehörige CIs abrufen	Vollzugriff
ITU Manager	Vollzugriff
Modeling Studio	Vollzugriff

Service Health Analyzer

Ressource	Zulässige Operationen
Verwaltung	Vollzugriff
Applikation	Vollzugriff

Service Level Management

Ressource	Zulässige Operationen
SLAs	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Bedarfsgesteuerte SiteScope-Monitore

Ressource	Zulässige Operationen
Verwaltung	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Ausführung	Ausführen
	Vollzugriff

System Availability Management

Ressource	Zulässige Operationen
SiteScopes	Hinzufügen

Transaction Management

Ressource	Zulässige Operationen
TransactionVision-Verarbeitungsserver	Änderung
	Vollzugriff
TransactionVision-Analyzer	Änderung
	Ausführen
	Vollzugriff
TransactionVision-Job-Manager	Änderung
	Ausführen
	Vollzugriff
TransactionVision-Abfrage-Engines	Änderung
	Ausführen
	Vollzugriff
Verwaltung	Änderung
	Vollzugriff
Benutzerdaten	Ansicht
	Vollzugriff
Applikationen	Hinzufügen

Benutzerdefinierte Reports

Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff
Trend-Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff

Ressource	Zulässige Operationen
Benutzerdefinierte Links	Änderung
	Ansicht
	Vollzugriff
Excel-Reports	Änderung
	Ansicht
	Vollzugriff
Standardkopf-/-fußzeile	Änderung
	Vollzugriff
Filter-Favorit	Änderung
	Ansicht
	Löschen
	Vollzugriff
Anmerkung	Änderung
	Löschen
	Vollzugriff
Service-Report	Änderung
	Löschen
	Vollzugriff
Reports für benutzerdefinierte Abfragen	Hinzufügen
	Ansicht
	Vollzugriff

Systemmodifikation

Die Rolle **Systemmodifikation** kann nur der Ressource **Business Service Management** zugewiesen werden.

Ein Benutzer mit dieser Rolle kann alle Ressourcen in BSM anzeigen und ändern. Für einige Ressourcen stehen jedoch keine Anzeige- oder Änderungsoperationen zur Verfügung. Ein Benutzer mit dieser Rolle hat nur Berechtigungen für die Operationen, die in BSM zur Verfügung stehen.

Business Process Insight

Ressource	Zulässige Operationen
Business Process Insight-Applikation	Ansicht
Business Process Insight-Verwaltung	Vollzugriff

Diagnostics

Ressource	Zulässige Operationen
Diagnostics	Änderung
	Ansicht

End User Management

Ressource	Zulässige Operationen
Warnung - Benachrichtigungsvorlage	Änderung
	Ansicht
Warnung - Abhängigkeiten erstellen	Änderung
Applikationen	Änderung
	Ansicht
BPM-Agenten	Ansicht
RUM-Engines	Ansicht
Skript-Repository	Ansicht
	Vollzugriff

MyBSM

Ressource	Zulässige Operationen
Pre-defined Pages	Ansicht
User Pages	Vollzugriff
User Components	Vollzugriff

Operations Orchestration-Integration

Ressource	Zulässige Operationen
Verwaltung	Änderung
	Ansicht

Ressource	Zulässige Operationen
Ausführung	Ausführen

Platform

Ressource	Zulässige Operationen
Audit Log	Ansicht
Users	Änderung
	Ansicht
User Groups	Änderung
	Ansicht
Data Collectors	Änderung
	Ansicht
Scheduled Reports	Änderung
	Ansicht
Recipients	Änderung
	Ansicht
Custom Data Types	Änderung
	Ansicht
Send SNMP trap	Änderung
Run executable file	Änderung
Log to Event Viewer	Änderung
Downtime	Vollzugriff
Databases	Änderung
	Ansicht
System Recipient Template	Änderung
	Ansicht

RTSM

Ressource	Zulässige Operationen
Ansichten	Änderung
	Ansicht
CI-Suche	Vollzugriff
Zugehörige CIs abrufen	Vollzugriff
ITU Manager	Vollzugriff
Modeling Studio	Vollzugriff

Service Health Analyzer

Ressource	Zulässige Operationen
Verwaltung	Vollzugriff
Applikation	Vollzugriff

Service Level Management

Ressource	Zulässige Operationen
SLAs	Änderung
	Ansicht

Bedarfsgesteuerte SiteScope-Monitore

Ressource	Zulässige Operationen
Verwaltung	Änderung
	Ansicht
Ausführung	Ausführen

System Availability Management

Ressource	Zulässige Operationen
SiteScopes	Änderung
	Ansicht

Transaction Management

Ressource	Zulässige Operationen
TransactionVision-Verarbeitungsserver	Änderung
TransactionVision-Analyzer	Änderung
	Ausführen
TransactionVision-Job-Manager	Änderung
	Ausführen
TransactionVision-Abfrage-Engines	Änderung
	Ausführen
Verwaltung	Änderung
Applikationen	Änderung
	Ansicht

Benutzerdefinierte Reports

Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Hinzufügen
	Änderung
	Ansicht
Trend-Reports	Hinzufügen
	Änderung
	Ansicht
Benutzerdefinierte Links	Änderung
	Ansicht
Excel-Reports	Änderung
	Ansicht
Standardkopf/-fußzeile	Änderung
Filter-Favorit	Änderung
	Ansicht
	Löschen

Ressource	Zulässige Operationen
Anmerkung	Änderung
	Löschen
Service-Report	Änderung
	Löschen
Reports für benutzerdefinierte Abfragen	Hinzufügen
	Ansicht

Systemanzeige

Die Rolle **Systemanzeige** kann nur der Ressource **Business Service Management** zugewiesen werden.

Ein Systemanzeige-Benutzer kann nur Ressourcen in BSM anzeigen und hat keine Berechtigungen zum Ändern, Hinzufügen oder Löschen von Ressourcen oder Ressourceninstanzen mit Ausnahme der RUM-Engines-Ressource. Bei einigen Ressourcen steht die Anzeigeoperation nicht zur Verfügung. Systemanzeige-Benutzer haben keinen Zugriff auf diese Ressourcen.

Business Process Insight

Ressource	Zulässige Operationen
Business Process Insight-Applikation	Ansicht

Diagnostics

Ressource	Zulässige Operationen
Diagnostics	Ansicht

End User Management

Ressource	Zulässige Operationen
Warnung - Benachrichtigungsvorlage	Ansicht
Applikationen	Ansicht
BPM-Agenten	Ansicht
RUM-Engines	Anzeigen, Bearbeiten
Skript-Repository	Ansicht

MyBSM

Ressource	Zulässige Operationen
Predefined Pages	Ansicht

Operations Orchestration-Integration

Ressource	Zulässige Operationen
Administration	Ansicht

Platform

Ressource	Zulässige Operationen
Audit Log	Ansicht
Users	Ansicht
User Groups	Ansicht
Data Collectors	Ansicht
Scheduled Reports	Ansicht
Recipients	Ansicht
Custom Data Types	Ansicht
Downtime	Ansicht
Databases	Ansicht
System Recipient Template	Ansicht

RTSM

Ressource	Zulässige Operationen
Ansichten	Ansicht
CI-Suche	Vollzugriff
Zugehörige CIs abrufen	Vollzugriff
ITU Manager	Vollzugriff
Modeling Studio	Vollzugriff

Service Health Analyzer

Ressource	Zulässige Operationen
Verwaltung	Vollzugriff

Ressource	Zulässige Operationen
Applikation	Vollzugriff

Service Level Management

Ressource	Zulässige Operationen
SLAs	Ansicht

Bedarfsgesteuerte SiteScope-Monitore

Ressource	Zulässige Operationen
Verwaltung	Ansicht

System Availability Management

Ressource	Zulässige Operationen
SiteScopes	Ansicht

Transaction Management

Ressource	Zulässige Operationen
Applikationen	Ansicht

Benutzerdefinierte Reports

Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Hinzufügen
	Ansicht
Trend-Reports	Hinzufügen
	Ansicht
Benutzerdefinierte Links	Ansicht
Excel-Reports	Ansicht
Filter-Favorit	Ansicht
Reports für benutzerdefinierte Abfragen	Hinzufügen
	Ansicht

Kunde - Superuser

Hinweis: Diese Rolle kann nur HP Software-as-a-Service-Kunden zugewiesen werden.

Die Rolle **Kunde - Superuser** kann nur der Ressourceninstanz **Aktiver Kunde** zugewiesen werden. Die Ressourceninstanz **Aktiver Kunde** steht nur HP Software-as-a-Service-Kunden zur Verfügung und stellt die Kundenebene in der Berechtigungsressourcenstruktur dar. Sie ist in allen Kontexten verfügbar und gilt für alle Kontexte (wie die Ressource **Business Service Management**).

Business Process Insight

Ressource	Zulässige Operationen
Business Process Insight-Applikation	Ansicht
Business Process Insight-Verwaltung	Vollzugriff

Diagnostics

Ressource	Zulässige Operationen
Diagnostics	Ansicht
	Ausführen

End User Management

Ressource	Zulässige Operationen
Warnung - Abhängigkeiten erstellen	Änderung
	Vollzugriff
Applikationen	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Ausführen
	Vollzugriff
BPM-Agenten	Ansicht
RUM-Engines	Ansicht

Ressource	Zulässige Operationen
Skript-Repository	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

MyBSM

Ressource	Zulässige Operationen
Predefined Pages	Vollzugriff
User Pages	Vollzugriff
User Components	Vollzugriff

MyBSM (Legacy)

Ressource	Zulässige Operationen
Module	Vollzugriff
Portlet-Definitionen	Vollzugriff

Platform

Ressource	Zulässige Operationen
Audit Log	Ansicht
	Vollzugriff
Users	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
User Groups	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Data Collectors	Änderung
	Ansicht
Central Repository Service	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Ausführen
	Vollzugriff
Notification System	Ansicht
	Ausführen
	Vollzugriff
Package Work Manipulation	Änderung
	Vollzugriff
Scheduled Reports	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
Recipients	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Custom Data Types	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Customer Recipient Template	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Downtime	Ansicht
	Vollzugriff

RTSM

Ressource	Zulässige Operationen
Ansichten	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
RTSM	Vollzugriff
CI-Suche	Vollzugriff
Datenmodifizierung	Vollzugriff

Ressource	Zulässige Operationen
Zugehörige CIs abrufen	Vollzugriff
ITU Manager	Vollzugriff
Modeling Studio	Vollzugriff

Service Health Analyzer

Ressource	Zulässige Operationen
Verwaltung	Vollzugriff
Applikation	Vollzugriff

Service Level Management

Ressource	Zulässige Operationen
SLAs	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

System Availability Management

Ressource	Zulässige Operationen
SiteScopes	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Ausführen
	Vollzugriff

Benutzerdefinierte Reports

Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff
Trend-Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff
Benutzerdefinierte Links	Änderung
	Ansicht
	Vollzugriff
Excel-Reports	Änderung
	Ansicht
	Vollzugriff
Standardkopf/-fußzeile	Änderung
	Vollzugriff
Filter-Favorit	Änderung
	Ansicht
	Löschen
	Vollzugriff
Anmerkung	Änderung
	Löschen
	Vollzugriff
Service-Report	Änderung
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
Reports für benutzerdefinierte Abfragen	Hinzufügen
	Ansicht
	Vollzugriff

Kunde - Administrator

Hinweis: Diese Rolle kann nur HP Software-as-a-Service-Kunden zugewiesen werden.

Die Rolle **Kunde - Administrator** kann nur der Ressourceninstanz **Aktiver Kunde** zugewiesen werden. Die Ressourceninstanz **Aktiver Kunde** steht nur HP Software-as-a-Service-Kunden zur Verfügung und stellt die Kundenebene in der Berechtigungsressourcenstruktur dar. Sie ist in allen Kontexten verfügbar und gilt für alle Kontexte (wie die Ressource **Business Service Management**).

Dem Kundenadministrator wird die vollständige Kontrolle für eine Auswahl von Ressourcen gewährt sowie Berechtigungen zum Anzeigen und/oder Ausführen für andere Ressourcen. Dieser Benutzer kann Profile jedes Typs hinzufügen und verfügt über die vollständige Kontrolle über die erstellten Profile. Dem Benutzer werden jedoch keine Berechtigungen für Profile gewährt, die von anderen Benutzern erstellt wurden, auch wenn diese Profile für den gleichen Kunden gelten. Bei MyBSM-Ressourcen können alle Benutzer mit dieser Rolle Änderungen an Ressourcen vornehmen, die von anderen Benutzern definiert wurden.

Business Process Insight

Ressource	Zulässige Operationen
Business Process Insight-Applikation	Ansicht
Business Process Insight-Verwaltung	Vollzugriff

Diagnostics

Ressource	Zulässige Operationen
Diagnostics	Ansicht
	Ausführen

End User Management

Ressource	Zulässige Operationen
Warnung - Abhängigkeiten erstellen	Änderung
	Vollzugriff

Ressource	Zulässige Operationen
Applikationen	Hinzufügen
	Ansicht
BPM-Agenten	Ansicht
RUM-Engines	Ansicht

MyBSM

Ressource	Zulässige Operationen
Predefined Pages	Ansicht
User Components	Vollzugriff
User Pages	Vollzugriff

MyBSM (Legacy)

Ressource	Zulässige Operationen
Module	Vollzugriff
Portlet-Definitionen	Vollzugriff

Platform

Ressource	Zulässige Operationen
Audit Log	Ansicht
	Vollzugriff
Users	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
User Groups	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Central Repository Service	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Ausführen
	Vollzugriff
Notification System	Ansicht
	Ausführen
	Vollzugriff
Package Work Manipulation	Änderung
	Vollzugriff
Scheduled Reports	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Empfänger	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

Ressource	Zulässige Operationen
Custom Data Types	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Customer Recipient Template	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
Ausfallzeit	Ansicht
	Vollzugriff

RTSM

Ressource	Zulässige Operationen
Ansichten	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff
RTSM	Vollzugriff
CI-Suche	Vollzugriff
Datenmodifizierung	Vollzugriff
Zugehörige CIs abrufen	Vollzugriff
ITU Manager	Vollzugriff
Modeling Studio	Vollzugriff

Service Health Analyzer

Ressource	Zulässige Operationen
Verwaltung	Vollzugriff
Applikation	Vollzugriff

Service Level Management

Ressource	Zulässige Operationen
SLAs	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

System Availability Management

Ressource	Zulässige Operationen
SiteScopes	Hinzufügen

Benutzerdefinierte Reports

Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff
Trend-Reports	Hinzufügen
	Änderung
	Ansicht
	Vollzugriff
Benutzerdefinierte Links	Änderung
	Ansicht
	Vollzugriff

Ressource	Zulässige Operationen
Excel-Reports	Änderung
	Ansicht
	Vollzugriff
Standardkopf/-fußzeile	Änderung
	Vollzugriff
Filter-Favorit	Änderung
	Ansicht
	Löschen
	Vollzugriff
Anmerkung	Änderung
	Löschen
	Vollzugriff
Service-Report	Änderung
	Löschen
	Vollzugriff
Reports für benutzerdefinierte Abfragen	Hinzufügen
	Ansicht
	Vollzugriff

BPM Viewer

Die Rolle **BPM Viewer** kann nur der Ressource **Business Service Management** zugewiesen werden.

Diese Benutzer haben Berechtigungen zum Anzeigen, können jedoch Einstellungen für Transaktionsschwellenwerte sowie Transaktionsbeschreibungen ändern.

Allen regulären Benutzern, die in der früheren Version in einem spezifischen BPM-Profil als Benutzer hinzugefügt wurden, wird die BPM Viewer-Rolle für dieses Profil zugewiesen.

Ressource	Zulässige Operationen	
Applikationen	Ansicht	
BPM-Agenten	Ansicht	
Skript-Repository	Ansicht	

BPM-Administrator

Die Rolle **BPM-Administrator** kann nur der Ressource **Business Service Management** zugewiesen werden.

Der BPM-Administrator kann alle BPM-Profile der Plattform verwalten, einschließlich der Berechtigungen für alle Profile.

Allen Administratoren, die in der früheren Version in einem spezifischen BPM-Profil als Benutzer hinzugefügt wurden, wird die BPM-Profiladministratorrolle für dieses Profil zugewiesen. Hierbei handelt es sich um einen Zusatz zur Administratorrolle, die weiter oben beschrieben wird. (Weitere Informationen finden Sie unter "Administrator" auf Seite 280.)

Ressource	Zulässige Operationen
Applikationen	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Ausführen
	Vollzugriff
BPM-Agenten	Ansicht
Skript-Repository	Hinzufügen
	Änderung
	Ansicht
	Löschen
	Vollzugriff

RUM-Administrator

Die Rolle **RUM-Administrator** kann nur der Ressource **Business Service Management** zugewiesen werden.

Ressource	Zulässige Operationen
Applikationen	Hinzufügen
	Ändern
	Ansicht
	Löschen
	Ausführen
	Vollzugriff
RUM-Engines	Ansicht

RUM Viewer

Die Rolle **RUM Viewer** kann nur der Ressource **Business Service Management** zugewiesen werden.

Diese Benutzer haben Berechtigungen zum Anzeigen, können jedoch Einstellungen für Transaktionsschwellenwerte sowie Transaktionsbeschreibungen ändern.

Allen regulären Benutzern, die in der früheren Version in einem spezifischen RUM-Profil als Benutzer hinzugefügt wurden, wird die Rolle **RUM Viewer** für dieses Profil zugewiesen.

Ressource	Zulässige Operationen	
Applikationen	Ansicht	
RUM-Engines	Ansicht	

Rollen in der Benutzerverwaltung für verschiedene Kontexte

Die folgenden Rollen können nur auf bestimmte Kontexte in BSM angewendet werden. Details zu den Ressourcen und Kontexten, auf die Rollen angewendet werden können, finden Sie im Folgenden in der Beschreibung der einzelnen Rollen.

Details zu Rollen, die in ganz BSM angewendet werden können, finden Sie unter "Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung" auf Seite 280.

BPI-Administrator

Die Rolle **BPI-Administrator** kann nur auf die Ressource **Business Process Insight-Verwaltung** im Kontext **Business Process Insight** angewendet werden.

Kontext	Ressource	Zulässige Operationen
Business Process Insight	Business Process Insight-Applikation	Vollzugriff
	Business Process Insight-Verwaltung	Vollzugriff

BPI-Benutzer

Die Rolle **BPI-Benutzer** kann nur auf die Ressource **Business Process Insight-Applikation** im Kontext **Business Process Insight** angewendet werden.

Kontext	Ressource	Zulässige Operationen
Business Process	Business Process Insight-Applikation	Ansicht
Insight	Business Process Insight- Prozessdefinitionen	Ansicht

BPI - Benutzer mit eingeschränkter Ansicht

Die Rolle BPI - Benutzer mit eingeschränkter Ansicht kann nur auf die Ressource Business Process Insight-Applikation im Kontext Business Process Insight angewendet werden.

Kontext	Ressource	Zulässige Operationen
Business Process	Business Process Insight-Applikation	Anzeigen nur der bereitgestellten BPI-Prozesse, denen die Berechtigung Ansicht zugewiesen wurde.
Insight-	Business Process Insight- Prozessdefinitionen	

CMDB Open API-Abfrage

Die Rolle **CMDB Open API-Abfrage** kann nur auf die Ressource **RTSM Open API** im Kontext **RTSM** angewendet werden.

Mit dieser Rolle können Benutzer die CMDB (Configuration Management Database, Konfigurationsverwaltungsdatenbank) auf die Kommunikation mit Drittanbieterapplikationen abfragen.

Kontext	Ressource	Zulässige Operationen
RTSM	RTSM Open API	Ansicht

CMDB Open API-Aktualisierung

Die Rolle CMDB Open API-Aktualisierung kann nur auf die Ressource RTSM Open API im Kontext RTSM angewendet werden.

Mit dieser Rolle können Benutzer die CMDB (Configuration Management Database, Konfigurationsverwaltungsdatenbank) für die Kommunikation mit Drittanbieterapplikationen aktualisieren.

Kontext	Ressource	Zulässige Operationen
RTSM	RTSM Open API	Ändern

CMDB Open API-Auswirkung

Die Rolle CMDB Open API-Auswirkung kann nur auf die Ressource RTSM Open API im Kontext RTSM angewendet werden.

Mit dieser Rolle können Benutzer Operationen in der CMDB beeinflussen.

Kontext	Ressource	Zulässige Operationen
RTSM	RTSM Open API	Ansicht

CMDB Open API-Klassenmodell

Die Rolle **CMDB Open API-Klassenmodell** kann nur auf die Ressource **RTSM Open API** im Kontext **RTSM** angewendet werden.

Mit dieser Rolle können Benutzer Operationen für CITs (Configuration Item Types) durchführen.

Kontext	Ressource	Zulässige Operationen
RTSM	RTSM Open API	Ansicht

SiteScope-Administrator

Die Rolle **SiteScope-Administrator** kann nur auf die Ressource **SiteScope** im Kontext **System Availability Management** oder auf spezifische Instanzen der Ressource angewendet werden.

Wenn diese Rolle auf Ebene der Ressourcensammlung gewährt wird, kann der SiteScope-Administrator alle SiteScopes der Plattform verwalten, einschließlich der Berechtigungen für die SiteScope-Collectoren. Wenn diese Rolle auf Instanzebene gewährt wird, kann der Administrator nur die Ressourcen verwalten, die der spezifischen SiteScope-Instanz zugeordnet sind.

Allen Administratoren, die in der früheren Version in einem spezifischen SiteScope als Benutzer hinzugefügt wurden, wird die SiteScope-Administratorrolle für diesen SiteScope zugewiesen.

Kontext	Ressource	Zulässige Operationen
System Availability Management	SiteScope	Hinzufügen
		Ändern
		Ansicht
		Löschen
		Ausführen
		Vollzugriff

Standard

Die Rolle **Standard** wird automatisch zugewiesen, wenn keine andere Rolle ausgewählt wurde. Sie umfasst sehr eingeschränkte Berechtigungen, vor allem das Hinzufügen und Anzeigen von benutzerdefinierten und Trend-Reports im Kontext **Benutzerdefinierte Reports**.

Hinweis: Zum Erstellen aussagekräftiger Reports benötigt der Benutzer zusätzliche Berechtigungen für spezifische Applikationen oder Konfigurationselemente.

Kontext	Ressource	Zulässige Operationen
Benutzerdefinierte Reports	Benutzerdefinierte Reports	Hinzufügen
	Trend-Reports	Hinzufügen

Transaction Management-Bediener

Die Rolle **Transaction Management-Bediener** kann nur auf die Ressource **TransactionVision-Analyzer** im Kontext **Transaction Management** angewendet werden.

Kontext	Ressource	Zulässige Operationen
Transaction Management	TransactionVision-Analyzer	Ausführen
	TransactionVision-Job-Manager	Ausführen
	TransactionVision-Abfrage-Engines	Ausführen
	Verwaltung	Ändern
	Applikationen	Ansicht

Transaction Management-Administrator

Die Rolle **Transaction Management-Administrator** kann nur auf die Ressource **TransactionVision-Verarbeitungsserver** im Kontext **Transaction Management** angewendet werden. Die Rolle **Transaction Management-Administrator** dient der erweiterten Sicherheit, indem die Benutzer einen Vollzugriff auf die TransactionVision-Verwaltung haben, aber keinen Zugriff auf die Benutzerdaten-Ressource.

Kontext	Ressource	Zulässige Operationen
Transaction Management	TransactionVision-Verarbeitungsserver	Ändern
		Vollzugriff
	TransactionVision-Analyzer	Ändern
		Ausführen
		Vollzugriff
	TransactionVision-Job-Manager	Ändern
		Ausführen
		Vollzugriff
	TransactionVision-Abfrage-Engines	Ändern
		Ausführen
		Vollzugriff
	Verwaltung	Ändern
		Vollzugriff
	Applikationen	Hinzufügen
		Ändern
		Ansicht
		Vollzugriff

Transaction Management-Benutzer

Die Rolle **Transaction Management-Benutzer** kann nur auf die Ressource **Applikationen** im Kontext **Transaction Management** angewendet werden.

Kontext	Ressource	Zulässige Operationen
Transaction Management	Applikationen	Ansicht

Operationen für die Benutzerverwaltung

In jedem unten aufgeführten Kontext befindet sich eine Tabelle, die Folgendes auflistet:

- Jede Ressource
- Welche Operationen auf die Ressource angewendet werden können
- Eine Beschreibung der Funktion der Operation

Business Process Insight

Verwenden Sie den Kontext **Business Process Insight**, um der im System konfigurierten Business Process Insight-Instanz Berechtigungen zuzuweisen.

Ressourcen	Operation	Beschreibung
Business Process Insight-Applikation	Ansicht	Ermöglicht das Aufrufen der Business Process Insight- Applikation.
Business Process Insight-Verwaltung	Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge in der Business Process Insight-Verwaltung sowie das Gewähren oder Entfernen von Berechtigungen für andere Benutzer.
Business Process Insight- Prozessdefinitionen	Ansicht	Ermöglicht das Anzeigen eines Prozesses in der Business Process Insight-Applikation.

Diagnostics

Der Kontext **Diagnostics** bietet Ihnen die Möglichkeit, Operationen zu definieren, die für die Diagnostics-Applikation zulässig sind.

Ressourcen	Operation	Beschreibung
Diagnostics	Änderung	Ermöglicht die Anzeige der Diagnostics-Verwaltung und die Konfiguration der Diagnostics-Einstellungen.
	Ansicht	Ermöglicht die Anzeige von Diagnostics beim Zugriff auf Diagnostics über BSM.
	Ausführen	Ermöglicht das Ändern der Einstellungen in der Diagnostics- Benutzeroberfläche, zum Beispiel das Festlegen von Schwellenwerten.
	Vollzugriff	Ermöglicht das Durchführen aller Operationen auf Diagnostics und das Gewähren und Entfernen von Berechtigungen für diese Operationen.

End User Management

Der Kontext **End User Management** bietet Ihnen die Möglichkeit, Operationen zu definieren, die für die End User Management-Applikation zulässig sind. Operationen, die einem Ordner zugewiesen werden, wirken sich auf alle untergeordneten Ordner aus.

Ressourcen	Operation	Beschreibung
Warnung - Benachrichtigungsvorlage	Änderung	Ermöglicht das Bearbeiten der Eigenschaften einer kundenspezifischen Benachrichtigungsvorlage.
	Ansicht	Ermöglicht das Anzeigen der Eigenschaften einer Benachrichtigungsvorlage.
	Vollzugriff	Ermöglicht das Ausführen aller in Bezug auf eine Benachrichtigungsvorlage verfügbaren Vorgänge sowie das Gewähren und Entfernen von Berechtigungen für diese Vorgänge.
Warnung - Abhängigkeiten erstellen	Änderung	Ermöglicht das Erstellen und Entfernen von Abhängigkeiten zwischen Warnungen.
	Vollzugriff	Ermöglicht das Erstellen und Entfernen von Abhängigkeiten zwischen Warnungen sowie das Gewähren und Entfernen von Berechtigungen für diese Vorgänge.
Applikationen	Hinzufügen	Ermöglicht das Hinzufügen von Applikationen.
	Änderung	Ermöglicht das Bearbeiten von Applikationen oder einer bestimmten Instanz von Applikationen.
	Ansicht	Ermöglicht das Anzeigen von Applikationen oder einer bestimmten Instanz von Applikationen.
	Löschen	Ermöglicht das Löschen von Applikationen oder einer bestimmten Instanz von Applikationen.
	Ausführen	Ermöglicht das Starten und Beenden von Applikationen oder einer bestimmten Instanz von Applikationen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Applikationen oder bestimmte Applikationsinstanzen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Ressourcen		Operation	Beschreibung
Applikationen (bestimmte Instanzen)	bestimmte	Hinzufügen	Ermöglicht das Erstellen einer Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.
		Änderung	Ermöglicht das Bearbeiten einer Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.
		Ansicht	Ermöglicht das Anzeigen einer Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.
		Löschen	Ermöglicht das Löschen einer Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.
		Ausführen	Ermöglicht das Aktivieren und Deaktivieren einer Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.
		Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge für eine Geschäftsprozesskonfiguration für eine bestimmte Instanz von Applikationen.

Ressourcen		Operation	Beschreibung
	RUM	Hinzufügen	Ermöglicht das Erstellen einer Real User Monitor- Konfiguration für eine bestimmte Instanz von Applikationen.
		Änderung	Ermöglicht das Bearbeiten einer Real User Monitor- Konfiguration für eine bestimmte Instanz von Applikationen.
		Ansicht	Ermöglicht das Anzeigen einer Real User Monitor- Konfiguration für eine bestimmte Instanz von Applikationen.
		Löschen	Ermöglicht das Löschen einer Real User Monitor- Konfiguration für eine bestimmte Instanz von Applikationen.
	Warnung	Ausführen	Ermöglicht das Aktivieren und Deaktivieren einer Real User Monitor-Konfiguration für eine bestimmte Instanz von Applikationen.
		Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge für eine Real User Monitor-Konfiguration für eine bestimmte Instanz von Applikationen.
		Ansicht	Ermöglicht das Anzeigen einer Warnungskonfiguration für eine bestimmte Instanz von Applikationen.
	Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge für eine Warnungskonfiguration für eine bestimmte Instanz von Applikationen.	
BPM-Agenten		Ansicht	Ermöglicht das Anzeigen von BPM-Agenten und das Verwalten von Monitoren für diese Agenten.
RUM-Engines		Ansicht	Ermöglicht das Anzeigen von Real User Monitor- Engines und das Verwalten von RUM- Konfigurationen für diese Engines.

Ressourcen	Operation	Beschreibung
Skript-Repository	Hinzufügen	Ermöglicht das Erstellen neuer Ordner im Skript- Repository.
	Änderung	Ermöglicht das Umbenennen von Skript- Repository-Ordnern und das Ändern von Skripts in diesen Ordnern.
	Ansicht	Ermöglicht das Anzeigen von Skript-Repository- Ordnern und von Skripts in diesen Ordnern.
	Löschen	Ermöglicht das Löschen von Ordnern aus dem Skript-Repository.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Skriptordner und Skripts im Skript-Repository verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

RTSM

Der Kontext **RTSM** bietet Ihnen die Möglichkeit, für Ansichten zulässige Vorgänge zu definieren, die in der IT Universe-Verwaltung definiert sind und in Model Explorer, Service Health und Service Level Management angezeigt werden.

Tipp: Wenn ein Benutzer die Berechtigung für eine Ansicht in RTSM besitzt, werden dem Benutzer alle Profile in dieser Ansicht angezeigt, auch wenn er keine Berechtigungen für die Profile besitzt. Um zu verhindern, dass ein Benutzer Profile anzeigen kann, für die er keine Berechtigung besitzt, und gleichzeitig zu gewährleisten, dass der Benutzer auf eine Ansicht zugreifen kann, erstellen Sie für den Benutzer eine Ansicht, die nur die Konfigurationselemente enthält, für die der Benutzer Berechtigungen besitzt. Anschließend gewähren Sie dem Benutzer die Berechtigungen für diese Ansicht.

Ressourcen	Operation	Beschreibung
Ansichten	Hinzufügen	Ermöglicht das Hinzufügen und Klonen von Ansichten.
	Änderung	Ermöglicht das Bearbeiten von Ansichten.
	Ansicht	Ermöglicht das Anzeigen von Ansichten.
	Löschen	Ermöglicht das Entfernen von Ansichten.
	Vollzugriff	Ermöglicht die Durchführung aller verfügbaren Vorgänge für Ansichten.
RTSM	Vollzugriff	Ermöglicht Verwaltungsvorgänge für alle RTSM- Komponenten (Run-time Service Model) bis auf ITU Manager und Modeling Studio.

Ressourcen	Operation	Beschreibung
CI-Suche	Vollzugriff	Ermöglicht die Verwendung der CI-Suche von jedem Standort aus im RTSM.
Datenmodifizierung	Vollzugriff	Ermöglicht die Datenmodifizierung von jedem Standort aus im RTSM.
Zugehörige CIs abrufen	Vollzugriff	Ermöglicht das Abrufen zugehöriger CIs von jedem Standort aus im RTSM.
ITU Manager	Vollzugriff	Ermöglicht dem Benutzer den Zugang zu ITU Manager. Die dann innerhalb von ITU Universe Manager verfügbare Funktionalität hängt von den Berechtigungen für Ansichten ab, die dem Benutzer gewährt wurden.
Modeling Studio	Vollzugriff	Ermöglicht dem Benutzer den Zugang zu Modeling Studio. Die dann innerhalb von ITU Universe Manager verfügbare Funktionalität hängt von den Berechtigungen für Ansichten ab, die dem Benutzer gewährt wurden.
RTSM Open API	Änderung	Ermöglicht das Ausführen von Updates in RTSM Open API.
	Ansicht	Ermöglicht das Ausführen von Abfragen in RTSM Open API.

Operationenverwaltung

Hinweis: Der Kontext **Operations Management** steht nur zur Verfügung, wenn Sie OMi auf Ihrem BSM-Computer installiert haben. Details zum Kontext **OMi** finden Sie unter "User Context Pane" im BSM-Benutzerhandbuch.

Der Kontext **Operations Manager i** (OMi) ermöglicht Ihnen das Zuweisen von Berechtigungen für die Arbeit mit dem Kontext **Operations Manager**. Details zu den im Kontext **Operations Manager i** (OMi) verfügbaren Vorgängen finden Sie unter "Registerkarte "Operationen" für Benutzer" im BSM-Benutzerhandbuch.

Ressourcen	Operation	Beschreibung
Dem Benutzer zugewiesene Ereignisse	Bearbeiten/Auflösen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Bearbeiten" oder "Auflösen" für Ereignisse, die ihm zugewiesen sind.
	Schließen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Geschlossen" für Ereignisse, die ihm zugewiesen sind.
	Erneut öffnen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Offen" für Ereignisse mit dem Status "Geschlossen", die ihm zugewiesen sind. Die Ereignisse können jetzt zur weiteren Untersuchung und Auflösung erneut zugewiesen werden.
		Hinweis: Das emeute Öffnen von Symptomereignissen mit einer geschlossenen Ursache ist nicht möglich.
	Zuweisen zu	Ermöglicht dem Benutzer das Zuweisen von ihm zugewiesenen Ereignissen zu einem bestimmten Benutzer.
	Operator-Aktion starten	Ermöglicht dem Benutzer das Ausführen von HP Operations Manager-Operator-Aktionen für Ereignisse, die ihm zugewiesen sind und ereignisbezogene Aktionen enthalten.

Ressourcen	Operation	Beschreibung
Dem Benutzer zugewiesene Ereignisse	Automatische Aktion starten	Ermöglicht dem Benutzer das Ausführen von automatischen Aktionen für HP Operations Manager für Ereignisse, die ihm zugewiesen sind und ereignisbezogene Aktionen enthalten.

Ressourcen	Operation	Beschreibung
	Übertragungssteuerung	Ermöglicht dem Benutzer die Übertragung der Kontrolle von ihm im Ereignis-Browser zugewiesenen Ereignissen an einen externen Manager.
	Übertragene schließen	Ermöglicht dem Benutzer das Schließen von ihm im Ereignis- Browser zugewiesenen Ereignissen, für die die Kontrolle an einen externen Manager übertragen wurde.
	Ereignisbeziehungen hinzufügen/entfernen	Ermöglicht dem Benutzer das Hinzufügen und Entfernen von Beziehungen zwischen Ereignissen, die ihm im Ereignis-Browser zugewiesen sind.
	Schweregrad ändern	Ermöglicht dem Benutzer das Ändern des Schweregrads von Ereignissen, die ihm zugewiesen sind.
	Priorität ändern	Ermöglicht dem Benutzer das Ändern der Priorität von Ereignissen, die ihm zugewiesen sind.
	Titel ändern	Ermöglicht dem Benutzer das Ändern des Titels von Ereignissen, die ihm zugewiesen sind.
	Beschreibung ändern	Ermöglicht dem Benutzer das Ändern der Beschreibung von Ereignissen, die ihm zugewiesen sind.
	Lösung ändern	Ermöglicht dem Benutzer das Ändern der Lösung von Ereignissen, die ihm zugewiesen sind.
	Anmerkungen hinzufügen/löschen/aktualisieren	Ermöglicht dem Benutzer das Erstellen, Ändern und Löschen von Anmerkungen für Ereignisse, die ihm zugewiesen sind.
	Benutzerdefinierte Attribute hinzufügen/löschen/aktualisieren	Ermöglicht dem Benutzer das Erstellen, Ändern und Löschen von benutzerdefinierten Attributen für Ereignisse, die ihm zugewiesen sind.

Ressourcen	Operation	Beschreibung
Dem Benutzer nicht zugewiesene Ereignisse	Ansicht	Ermöglicht dem Benutzer das Anzeigen von Ereignissen, die ihm nicht zugewiesen sind.

Ressourcen	Operation	Beschreibung
	Bearbeiten/Auflösen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Bearbeiten" oder "Auflösen" für Ereignisse, die ihm nicht zugewiesen sind.

Ressourcen	Operation	Beschreibung
	Schließen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Geschlossen" für Ereignisse, die ihm nicht zugewiesen sind.
	Erneut öffnen	Ermöglicht dem Benutzer das Festlegen des Lebenszyklusstatus "Offen" für Ereignisse mit dem Status "Geschlossen", die ihm nicht zugewiesen sind. Die Ereignisse können jetzt zur weiteren Untersuchung und Auflösung erneut zugewiesen werden.
		Hinweis: Das erneute Öffnen von Symptomereignissen mit einer geschlossenen Ursache ist nicht möglich.
	Zuweisen zu	Ermöglicht dem Benutzer das Zuweisen von ihm nicht zugewiesenen Ereignissen zu einem bestimmten Benutzer oder einer Gruppe.
	Operator-Aktion starten	Ermöglicht dem Benutzer das Ausführen von HP Operations Manager-Operator-Aktionen für Ereignisse, die ihm nicht zugewiesen sind und ereignisbezogene Aktionen enthalten.
	Automatische Aktion starten	Ermöglicht dem Benutzer das Ausführen automatischer Aktionen für HP Operations Manager für Ereignisse, die ihm nicht zugewiesen sind und ereignisbezogene Aktionen enthalten.
	Übertragungssteuerung	Ermöglicht dem Benutzer die Übertragung der Kontrolle von ihm im Ereignis-Browser nicht zugewiesenen Ereignissen an einen externen Manager.

Ressourcen	Operation	Beschreibung
Dem Benutzer nicht zugewiesene Ereignisse	Übertragene schließen	Ermöglicht dem Benutzer das Schließen von ihm im Ereignis- Browser nicht zugewiesenen Ereignissen, für die die Kontrolle an einen externen Manager übertragen wurde.
	Ereignisbeziehungen hinzufügen/entfernen	Ermöglicht dem Benutzer das Hinzufügen und Entfernen von Beziehungen zwischen Ereignissen, die ihm im Ereignis-Browser nicht zugewiesen sind.
	Schweregrad ändern	Ermöglicht dem Benutzer das Ändern des Schweregrads von Ereignissen, die ihm nicht zugewiesen sind.
	Priorität ändern	Ermöglicht dem Benutzer das Ändern der Priorität von Ereignissen, die ihm nicht zugewiesen sind.
	Titel ändern	Ermöglicht dem Benutzer das Ändern des Titels von Ereignissen, die ihm nicht zugewiesen sind.
	Beschreibung ändern	Ermöglicht dem Benutzer das Ändern der Beschreibung von Ereignissen, die ihm nicht zugewiesen sind.
	Lösung ändern	Ermöglicht dem Benutzer das Ändern der Lösung von Ereignissen, die ihm nicht zugewiesen sind.
	Anmerkungen hinzufügen/löschen/aktualisieren	Ermöglicht dem Benutzer das Erstellen, Ändern und Löschen von Anmerkungen für Ereignisse, die ihm nicht zugewiesen sind.
	Benutzerdefinierte Attribute hinzufügen/löschen/aktualisieren	Ermöglicht dem Benutzer das Erstellen, Ändern und Löschen von benutzerdefinierten Attributen für Ereignisse, die ihm nicht zugewiesen sind.

Ressourcen	Operation	Beschreibung
Zustandsindikatoren	Zurücksetzen	Ermöglicht dem Benutzer das Löschen des aktuellen Status eines Zustandsindikators und das Zurücksetzen des Zustandsindikators auf den Status, der im Zustandsindikator-Standardwert angegeben ist.
Verwaltungs- benutzer- oberflächen	Ansicht	Gewährt Zugriff auf die Verwaltungsfunktionen in der Operations Management-Verwaltung, wie zum Beispiel:
		Correlation Rules Manager
		Content Packs Manager
		Performance Graphs Manager
		View Mappings-Manager
		Ereignisverarbeitungsanpassung
		Benutzerdefinierte Aktionen
		Benutzern, die keinen Lesezugriff für die Operations Management- Verwaltung besitzen, werden die Operations Management- Verwaltungsfunktionen nicht angezeigt, oder ihnen wird eine Fehlermeldung angezeigt, wenn sie versuchen, einen Verwaltungsmanager zu starten.
Werkzeugkategorien	Ausführen	Gewährt Zugriff auf Werkzeugkategorien. Alle Werkzeuge, die zu einer Werkzeugkategorie gehören, auf die ein Benutzer Zugriff besitzt, können von dem Benutzer ausgeführt werden.
Benutzerdefinierte Aktionen	Ausführen	Gewährt Zugriff auf benutzerdefinierte Aktionen. Alle benutzerdefinierten Aktionen, auf die ein Benutzer Zugriff besitzt, können von dem Benutzer ausgeführt werden.

Operations Orchestration-Integration

Der Kontext **Operations Orchestration-Integration** bietet Ihnen die Möglichkeit, Operationen zu definieren, die für die Operations Orchestration Administration-Applikation zulässig sind.

Ressourcen	Operation	Beschreibung
Verwaltung	Hinzufügen	Ermöglicht das Hinzufügen eines Runbooks.
	Ansicht	Ermöglicht das Anzeigen der Runbook-Verwaltung.
	Änderung	Ermöglicht das Bearbeiten der Runbook-Verwaltung.
	Löschen	Ermöglicht das Löschen eines Runbooks.
	Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge in der Runbook-Verwaltung sowie das Gewähren oder Entfernen von Berechtigungen für andere Benutzer.
Ausführung	Ausführen	Ermöglicht die Runbook-Ausführung.
	Vollzugriff	Ermöglicht das Durchführen aller verfügbaren Vorgänge bzgl. der Runbook-Ausführung sowie das Gewähren oder Entfernen von Berechtigungen für andere Benutzer.

Platform

Der Kontext **Platform** enthält alle Ressourcen, die mit der Verwaltung der Plattform verbunden sind.

Ressourcen	Operation	Beschreibung
Authentication Strategy	Änderung	Aktiviert die Schaltfläche Konfigurieren auf der Seite Authentifizierungsstrategie , die das Ändern von Konfigurationen im Assistenten für die Authentifizierungsstrategie ermöglicht.
	Ansicht	Ermöglicht das Anzeigen des Assistenten für die Authentifizierungsstrategie.
	Vollzugriff	Ermöglicht die Durchführung aller Vorgänge, die für den Assistenten für die Authentifizierungsstrategie zur Verfügung stehen.
Audit Log	Ansicht	Ermöglicht das Anzeigen des Audit-Protokolls.
	Vollzugriff	Ermöglicht das Anzeigen des Audit-Protokolls sowie das Gewähren und Entziehen von Berechtigungen zum Anzeigen des Audit-Protokolls.

Ressourcen	Operation	Beschreibung
Benutzer	Hinzufügen	Ermöglicht das Hinzufügen von Benutzern zum System.
	Änderung	Ermöglicht das Ändern von Benutzerdetails.
	Ansicht	Ermöglicht das Anzeigen von Benutzerdetails.
	Löschen	Ermöglicht das Löschen von Benutzern aus dem System.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Benutzer verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
User Groups	Hinzufügen	Ermöglicht das Hinzufügen von Benutzergruppen zum System.
	Änderung	Ermöglicht das Ändern von Benutzergruppendetails.
	Ansicht	Ermöglicht das Anzeigen von Benutzergruppendetails.
	Löschen	Ermöglicht das Löschen von Benutzergruppen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Benutzergruppen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Data Collectors	Änderung	Ermöglicht die Durchführung von Remote-Upgrades, Remote-Deinstallationen und das Festlegen von Aktualisierungen für Daten-Collectoren in der Daten- Collector-Verwaltung.
	Ansicht	Ermöglicht das Anzeigen der Daten-Collectoren in der Daten-Collector-Verwaltung.
	Löschen	Ermöglicht das Entfernen von Daten-Collector- Instanzen.
	Vollzugriff	Ermöglicht die Durchführung aller in der Datenerfassungsverwaltung verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Ressourcen	Operation	Beschreibung
Benachrichtigungssystem	Ansicht	Ermöglicht das Anzeigen von Systemticket-Details.
	Ausführen	Ermöglicht das Ausführen von Systemtickets im System.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Systemtickets verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Scheduled Reports	Hinzufügen	Ermöglicht das Erstellen neuer geplanter Reports.
	Änderung	Ermöglicht das Ändern geplanter Reports.
	Ansicht	Ermöglicht das Anzeigen geplanter Reports.
	Löschen	Ermöglicht das Löschen geplanter Reports.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf geplante Reports verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Recipients	Hinzufügen	Ermöglicht das Hinzufügen von Empfängern zur Plattform.
	Änderung	Ermöglicht das Bearbeiten von Empfängerdetails.
	Ansicht	Ermöglicht das Anzeigen von Empfängern und Empfängerdetails.
	Löschen	Ermöglicht das Entfernen von Empfängern von der Plattform.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Empfänger verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Ressourcen	Operation	Beschreibung
Custom Data Types	Hinzufügen	Ermöglicht das Hinzufügen von benutzerdefinierten Datentypen zum System.
	Änderung	Ermöglicht das Ändern von benutzerdefinierten Datentypen im System.
	Ansicht	Ermöglicht das Anzeigen von benutzerdefinierten Datentypen im System.
	Löschen	Ermöglicht das Löschen von benutzerdefinierten Datentypen im System.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Stichprobentypen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Send SNMP trap	Änderung	Ermöglicht das Aktivieren und Deaktivieren der Option zum Senden von SNMP-Traps bei Warnung sowie das Bearbeiten von SNMP-Trap-Adressen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf das Senden von SNMP-Traps bei Warnung verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Run executable file	Änderung	Ermöglicht das Aktivieren und Deaktivieren der Option zur Ausführung von ausführbaren Dateien bei Warnung sowie das Auswählen und Bearbeiten von bei Warnung auszuführenden ausführbaren Dateien.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf die Ausführung von ausführbaren Dateien bei Warnung verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Log To Event Viewer	Änderung	Ermöglicht die Festlegung, ob Warnungen in der Windows-Ereignisanzeige der Windows-Verwaltung protokolliert werden sollen.
	Vollzugriff	Ermöglicht die Festlegung, ob Warnungen in der Windows-Ereignisanzeige der Windows-Verwaltung protokolliert werden sollen, sowie das Gewähren und Entziehen von Berechtigungen für diesen Vorgang.

Ressourcen	Operation	Beschreibung
Downtime	Ansicht	Ermöglicht das Anzeigen von Ausfallzeit- Eigenschaften.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Ausfallzeiten verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Databases	Hinzufügen	Ermöglicht das Hinzufügen von Profildatenbanken zum System.
	Änderung	Ermöglicht das Ändern von Profildatenbankdetails in der Datenbankverwaltung.
	Ansicht	Ermöglicht das Anzeigen von Details der Profildatenbankverwaltung.
	Löschen	Ermöglicht das Löschen von Profildatenbanken aus dem System.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Profildatenbanken in der Datenbankverwaltung verfügbaren Vorgänge, das Arbeiten mit dem Purging Manager sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
System Recipient Template	Hinzufügen	Ermöglicht das Erstellen und Klonen von Systemempfängervorlagen.
	Änderung	Ermöglicht das Bearbeiten von Eigenschaften von Systemempfängervorlagen.
	Ansicht	Ermöglicht das Anzeigen der Eigenschaften von Systemempfängervorlagen.
	Löschen	Ermöglicht das Löschen von Systemempfängervorlagen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Systemempfängervorlagen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Ressourcen	Operation	Beschreibung
Customer Recipient Template	Hinzufügen	Ermöglicht das Hinzufügen einer kundenspezifischen Empfängervorlage.
	Änderung	Ermöglicht das Bearbeiten einer kundenspezifischen Empfängervorlage.
	Ansicht	Ermöglicht das Anzeigen der Eigenschaften einer kundenspezifischen Empfängervorlage.
	Löschen	Ermöglicht das Löschen einer kundenspezifischen Empfängervorlage.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf eine kundenspezifische Empfängervorlage verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Package Work Manipulation (nur HP Software-as-a-	Änderung	Ermöglicht das Ändern von Package-Standorten, das Umbenennen von Packages und das Auswählen von Empfängern für Package-Benachrichtigungen.
Service)	Ansicht	Ermöglicht das Anzeigen von Package-Informationen.
	Löschen	Ermöglicht das Entfernen von Packages von einem Standort.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Package-Informationen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Service Health

Ressourcen	Operation	Beschreibung
Benutzerseiten	Hinzufügen	Ermöglicht das Hinzufügen von Benutzerseiten.
	Änderung	Ermöglicht das Bearbeiten von Benutzerseiten.
	Ansicht	Ermöglicht das Anzeigen von Benutzerseiten.
	Löschen	Ermöglicht das Entfernen von Benutzerseiten.
	Vollzugriff	Ermöglicht die Durchführung aller verfügbaren Vorgänge für Benutzerseiten.
Vordefinierte Seiten	Ansicht	Ermöglicht das Anzeigen vordefinierter Seiten.

Ressourcen	Operation	Beschreibung
Benutzerkomponenten	Hinzufügen	Ermöglicht das Hinzufügen und Klonen von Komponentendefinitionen.
	Änderung	Ermöglicht das Bearbeiten von Komponentendefinitionen.
	Ansicht	Ermöglicht das Anzeigen von Komponentendefinitionen.
	Löschen	Ermöglicht das Entfernen von Komponentendefinitionen.
	Vollzugriff	Ermöglicht die Durchführung aller verfügbaren Vorgänge für Komponentendefinitionen.

Service Level Management

Sie verwenden den Kontext **Service Level Management**, um Berechtigungen für alle SLAs oder bestimmte Instanzen zuzuweisen.

Ressourcen	Operation	Beschreibung
SLAs	Hinzufügen	Ermöglicht das Hinzufügen von SLAs.
	Änderung	Ermöglicht das Umbenennen von SLAs, das Hinzufügen von Beschreibungen zu SLAs, das Anzeigen einer SLA-Konfiguration auf den Verwaltungsseiten und das Ändern von SLA-Konfigurationen.
	Ansicht	Ermöglicht das Generieren und Anzeigen von Reports und benutzerdefinierten Reports für SLAs.
	Löschen	Ermöglicht das Löschen von SLAs.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf SLAs verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

System Availability Management

Sie verwenden den Kontext **System Availability Management**, um den im System konfigurierten SiteScope-Instanzen Berechtigungen zuzuweisen.

Hinweis: Die im Kontext **System Availability Management** gewährten Berechtigungsebenen überschreiben alle in der eigenständigen SiteScope-Benutzeroberfläche gewährten Berechtigungsebenen.

Ressourcen	Operation	Beschreibung
SiteScopes	Hinzufügen	Ermöglicht das Hinzufügen von SiteScope-Profilen zu System Availability Management.
	Änderung	Ermöglicht das Ändern eines SiteScope-Profils in System Availability Management und das Hinzufügen des Inhalts zum SiteScope-Stammknoten (Gruppe, Warnung, Report) sowie das Ändern des Inhalts im SiteScope-Stammknoten (Warnung, Report), wenn der Benutzer Berechtigungen für diese Ressourcen besitzt.
	Ansicht	Ermöglicht das Anzeigen von SiteScope-Profilen in System Availability Management.
	Löschen	Ermöglicht das Löschen eines SiteScope-Profils aus System Availability Management und das Löschen des Inhalts des SiteScope-Stammknotens (Warnung, Report), wenn der Benutzer Berechtigungen für diese Ressourcen besitzt.
	Ausführen	Ermöglicht das Ausführen des Inhalts des SiteScope- Stammknotens (Warnung, Report), wenn der Benutzer Berechtigungen für diese Ressourcen besitzt.
	Vollzugriff	Ermöglicht die Durchführung aller verfügbaren Vorgänge für das SiteScope-Profil und den SiteScope-Stammknoten.

Transaction Management

Ressourcen	Operation	Beschreibung
TransactionVision- Verarbeitungsserver	Änderung	Ermöglicht das Ändern von TransactionVision- Verarbeitungsservern.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf TransactionVision-Verarbeitungsserver verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
TransactionVision-	Änderung	Ermöglicht das Ändern von TransactionVision-Analyzern.
Analyzer	Ausführen	Ermöglicht das Starten und Beenden von TransactionVision-Analyzern.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf TransactionVision-Analyzer verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Ressourcen	Operation	Beschreibung
TransactionVision- Job-Manager	Änderung	Ermöglicht das Ändern von TransactionVision-Job- Managern.
	Ausführen	Ermöglicht das Starten und Beenden von TransactionVision-Job-Managern.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf TransactionVision-Job-Manager verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
TransactionVision- Abfrage-Engines	Änderung	Ermöglicht das Ändern von TransactionVision-Abfrage- Engines.
	Ausführen	Ermöglicht das Starten und Beenden von TransactionVision-Abfrage-Engines.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf TransactionVision-Abfrage-Engines verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Verwaltung	Änderung	Ermöglicht die Durchführung von Verwaltungsänderungen. Dies umfasst keine TransactionVision-spezifischen Änderungen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf die Verwaltung verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Benutzerdaten	Ansicht	Ermöglicht das Anzeigen von Benutzerdaten in Reports und in Ereignisdetails.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Benutzerdaten verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Applikationen	Hinzufügen	Ermöglicht das Hinzufügen von Applikationen.
	Änderung	Ermöglicht das Ändern von Applikationen.
	Ansicht	Ermöglicht das Anzeigen von Applikationen.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Applikationen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Benutzerdefinierte Reports

Sie verwenden den Kontext **Benutzerdefinierte Reports**, um Berechtigungen für die unterschiedlichen Typen benutzerdefinierter Reports und die verbundenen Einstellungen zuzuweisen.

Ressourcen	Operation	Beschreibung
Benutzerdefinierte	Hinzufügen	Ermöglicht das Hinzufügen benutzerdefinierter Reports.
Reports	Änderung	Ermöglicht das Erstellen, Bearbeiten und Löschen von benutzerdefinierten Reports.
	Ansicht	Ermöglicht das Anzeigen benutzerdefinierter Reports.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf benutzerdefinierte Reports verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge
Trend-Reports	Hinzufügen	Ermöglicht das Erstellen von Trend-Reports.
	Änderung	Ermöglicht das Erstellen, Bearbeiten und Löschen von Trend- Reports.
	Ansicht	Ermöglicht das Anzeigen von Trend-Reports.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Trend-Reports verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge
Benutzerdefinierte Links	Änderung	Ermöglicht das Erstellen und Löschen von benutzerdefinierten Links.
	Ansicht	Ermöglicht das Anzeigen benutzerdefinierter Links.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf benutzerdefinierte Links verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge
Excel-Reports	Änderung	Ermöglicht das Hinzufügen, Löschen und Aktualisieren von Excel Open API-Reports.
	Ansicht	Ermöglicht das Anzeigen von Excel Open API-Reports.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Excel Open API-Reports verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Standardkopf/- fußzeile	Änderung	Ermöglicht das Ändern der Standardkopfzeilen/-fußzeilen für benutzerdefinierte Reports/Trend-Reports.
	Vollzugriff	Ermöglicht das Ändern, Gewähren und Aufheben von Berechtigungen zum Ändern der Standardkopfzeilen/- fußzeilen für benutzerdefinierte Reports und Trend-Reports.

Ressourcen	Operation	Beschreibung
Filter-Favorit	Änderung	Ermöglicht das Bearbeiten des Filter-Favoriten.
	Löschen	Ermöglicht das Löschen des Filter-Favoriten
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf den Favoriten- Filter verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge
Anmerkung	Änderung	Ermöglicht das Bearbeiten einer Anmerkung.
	Löschen	Ermöglicht das Löschen einer Anmerkung.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Anmerkungen verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.
Service-Report	Änderung	Ermöglicht das Bearbeiten eines Service-Reports.
	Löschen	Ermöglicht das Löschen eines Service-Reports.
	Vollzugriff	Ermöglicht die Durchführung aller in Bezug auf Service- Reports verfügbaren Vorgänge sowie das Gewähren und Entziehen von Berechtigungen für diese Vorgänge.

Benutzerverwaltung – Benutzeroberfläche

Dialogfeld "Gruppe erstellen"

In diesem Dialogfeld können Sie Gruppen erstellen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen >		
	Benutzerverwaltung aus, klicken Sie auf die Schaltfläche Erstellen *, und wählen Sie Gruppe erstellen aus.		
Siehe auch	"Gruppen- und Benutzerhierarchie" auf Seite 254		

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung	
Gruppenbeschreibung	Die Beschreibung der Gruppe.	
	Hinweis: Dieses Feld ist optional.	
	Syntaxausnahmen:	
	Darf 99 Zeichen nicht überschreiten.	
Gruppenname	Name der Gruppe	
	Syntaxausnahmen:	
	Darf 40 Zeichen nicht überschreiten	
	Folgende Zeichen werden nicht unterstützt: "\/[]: <>+=;,?*% &	
	Der Name muss eindeutig sein.	

Dialogfeld "Benutzer erstellen"

In diesem Dialogfeld können Sie einen neuen Benutzer erstellen und einen Empfänger, der mit dem Benutzer verknüpft ist.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, klicken Sie auf die Schaltfläche zum Erstellen eines		
	Benutzers/einer Gruppe in der ausgewählten Gruppe und wählen Sie Benutzer erstellen aus.		

Wichtiger	Das Dialogfeld Benutzer erstellen enthält die folgenden Registerkarten:
Hinweis	Benutzerkonto. Weitere Informationen finden Sie unter "Registerkarte "Allgemein" (Benutzerverwaltung)" auf der nächsten Seite.
	Empfänger. Weitere Informationen finden Sie unter "Registerkarte "Empfänger" (Benutzerverwaltung)" auf Seite 344.
Relevante	"Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257
Aufgaben	"Anpassen von Benutzermenüs" auf Seite 273
Siehe auch	"Benutzerverwaltung" auf Seite 246

Registerkarte "Anpassung" (Benutzerverwaltung)

Auf dieser Registerkarte können Sie die Seite, die Benutzern beim Aufrufen von BSM angezeigt wird, sowie die Menüelemente auswählen, die auf den Seiten von BSM zur Verfügung stehen sollen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung und einen Knoten aus dem Ausschnitt Gruppen/Benutzer aus und klicken Sie auf die Registerkarte Anpassung.	
Wichtiger Hinweis	Eigenschaften werden nach der Hierarchie der Knoten vererbt. Wird ein Kontext für einen Gruppenknoten deaktiviert (ausgeblendet), kann er für untergeordnete Knoten nicht ausgewählt werden.	
Relevante Aufgaben	 "Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257 "Anpassen von Benutzermenüs" auf Seite 273 	
Siehe auch	"Anpassen der Benutzermenüs" auf Seite 256	

Elemente der Oberfläche	Beschreibung
Kontexte	Wählen Sie einen BSM-Kontext aus. Sie können für den Kontext folgende Aktionen durchführen:
	Wählen Sie Kontexte und Applikationen, die für den angegebenen Benutzer bzw. die Gruppe sichtbar sein sollen, im Bereich Kontexte aus. Deaktivieren Sie das Kontrollkästchen, um einen Kontext oder eine Applikation auszublenden. Standardmäßig sind alle Kontexte sichtbar.
	Wählen Sie Seiten und Registerkarten, die für den angegebenen Benutzer oder die Gruppe sichtbar sein sollen, im Bereich Seiten und Registerkarten aus. Standardmäßig sind alle Seiten und Registerkarten sichtbar.
	Klicken Sie auf die Schaltfläche Als standardmäßigen Eingangskontext festlegen, um den Kontext als Kontext festzulegen, der angezeigt wird, wenn sich der Benutzer bei BSM anmeldet.
	Weitere Informationen zu BSM-Kontexten finden Sie unter "Ausschnitt "Ressourcenstruktur"" auf Seite 347.
Seiten und Registerkarten	Wählen Sie die Seiten und Registerkarten aus, die für den im Bereich Kontexte ausgewählten BSM-Kontext sichtbar sein sollen.
	Weisen Sie eine Seite oder Registerkarte als Standardseite zu, die für den im Bereich Kontexte ausgewählten Kontext geöffnet wird.
	Hinweis: Für die Applikationen Service Health und Operations Management können Sie keinen Benutzerzugriff für spezifische Seiten definieren, Sie können hier nur den Benutzerzugriff auf Applikationsebene aktivieren oder deaktivieren.
Als standardmäßigen	Legt den im Bereich Kontexte ausgewählten Kontext als Eingabekontext fest, der angezeigt wird, wenn sich ein Benutzer bei BSM anmeldet.
Eingangskontext festlegen	Hinweis: Das Symbol Standardmäßiger Eingangskontext wird neben dem angegebenen Kontext angezeigt.
Als standardmäßige	Weist die angegebene Seite oder Registerkarte als Standardseite zu, die für den im Bereich Kontexte ausgewählten Kontext geöffnet wird.
Eingangsseite festlegen	Hinweis: Das Symbol Standardmäßige Eingangsseite wird neben der angegebenen Seite oder Registerkarte angezeigt.

Registerkarte "Allgemein" (Benutzerverwaltung)

Diese Registerkarte enthält die Parameter für den ausgewählten Benutzer bzw. für die ausgewählte Gruppe.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung > Allgemein aus.
Wichtiger Hinweis	Sie können die Parameter des Benutzers oder der Gruppe bearbeiten, indem Sie die entsprechenden Felder in der Registerkarte Allgemein ändern.
	Die Felder Gruppenname und Gruppenbeschreibung werden nur angezeigt, wenn im Bereich Gruppen/Benutzer eine Gruppe ausgewählt ist. Alle anderen Felder werden nur angezeigt, wenn im Bereich Gruppen/Benutzer ein Benutzer ausgewählt ist.
Relevante Aufgaben	"Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257
Siehe	"Benutzerverwaltung" auf Seite 246
auch	"Dialogfeld "Gruppe erstellen"" auf Seite 339
	"Dialogfeld "Benutzer erstellen"" auf Seite 339
	"Ausschnitt "Gruppen/Benutzer"" auf Seite 352

Die im Folgenden beschriebenen Elemente der Benutzeroberfläche werden angezeigt, wenn Sie im linken Bereich einen Benutzer auswählen:

Elemente der Oberfläche	Beschreibung
Kennwort bestätigen	Geben Sie das Kennwort erneut ein, das Sie in das Feld Kennwort eingegeben haben.
E-Mail	Die E-Mail-Adresse des Benutzers.
Anmeldename	Der Name, mit dem der Benutzer sich bei BSM anmeldet.
	Syntaxausnahmen:
	Darf 99 Zeichen nicht überschreiten.
	 Folgende Zeichen werden nicht unterstützt: "\/[]: <> + = ; , ? * % & <leerzeichen></leerzeichen>
	Der Name muss eindeutig sein.
	Hinweise:
	Der Anmeldename wird als Quickinfo angezeigt, wenn Sie in der Registerkarte Durchsuchen des Bereichs Gruppen/Benutzer auf den Benutzernamen zeigen.
	Der Anmeldename kann nicht geändert werden.

Elemente der Oberfläche	Beschreibung
Kennwort	Das Kennwort, mit dem der Benutzer sich bei BSM anmeldet.
	Syntaxausnahmen:
	Darf 20 Zeichen nicht überschreiten.
	Hinweise:
	Als Sicherheitsvorkehrung wird dieses Feld in der Registerkarte Allgemein leer angezeigt. Um das Kennwort zu ändern, geben Sie das Kennwort in das Feld für die Kenworteingabe und dann erneut in das Feld Kennwort bestätigen ein.
	Nur ein Benutzer, dem die Berechtigungen eines Sicherheits-Officers zugewiesen wurden, kann sein Kennwort ändern.
Zeitzone	Die Zeitzone des Benutzerstandortes entsprechend der Angabe im Feld Benutzer erstellen .
	Hinweis: Wenn Sie die Zeitzone ändern, wird auch der verbundene Empfänger-Offset von der GMT geändert, nachdem Sie die Änderung bestätigt haben.
Benutzermodus	Der Benutzermodus entsprechend der Konfiguration im Dialogfeld Benutzer erstellen . Folgende Optionen stehen zur Verfügung:
	Nicht angegeben. Der Benutzer befindet sich in keinem bestimmten Modus. Wählen Sie diese Option aus, wenn folgende Bedingungen erfüllt sind:
	 BSM arbeitet mit Benutzermodi und Sie möchten, dass dieser Benutzer KPIs für beide Modi in Service Health-Ansichten anzeigen können soll.
	 Ihr System arbeitet nicht mit Benutzermodi.
	Operationsbenutzer. Ermöglicht dem Benutzer das Anzeigen der Operationsversion von KPIs.
	Geschäftsbenutzer. Ermöglicht dem Benutzer das Anzeigen der Geschäftsversion von KPIs.
Benutzername	Der Name des Benutzers, der im Dialogfeld Benutzer erstellen konfiguriert ist.
	Syntaxausnahmen:
	Darf 50 Zeichen nicht überschreiten.
	• Folgende Zeichen werden nicht unterstützt: "\/[]: <>+=;,?*%&

Die im Folgenden beschriebenen Elemente der Benutzeroberfläche werden angezeigt, wenn Sie im linken Bereich eine Gruppe auswählen:

Elemente der Oberfläche	Beschreibung
Gruppenbeschreibung	Die Beschreibung der Gruppe, die im Dialogfeld Gruppe erstellen konfiguriert ist.
	Hinweis: Dieses Feld ist optional.
Gruppenname	Der Name der Gruppe, der im Dialogfeld Gruppe erstellen konfiguriert ist.

Registerkarte "Empfänger" (Benutzerverwaltung)

Auf dieser Seite können Sie Empfänger, deren E-Mail-, Pager- und SMS-Informationen sowie die Vorlage definieren, die zum Senden von Warnungsbenachrichtigungen oder geplanten Reports an diese Empfänger verwendet werden soll.

Details zum Konzept finden Sie unter "Empfängerverwaltung" auf Seite 358.

Informationen zur Benutzeroberfläche finden Sie unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten" auf Seite 364.

Registerkarte "Hierarchie" (Benutzerverwaltung)

Auf dieser Registerkarte könne Sie Benutzer zu einer Gruppe zuweisen, die Zuweisung auflösen oder Gruppen unterordnen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung und eine Gruppe oder einen Benutzer aus dem Ausschnitt Gruppen/Benutzer aus und klicken Sie auf die Registerkarte Hierarchie.
	Auf der Registerkarte Hierarchie wird Folgendes angezeigt:
	Übergeordnete Gruppen. Die Gruppen, denen die ausgewählte Gruppe untergeordnet ist.
	Untergeordnete Gruppen und Benutzer. Die Gruppen und Benutzer, die direkt der ausgewählten Gruppe untergeordnet sind.

Wichtiger Hinweis	 Um einen Benutzer unterzuordnen, müssen Sie die Gruppe auswählen, der er untergeordnet werden soll, und dann auf die Schaltfläche Untergeordnete Gruppen und Benutzer bearbeiten klicken.
	Wird eine untergeordnete Gruppe von der übergeordneten Gruppe entfernt, wird die Gruppe selber nicht gelöscht.
	Beim Löschen einer übergeordneten Gruppe werden die untergeordneten Gruppen und Benutzer nicht gelöscht.
	 Wenn BSM-Gruppen mit Gruppen auf einem externen LDAP-Server synchronisiert wurden, k\u00f6nnen BSM-Benutzer nicht zwischen Gruppen verschoben werden und es werden nur Gruppen auf der Benutzeroberfl\u00e4che angezeigt. Informationen zum Synchronisieren von Gruppen finden Sie unter "Synchronisieren von Benutzern" auf Seite 419.
Relevante Aufgaben	 "Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257 "Konfigurieren der Gruppen- und Benutzerhierarchie" auf Seite 267
Siehe auch	"Gruppen- und Benutzerhierarchie" auf Seite 254

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
	Gibt eine Gruppe an, der die ausgewählte Gruppe oder der Benutzer untergeordnet ist.
<u></u>	Gibt einen Benutzer an, der der ausgewählten Gruppe untergeordnet ist.
Untergeordnete Gruppen und Benutzer	Zeigt die Gruppen und Benutzer, die direkt der im Ausschnitt Gruppen/Benutzer ausgewählten Gruppe untergeordnet sind.
Untergeordnete Gruppen und Benutzer bearbeiten	Öffnet das Fenster Untergeordnete Gruppen und Benutzer bearbeiten , in dem Sie Gruppen und Benutzer aus der ausgewählten Gruppe unterordnen oder entfernen können. Weitere Informationen finden Sie unter "Registerkarte "Hierarchie" (Benutzerverwaltung)" auf der vorherigen Seite.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie eine Gruppe im Ausschnitt Gruppen/Benutzer auswählen.
Übergeordnete Gruppen	Zeigt die Gruppen an, denen die Gruppen oder Benutzer, die im Ausschnitt Gruppen/Benutzer ausgewählt wurden, direkt untergeordnet werden.

Dialogfeld "Untergeordnete Gruppen und Benutzer bearbeiten"

Elemente der Oberfläche	Beschreibung
	Verschiebt die Gruppe oder den Benutzer in den Ausschnitt Untergeordnete Gruppen und Benutzer und ordnet die Gruppe oder den Benutzer der angegebenen Gruppe unter.
	Verschiebt die Gruppe oder den Benutzer in den Ausschnitt Gruppen/Benutzer und entfernt die Gruppe oder den Benutzer aus der Verschachtelung unter der angegebenen Gruppe.
Untergeordnete Gruppen und Benutzer	Wählen Sie eine Gruppe oder einen Benutzer aus, den Sie aus der angegebenen Gruppe entfernen möchten.
Gruppen/Benutzer	Wählen Sie eine Gruppe oder einen Benutzer aus, den Sie der angegebenen Gruppe unterordnen möchten.

Registerkarte "Berechtigungen" (Benutzerverwaltung)

Diese Registerkarte bietet Ihnen die Möglichkeit, Berechtigungen für Gruppen und Benutzer auf bestimmte Ressourcen und Instanzen der im System definierten Ressourcen anzuwenden.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung > Berechtigungen aus.
	Die Registerkarte Berechtigungen ist in folgende Bereiche unterteilt:
	Ausschnitt Gruppen/Benutzer links auf der Seite. Weitere Informationen finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.
	 Ausschnitt mit der Ressourcenstruktur in der Mitte der Seite. Weitere Informationen finden Sie unter "Ausschnitt "Ressourcenstruktur"" auf der nächsten Seite.
	Registerkarte Rollen rechts auf der Seite. Weitere Informationen finden Sie unter "Registerkarte "Rollen"" auf Seite 349.
	Registerkarte Operationen rechts auf der Seite. Weitere Informationen finden Sie unter "Registerkarte "Operationen"" auf Seite 350.
Wichtiger Hinweis	Sie können Berechtigungen immer nur einem Benutzer oder einer Gruppe erteilen.
	 Das Gewähren von Hinzufügen-Berechtigungen in der Registerkarte Operationen umfasst nicht automatisch Ansicht-Berechtigungen für die entsprechende Ressource.
	Wenn Sie mehreren Benutzern Berechtigungen zuweisen möchten, wird empfohlen, die Benutzer mithilfe der Registerkarte Hierarchie in logische Gruppen einzuteilen. Weitere Informationen finden Sie unter "Registerkarte "Hierarchie" (Benutzerverwaltung)" auf Seite 344.

Relevante	"Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257
Aufgaben	"Zuweisen von Berechtigungen" auf Seite 266
Siehe auch	"Berechtigungen" auf Seite 248

Ausschnitt "Ressourcenstruktur"

Auf dieser Registerkarte werden die Instanzen und Ressourcen angezeigt, die in jedem BSM-Kontext zur Verfügung stehen, für den Sie Berechtigungen einstellen.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung > Berechtigungen aus.
	Die folgenden Ressourcentypen werden im Ausschnitt Ressourcenstruktur angezeigt:
	Ressourcen mit Instanzen
	Instanzen einer Ressource
	Hinweis: Wenn ein Benutzer eine Instanz einer Ressource definiert oder erstellt, beispielsweise wenn er ein Profil "Geschäftsprozess" erstellt, besitzt der Benutzer die Berechtigung Vollzugriff für die Ressourceninstanz und alle untergeordneten Ressourcen.
	Ressource ohne Instanzen
Wichtiger Hinweis	Die Business Service Management-Ressource bezieht sich auf alle Kontexte in BSM und ihr können nur Rollen zugewiesen werden.
	Die Ressourcen werden anhand des Kontextes eingeteilt, in dem sie innerhalb der Plattform funktionieren, und nicht notwendigerweise danach, wo sie sich auf der Benutzeroberfläche befinden.
	Sie können nur mehrere Ressourcen auswählen, wenn Sie Instanzen auswählen. Informationen zu Instanzen finden Sie unter "Grundlegende Informationen zu Berechtigungen für Ressourcen" auf Seite 249.
Relevante Aufgaben	"Zuweisen von Berechtigungen" auf Seite 266
Siehe	"Grundlegende Informationen zu Berechtigungen für Ressourcen" auf Seite 249
auch	"Ausschnitt "Ressourcenstruktur"" oben

Elemente der Oberfläche	Beschreibung
≗ ¥	Eine Instanz einer Ressource.

Elemente der Oberfläche	Beschreibung
1	Eine Ressource ohne Instanzen.
	Eine Ressource, die über Instanzen verfügt (eine Ressourcensammlung).
Kontext auswählen	Wählen Sie einen BSM-Kontext aus, für den Sie Berechtigungen konfigurieren möchten. Weitere Informationen zu BSM-Kontexten finden Sie unter "Ausschnitt "Ressourcenstruktur"" auf der vorherigen Seite.
Einstellungen	Einstellungen für spezielle Berechtigungen für Konfigurationen in Ihrer Sitzung zur Benutzerverwaltung. Sie können unter den folgenden Optionen wählen:
	Berechtigungen automatisch bei Auswahl einer anderen Ressource übernehmen. Wenn Sie diese Option auswählen, müssen Sie nicht mehr nach jedem Vorgang auf die Schaltfläche Berechtigungen übernehmen klicken. Wird diese Option nicht ausgewählt, müssen Sie auf Berechtigungen übernehmen klicken, bevor Sie mit dem nächsten Vorgang fortfahren.
	Keine Warnmeldung anzeigen beim Widerrufen von VIEW von Ressource. Wird der Ansicht-Vorgang für einen Benutzer aus der Ressource entfernt, hat dieser Benutzer keinen Zugriff auf die Ressource oder auf die untergeordneten Ressourcen oder Instanzen. Aus diesem Grund wird eine Warnmeldung angezeigt, wenn Berechtigungen zur Ansicht entfernt werden Durch das Auswählen dieser Option wird die Warnmeldung deaktiviert.
	Hinweis: Wenn Sie die Berechtigungseinstellungen auswählen, gelten die ausgewählten Optionen nur für die aktuelle BSM-Sitzung.

Ressourcenkontexte

Folgende Kontexte sind enthalten:

Elemente der Oberfläche	Beschreibung
Business Process Insight	Dazu gehören die Ressourcen für die Aktivierung von Berechtigungen für das Ausführen und Verwalten der Business Process Insight-Applikation.
Diagnostics	Dazu gehören alle Ressourcen, die mit Diagnostics verknüpft sind.
End User Management	Dazu gehören alle Ressourcen für die Durchführung und Verwaltung der End User Management-Applikation.
MyBSM	Dazu gehören Ressourcen, die für die Verwaltung von Benutzerseiten, vordefinierten Seiten und Benutzerkomponenten erforderlich sind.

Elemente der Oberfläche	Beschreibung
MyBSM (Legacy)	Dazu gehören Ressourcen, die für die Verwaltung von Modulen und Portlet-Definitionen erforderlich sind.
Operationenverwaltung	Dazu gehören alle Ressourcen für die Durchführung und Verwaltung der Operationenverwaltungs-Applikation.
Operations Orchestration- Integration	Dazu gehören die Ressourcen für die Aktivierung von Berechtigungen für das Ausführen und Verwalten der Operations Orchestration-Applikation.
Platform	Dazu gehören alle Ressourcen für die Verwaltung der Plattform.
RTSM	Dazu gehören alle Ressourcen für Run-time Service Model (RTSM).
Service Health Analyzer	Dazu gehören alle Ressourcen für die Durchführung und Verwaltung der Service Health Analyzer-Applikation.
Service Level Management	Dazu gehört die SLA-Ressource.
Bedarfsgesteuerte SiteScope-Monitore	
System Availability Management	Dazu gehören die verschiedenen SiteScope-Gruppen
Transaction Management	Dazu gehören die Ressourcen für die Durchführung der TransactionVision-Applikation.
Benutzerdefinierte Reports	Dazu gehören der benutzerdefinierte Report, der Trend-Report, der benutzerdefinierte Link und Ressourcen der Excel-Reports.

Registerkarte "Rollen"

Zeigt die Rollen an, die für Gruppen und Benutzer in BSM konfiguriert werden können.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung > Berechtigungen aus.
Relevante Aufgaben	"Zuweisen von Berechtigungen" auf Seite 266
Siehe auch	 "Grundlegende Informationen zu Berechtigungen für Ressourcen" auf Seite 249 "Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung" auf Seite 280

Elemente der Oberfläche	Beschreibung
Berechtigungen übernehmen	Übernimmt die für die Rollen konfigurierten Berechtigungen.
Gewähren	Aktivieren Sie das Kontrollkästchen, um die angegebenen Rollen der Gruppe oder dem Benutzer zuzuweisen.
Rollen	Die Rollen, die einer Gruppe oder einem Benutzer für die ausgewählte Ressource bzw. Instanzen zugewiesen werden können. Eine Beschreibung der verfügbaren Rollen finden Sie unter "Innerhalb von BSM angewendete Rollen für die Benutzerverwaltung" auf Seite 280.

Registerkarte "Operationen"

Zeigt die vordefinierten Operationen an, die für Gruppen und Benutzer in BSM konfiguriert werden können.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung > Berechtigungen aus.
Relevante Aufgaben	"Zuweisen von Berechtigungen" auf Seite 266
Siehe auch	 "Grundlegende Informationen zu Berechtigungen für Ressourcen" auf Seite 249 "Operationen für die Benutzerverwaltung" auf Seite 314

Elemente der Oberfläche	Beschreibung
Berechtigungen übernehmen	Übernimmt die für die Ressource konfigurierten Berechtigungen.
Gewähren	Aktivieren Sie das Kontrollkästchen, um die angegebene Operation der Gruppe oder dem Benutzer zuzuweisen.

Elemente der Oberfläche	Beschreibung
Gewährt von Gruppe/Rollen/Übergeordnetem Element	Zeigt die Berechtigungen an, die von einer Gruppe, einer Rolle oder einer übergeordneten Ressource gewährt wurden.
	Hinweis:
	Sie können diese Berechtigungen nicht einzeln entfernen. Es ist allerdings möglich, zusätzliche Berechtigungen zu erteilen.
	Wenn Sie Berechtigungen entfernen möchten, die von einer Gruppe, einer Rolle oder einer übergeordneten Ressource gewährt wurden, müssen Sie diese Änderung auf der Ebene der Gruppe, Rolle oder übergeordneten Ressource durchführen.
Erben	Aktivieren Sie das Kontrollkästchen in der Spalte Erben , damit die Operation an die untergeordneten Ressourcen innerhalb der ausgewählten Ressource vererbt wird.
	Hinweis:
	Das Kontrollkästchen Erben wird nur für die ausgewählten Ressourcen aktiviert.
	Standardmäßig ist das Kontrollkästchen Erben aktiviert, wenn Sie eine Operation zu bestimmten Ressourceninstanzen zuweisen. Sie können die Option Erben deaktivieren, damit die Operation nicht an die untergeordneten Ressourcen innerhalb der ausgewählten Ressource vererbt wird.
Operation	Die Operationen, die einer Gruppe oder einem Benutzer für die ausgewählte Ressource bzw. die Instanzen zugewiesen werden können. Weitere Informationen zu den verfügbaren Operationen finden Sie unter "Operationen für die Benutzerverwaltung" auf Seite 314.

Hauptseite der Benutzerverwaltung

Auf dieser Seite werden Informationen zu den Gruppen und Benutzern angezeigt, die für den Zugriff auf BSM konfiguriert wurden, einschließlich der entsprechenden Berechtigungsstufen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen >	
	Benutzerverwaltung aus.	

Wichtiger Beim ersten Öffnen der Benutzerverwaltung oder wenn sich der Mauszeiger auf Hinweis dem Knoten **Alle** befindet, umfasst die Seite folgende Komponenten: • den Ausschnitt **Gruppen/Benutzer**. Details finden Sie unter "Ausschnitt "Gruppen/Benutzer"" unten. • den Ausschnitt für den **Workflow**. Auf der Seite für den Workflow werden einführende Informationen zur Applikation Benutzerverwaltung und ein empfohlener Workflow für die Konfiguration von Benutzern und Gruppen angezeigt. Bei Auswahl eines **Benutzers** enthält die Seite folgende Registerkarten: • Allgemein. Details finden Sie unter "Registerkarte "Allgemein" (Benutzerverwaltung)" auf Seite 341. • Empfänger. Details finden Sie unter "Registerkarte "Empfänger" (Benutzerverwaltung)" auf Seite 344. • Berechtigungen. Details finden Sie unter "Registerkarte "Berechtigungen" (Benutzerverwaltung)" auf Seite 346. • Hierarchie. Details finden Sie unter "Registerkarte "Hierarchie" (Benutzerverwaltung)" auf Seite 344. • Anpassung. Details finden Sie unter "Registerkarte "Anpassung" (Benutzerverwaltung)" auf Seite 340. Bei Auswahl einer **Gruppe** enthält die Seite folgende Registerkarten: • Allgemein. Details finden Sie unter "Registerkarte "Allgemein" (Benutzerverwaltung)" auf Seite 341. • Berechtigungen. Details finden Sie unter "Registerkarte "Berechtigungen" (Benutzerverwaltung)" auf Seite 346. • Hierarchie. Details finden Sie unter "Registerkarte "Hierarchie" (Benutzerverwaltung)" auf Seite 344. Relevante "Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257 Aufgaben Siehe • "Benutzerverwaltung" auf Seite 246 auch • "Ausschnitt "Gruppen/Benutzer"" unten

Ausschnitt "Gruppen/Benutzer"

Dieser Ausschnitt zeigt die Liste der Benutzer und Benutzergruppen an, die für den Zugriff auf BSM konfiguriert sind.

Zugriff	Wählen Sie Admin > Plattform > Benutzerverwaltung . Der Ausschnitt Gruppen/Benutzer wird auf der linken Seite aller Registerkarten der Applikation für die Benutzerverwaltung angezeigt.
	Der Ausschnitt Gruppen/Benutzer enthält die folgenden Registerkarten:
	Durchsuchen. Zeigt eine Liste der konfigurierten Benutzer und Gruppen an und ermöglicht Ihnen das Erstellen oder Löschen von Benutzern und Gruppen.
	 Suchen. Zeigt eine Tabellenansicht der Benutzer und Gruppen an und ermöglicht Ihnen die Suche nach einem Benutzer oder einer Gruppe nach den folgenden Kriterien:
	■ Gruppenname
	■ Anmeldename
	■ Benutzername
	■ Letzte Anmeldung des Benutzers
	Sie können die Spalten sortieren, indem Sie auf eine der Spaltenüberschriften über den Feldern klicken.
	Sie können bei der Suche Platzhalterzeichen (*) verwenden.
Wichtiger Hinweis	 Wenn Sie mehrere Benutzer oder Gruppen verwenden und die Parameter ändern, werden die Änderungen erst nach dem ersten ausgewählten Benutzer wirksam. Eine Ausnahme bildet die Option Löschen, bei der mehrere Benutzer gleichzeitig gelöscht werden.
	Beim Erstellen einer Gruppe werden die Zugriffsberechtigungen automatisch an die Benutzer der Gruppe vererbt.
	Beim Erstellen von Benutzern mit dem Cursor auf einer Gruppe werden die Benutzer automatisch innerhalb der Gruppe verschachtelt.
Relevante Aufgaben	"Konfigurieren von Benutzern und Berechtigungen – Workflow" auf Seite 257
Siehe auch	"Hauptseite der Benutzerverwaltung" auf Seite 351

Elemente der	
	Beschreibung
* マ	Erstellt einen Benutzer oder eine Gruppe.
	Je nachdem, ob Sie das Erstellen eines Benutzer oder einer Gruppe wählen, wird das Fenster Benutzer erstellen oder Gruppe erstellen angezeigt.
	Wenn Sie eine neue Gruppe oder einen neuen Benutzer erstellen, wird der Ausschnitt Gruppe/Benutzer aktualisiert und die neu erstellte Gruppe bzw. der Benutzer ausgewählt.
	Hinweis: In Firefox wird nach der Aktualisierung der Knoten Alle ausgewählt.
	Weitere Informationen finden Sie unter "Dialogfeld "Benutzer erstellen"" auf Seite 339 oder "Dialogfeld "Gruppe erstellen"" auf Seite 339.
<u>-</u>	Klont die Einstellung eines vorhandenen Benutzers oder einer Gruppe zu einem neuen Benutzer bzw. einer Gruppe.
×	Löscht den ausgewählten Benutzer bzw. die Gruppe.
	Hinweis: Wenn Sie einen Benutzer löschen, wird der verknüpfte Empfänger ebenfalls gelöscht.
*	Blendet die in der Hierarchiestruktur ausgewählten Gruppen ein bzw. aus.
	Hinweis: Es werden nur zuvor geladene Knoten eingeblendet.
Ů\$×	Klicken Sie auf Gruppenzuordnungen , um lokale Gruppen Gruppen zuzuordnen, die auf dem LDAP-Server konfiguriert sind, oder wählen Sie Veraltete Benutzer löschen , um BSM-Benutzer zu löschen, die nicht mehr auf dem LDAP-Server konfiguriert sind. Wenn Sie Veraltete Benutzer löschen ausgewählt haben, können Sie mehrere Benutzer gleichzeitig entfernen, indem Sie bei der Auswahl von Benutzern die Strg-Taste gedrückt halten.
	Details finden Sie unter "Dialogfeld "Gruppenzuordnungen" auf der nächsten Seite.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn die Option Zuordnung im Assistent zur Verwaltung von Authentifizierungen aktiviert wurde. Details finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Elemente der Oberfläche	Beschreibung
%	Klicken Sie, um den Sicherheits-Officer zuzuweisen oder anzuzeigen. Der Sicherheits-Officer ist ein Benutzer, der bestimmte sensible Report-Informationen im System konfigurieren kann, beispielsweise, welche RUM-Transaktionsparameter in bestimmten Reports (Sitzungsdetails, Sitzungs-Analyzer etc.) enthalten oder nicht enthalten sein sollen.
	Es kann nur ein Sicherheits-Officer im System zugewiesen werden. Nur ein Benutzer mit Superuser-Berechtigungen kann den Sicherheits-Officer erstmalig zuweisen. Nur der Sicherheits-Officer selbst kann diesen einem anderen Benutzer zuweisen oder sein eigenes Kennwort ändern, sobald dieses zugewiesen wurde. Weitere Informationen zu diesem Thema finden Sie unter "Sicherheits-Officer" auf Seite 252.
a	Ein konfigurierter Benutzer
	Eine konfigurierte Gruppe
1 8	Sicherheits-Officer
	Stammknoten

Dialogfeld "Gruppenzuordnungen"

In diesem Dialogfeld können Sie Gruppen, die in BSM konfiguriert sind, Gruppen zuordnen, die auf dem LDAP-Server konfiguriert sind.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus. Klicken Sie im Ausschnitt Gruppen/Benutzer auf die Schaltfläche LDAP-Konfiguration , und wählen Sie Gruppenzuordnungen aus.
	Das Dialogfeld Gruppenzuordnungen umfasst die folgenden Bereiche:
	Ausschnitt Unternehmensverzeichnis. Weitere Informationen finden Sie unter "Dialogfeld "Gruppenzuordnungen"".
	Ausschnitt "Lokales BSM-Repository für Remote-Gruppe: <gruppenname>". Weitere Informationen finden Sie unter "Dialogfeld "Gruppenzuordnungen"".</gruppenname>
	Zuweisungen zwischen lokalen Gruppen und Remote-Gruppe. Zeigt eine Tabelle der LDAP-Gruppen und der BSM-Gruppen an, denen sie zugewiesen sind. Die LDAP-Gruppen werden in der Spalte Name der Remote-Gruppe und die BSM-Gruppen in der Spalte Name der lokalen Gruppe angezeigt.

Wichtiger Hinweis

Hinweis: Dieses Dialogfeld ist nur verfügbar, wenn der LDAP-Modus im Assistenten für die Authentifizierung aktiviert wurde. Weitere Informationen finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Wenn Sie zwischen den LDAP-Servern wechseln, stellen Sie sicher, alle bestehenden Gruppenzuordnungen vom originalen LDAP-Server zu entfernen, bevor Sie eine Zuordnung neu erstellen.

Ausschnitt "Unternehmensverzeichnis"

In diesem Ausschnitt können Sie BSM-Gruppen zu LDAP-Gruppen zuweisen und die Benutzer in den LDAP-Gruppen auflisten.

Beschreibung	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen aus; klicken Sie im Ausschnitt Gruppen/Benutzer auf die Schaltfläche LDAP-Konfiguration , und wählen Sie Gruppenzuordnungen aus.
Wichtiger Hinweis	Zum Synchronisieren der LDAP-Gruppen mit BSM-Gruppen klicken Sie auf Gruppen zuweisen, um das Dialogfeld Wählt lokale Gruppen für die Remote-Gruppe aus zu öffnen.
	Um eine Liste der mit den jeweiligen LDAP-Gruppen verknüpften Benutzern anzuzeigen, klicken Sie auf Benutzer auflisten .
	Sie können diese Optionen auch auswählen, indem Sie mit der rechten Maustaste auf die Gruppe klicken.
	 Nachdem die LDAP-Gruppen den BSM-Gruppen zugeordnet wurden, können die BSM-Gruppen nur über die LDAP-Benutzeroberfläche verwaltet werden. Davon sind die folgenden Felder im Fenster Benutzer und Berechtigungen betroffen:
	■ Die Option Benutzer erstellen ist deaktiviert.
	■ Die Option Benutzername ist deaktiviert.
	 Das Feld Kennwort wird nicht angezeigt.
	 Die Registerkarte Hierarchie steht nur für Gruppen und nicht für Benutzer zur Verfügung.

Ausschnitt "Lokales BSM-Repository für Remote-Gruppe: <Gruppenname>"

In diesem Ausschnitt werden die Gruppen angezeigt, die der im Ausschnitt **Unternehmensverzeichnis** ausgewählten LDAP-Gruppe zugewiesen wurden. Sie können die zugewiesenen BSM-Gruppen entfernen.

Zugriff

Wählen Sie **Admin > Plattform > Benutzer und Berechtigungen** aus; klicken Sie im Ausschnitt **Gruppen/Benutzer** auf die Schaltfläche **LDAP-Konfiguration**

ibr, und wählen Sie Gruppenzuordnungen aus.

Wichtiger Hinweis

- Um Gruppen zu entfernen, wählen Sie die entsprechenden Gruppe aus und klicken auf **Gruppen entfernen**.
- Sie können mehrere Gruppen gleichzeitig entfernen, indem Sie die Strg-Schaltfläche beim Auswählen gedrückt halten.

Kapitel 19

Empfängerverwaltung

Sie können Empfänger Benutzern zuweisen. Eine Empfängerdefinition enthält Informationen darüber, wie mit dem Empfänger kommuniziert werden soll. Empfänger können ausgelöste Warnungen oder geplante Reports empfangen:

- Warnungen. Für jeden Empfänger können eine oder mehrere Benachrichtigungsmethoden (eine beliebige Kombination aus E-Mail, Pager und/oder SMS) sowie die Vorlage für Warnungsbenachrichtigungen festgelegt werden. Außerdem können Sie Warnungen so konfigurieren, dass bestimmte Empfänger über die Warnungen informiert werden, wenn diese ausgelöst werden. Weitere Informationen zu Warnungen finden Sie unter "Einrichten eines Bereitstellungssystems für Warnungen" auf Seite 441.
- Geplante Reports. Sie können im Report Manager auch die geplanten Intervalle konfigurieren, in denen Empfänger Reports oder Reportelemente erhalten. Es können nur die Empfänger für den Empfang geplanter Reports ausgewählt werden, die für den Empfang von E-Mails konfiguriert wurden. Diese Empfänger sind beim Konfigurieren geplanter Reports in der Liste Verfügbare Empfänger aufgeführt. Weitere Informationen zu geplanten Reports finden Sie unter "Report Schedule Manager" auf Seite 438.

Weitere Details zum Konfigurieren und Verwalten von Empfängern finden Sie unter "Seite "Empfänger" auf Seite 362.

Konfigurieren und Verwalten von Empfängern

In dieser Aufgabe wird die empfohlene Vorgehensweise zum Verwalten von Empfängern beschrieben.

Sie erstellen Empfänger, indem Sie eine oder mehrere Benachrichtigungsmethoden, die für Warnungsbenachrichtigungen verwendete Vorlage und einen Benachrichtigungszeitplan für den Empfang von Reports definieren. Sie erstellen Empfänger und verwalten vorhandene Empfänger auf der Seite **Empfänger**. Informationen zur Benutzeroberfläche finden Sie unter "Seite "Empfänger" auf Seite 362.

Sie können Empfänger auch beim Konfigurieren von Benutzern erstellen. Diese Empfänger werden der Empfängerliste auf der Seite **Empfänger** unter **Admin > Plattform > Empfänger > Empfängerverwaltung** automatisch hinzugefügt.

Die Empfänger, die Sie auf der Seite **Empfänger** erstellen, werden automatisch als verfügbare Empfänger angezeigt, wenn Sie Benutzer unter **Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung** konfigurieren.

Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS

Wenn Sie Warnungen konfigurieren, die per Pager oder SMS gesendet werden sollen, und Ihr Pager- oder SMS-Serviceprovider in der Liste der Standardanbieter nicht aufgeführt ist, können Sie den Anbieter manuell zu BSM hinzufügen, wenn er ein E-Mail-Gateway verwendet. Anschließend wird der Anbieter in der Liste aufgeführt.

Um einen Anbieter hinzuzufügen, der ein E-Mail-Gateway verwendet, geben Sie die Gateway-Informationen manuell in die Verwaltungsdatenbank ein. Wenden Sie sich an den Datenbankadministrator, wenn Sie Hilfe benötigen.

So fügen Sie einen Anbieter hinzu, der ein E-Mail-Gateway verwendet:

- Öffnen Sie die Tabelle NOTIFICATION_PROVIDERS in der Verwaltungsdatenbank.
- 2. Fügen Sie in der Spalte **NP_NOTIFICATION_PROVIDER_NAME** den Namen des Anbieters unten in der Liste ein.

Fügen Sie den Namen genau so hinzu, wie er in der Anbieterliste angezeigt werden soll, die in der Registerkarte **SMS** des Assistenten für die Empfängereigenschaften geöffnet wird. Details finden Sie unter "Registerkarte "SMS"" auf Seite 372.

Beachten Sie die ID-Nummer, die dem Anbieter automatisch zugewiesen wird.

- Schließen Sie die Tabelle NOTIFICATION_PROVIDERS und öffnen Sie die Tabelle NOTIFPROVIDER_NOTIFTYPE.
- 4. Fügen Sie in der Spalte **NN_NOTIF_PROVIDER_ID** die ID-Nummer hinzu, die dem neuen Anbieter zugewiesen wurde.
- 5. Fügen Sie dem Anbieter in der Spalte **NN_NOTIF_TYPE_ID** einen der folgenden Benachrichtigungstypen hinzu:
 - 102 für Pager-Dienstanbieter
 - 101 für SMS-Dienstanbieter
- 6. Schließen Sie die Tabelle **NOTIFPROVIDER_NOTIFTYPE** und öffnen Sie die Tabelle **NOTIFICATION_PROVIDER_PROP**.
- 7. Fügen Sie in der Spalte **NPP_NOTIFICATION_PROVIDER_ID** die ID-Nummer hinzu, die dem neuen Anbieter zugewiesen wurde.

Achten Sie darauf, dass Sie die ID-Nummer in zwei aufeinanderfolgenden Zeilen hinzufügen.

 Fügen Sie in den Spalten NPP_NPROVIDER_PROP_NAME und NPP_NPROVIDER_ PROP_VALUE die folgenden neuen Eigenschaftsnamen und -werte für den Anbieter untereinander hinzu (Beispiele finden Sie in den bestehenden Einträgen):

Eigenschaftenname	Eigenschaftenwert	Beschreibung
EMAIL_SUFFIX	<e_mail_suffix></e_mail_suffix>	Das E-Mail-Suffix des Gateways. Wenn die E-Mail-Adresse des Gateways beispielsweise 12345@xyz.com lautet, geben Sie xyz.com als Eigenschaftenwert für EMAIL_SUFFIX an.
EMAIL_MAX_LEN	<max_länge></max_länge>	Die maximale Textlänge der E-Mail-Nachricht in Zeichen. Beispiel: 500. Wenn Sie diesen Wert festlegen, beachten Sie die maximale Länge, die durch den Dienstanbieter limitiert wird, sowie die Vorgaben Ihres Pagers oder Mobiltelefons.

- 9. Geben Sie in der Spalte NPP_NPROVIDER_PROP_DATATYPE_ID wie folgt einen ID-Wert an:
 - Für EMAIL_SUFFIX: 1
 - Für EMAIL_MAX_LEN: 2
- 10. Starten Sie BSM erneut.

Empfängerverwaltung - Benutzeroberfläche

Dieser Abschnitt umfasst die folgenden Themen:

- "Dialogfeld "Benutzer an Empfänger anhängen""
- "Seite "Empfänger""
- "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"" auf Seite 364

Dialogfeld "Benutzer an Empfänger anhängen"

In diesem Dialogfeld können Sie den Benutzer auswählen, den Sie dem ausgewählten Empfänger anhängen möchten.

Zugriff	Wählen Sie die Registerkarte Admin > Plattform > Empfänger > Empfängerverwaltung. Wählen Sie einen Empfänger aus der Tabelle aus und klicken Sie auf der Seite Empfänger auf die Schaltfläche Benutzer an ausgewählten Empfänger anhängen	
Siehe auch	"Gruppen- und Benutzerhierarchie" auf Seite 254	

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Benutzeranmeldung	Der Name, der für die Anmeldung an BSM verwendet wird.
Benutzername	Der Name des Benutzers, wie auf der Seite Benutzerverwaltung konfiguriert.
Auswählen	Um einen Benutzer zum ausgewählten Empfänger zuzuweisen, wählen Sie den Benutzer aus und klicken Sie auf Auswählen .

Seite "Empfänger"

Ermöglicht Ihnen das Erstellen oder Bearbeiten von Empfängerinformationen, einschließlich des entsprechenden Benutzers und der E-Mail-, SMS- und Pager-Informationen. Falls Sie über die entsprechenden Berechtigungen verfügen, können Sie den aktuellen Empfänger auch vom Benutzer trennen, den Benutzer mit vorhandenen Empfängern verbinden oder den verbundenen Empfänger löschen.

Zugriff	Wählen Sie Admin > Plattform > Empfänger > Empfängerverwaltung.
---------	---

Wichtiger Hinweis	Wie Sie auf die Seite Empfänger zugreifen und was auf der Seite angezeigt wird, hängt von Ihren Benutzerberechtigungen ab. Details finden Sie unter "Registerkarte "Berechtigungen" (Benutzerverwaltung)" auf Seite 346.	
	Zum Filtern der in der Tabelle angezeigten Informationen geben Sie die Zeichenfolge oben in die entsprechende Spalte ein und drücken die EINGABETASTE. Es werden nur die entsprechenden Tabellenzeilen angezeigt. Löschen Sie zum Zurücksetzen des Filters die zum Filtern der Informationen verwendete Zeichenfolge und drücken Sie die EINGABETASTE.	
	Zwischen Benutzer und Empfänger besteht eine 1:1-Beziehung: Ein Empfänger kann einem oder keinem Benutzer zugewiesen sein und ein Benutzer kann eine Verbindung zu einem oder keinem Empfänger haben.	
Relevante Aufgaben	, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	
Siehe auch	"Empfängerverwaltung" auf Seite 358	

Elemente der Oberfläche	Beschreibung
*	Neuen Empfänger hinzufügen. Öffnet das Dialogfeld Neuer Empfänger. Details finden Sie unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"" auf der nächsten Seite.
0	Ausgewählten Empfänger bearbeiten. Öffnet das Dialogfeld Empfänger bearbeiten. Details finden Sie unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten" auf der nächsten Seite.
×	Den an Benutzer angehängten Empfänger löschen. Trennt den Empfänger vom Benutzer und löscht den aktuellen Empfänger.
100 to 10	Benutzer an ausgewählten Empfänger anhängen. Wählen Sie einen Empfänger in der Liste aus und klicken Sie auf diese Schaltfläche, um das Dialogfeld Benutzer an Empfänger anhängen zu öffnen, in dem Sie den entsprechenden Benutzer auswählen können. Details finden Sie unter "Dialogfeld "Benutzer an Empfänger anhängen"" auf der vorherigen Seite.
4	Benutzer von ausgewählten Empfängern trennen. Trennt den aktuellen Empfänger vom entsprechenden (auf der Seite aufgelisteten) Benutzer. Es wird eine Bestätigungsmeldung angezeigt.
8	E-Mail-Adresse der ausgewählten Empfänger aus LDAP aktualisieren. Dieses Symbol wird nur angezeigt, wenn LDAP mit der BSM-Applikation verbunden ist. Klicken Sie hier, um die Benutzerdaten zu synchronisieren, sodass die im Benutzerrepository für den jeweiligen Benutzer gespeicherten E-Mail-Informationen die E-Mail-Empfängerinformationen entsprechend dem mit dem Empfänger verknüpften Benutzer aktualisieren.

Elemente der Oberfläche	Beschreibung	
E-Mail	Die auf der Registerkarte Allgemein angegebene E-Mail-Adresse des Empfängers.	
Verknüpfter	Der Name des mit dem Empfänger verknüpften Benutzers.	
Benutzer	Wichtig: Darf 49 Zeichen nicht überschreiten.	
	Syntaxausnahmen: Folgende Zeichen werden nicht unterstützt: `~!@#\$%^&*-+=[]{}\ /?.,"':;<>	
Pager	Die Pager-Nummern des Empfängers.	
	Syntaxausnahmen:	
	Folgende Zeichen werden nicht unterstützt: @ & " '	
	• Folgende Zeichen sind nicht zulässig: () + = [] { } : ; < > . ,	
Empfängername	Der Name des Empfängers.	
	Wichtig: Darf 49 Zeichen nicht überschreiten.	
	Syntaxausnahmen: Folgende Zeichen werden nicht unterstützt: `~!@#\$%^&*-+=[]{}\ /?.,"':;<>	
SMS	Die SMS-Nummern des Empfängers.	
	Syntaxausnahmen:	
	Folgende Zeichen werden nicht unterstützt: @ & " '	
	• Folgende Zeichen sind nicht zulässig: () + = [] { } : ; < > . ,	

Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"

Auf dieser Seite können Sie Empfänger, deren E-Mail-, Pager- und SMS-Informationen sowie die Vorlage definieren, die zum Senden von Warnungsbenachrichtigungen an diese Empfänger verwendet werden soll.

Zugriff	Sie können auch auf folgende Weise auf diese Seite zugreifen:	
	Wählen Sie Admin > Plattform > Empfänger > Empfängerverwaltung und	
	klicken Sie auf 🍍.	
	 Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung, wählen Sie einen Benutzer aus und klicken Sie auf die Registerkarte Empfänger. 	
	Wählen Sie Admin > Persönliche Einstellungen > Empfänger.	
	 Klicken Sie im Assistenten zum Erstellen einer neuen Warnung für CI- Statuswarnungen auf der Seite Vorlagen und Empfänger auf die Schaltfläche Neuer Empfänger. Weitere Informationen finden Sie unter "Templates and Recipients Page" im BSM-Benutzerhandbuch. 	
	 Klicken Sie im Assistenten zum Erstellen einer neuen Warnung für SLA- Warnungen auf der Seite Vorlagen und Empfänger auf die Schaltfläche Neuer Empfänger. Weitere Informationen finden Sie unter "Templates and Recipients Page" im BSM-Benutzerhandbuch. 	
	Klicken Sie im Dialogfeld Empfänger anhängen für ereignisbasierte Warnungen auf die Schaltfläche Empfänger erstellen . Weitere Informationen finden Sie unter "Attach Recipients Dialog Box" im BSM-Benutzerhandbuch.	
	Klicken Sie auf die Schaltfläche Neuer Empfänger auf der Hauptseite des Report Manager. Weitere Informationen finden Sie unter "Report Manager Main Page" im BSM-Benutzerhandbuch.	
Wichtiger Hinweis	Wie Sie auf die Seite Empfänger zugreifen und was auf der Seite angezeigt wird, hängt von den Berechtigungen des Benutzers ab. Details finden Sie unter "Registerkarte "Berechtigungen" (Benutzerverwaltung)" auf Seite 346.	
	Zwischen Benutzer und Empfänger besteht eine 1:1-Beziehung: Ein Empfänger kann einem oder keinem Benutzer zugewiesen sein und ein Benutzer kann eine Verbindung zu einem oder keinem Empfänger haben.	
Relevante Aufgaben	"Konfigurieren und Verwalten von Empfängern" auf Seite 359	
Siehe auch	"Empfängerverwaltung" auf Seite 358	

Elemente der Oberfläche	Beschreibung
№	Benutzer an ausgewählten Empfänger anhängen. Wählen Sie einen Empfänger in der Liste aus und klicken Sie auf diese Schaltfläche, um das Dialogfeld Benutzer an Empfänger anhängen zu öffnen, in dem Sie den entsprechenden Benutzer auswählen können. Details finden Sie unter "Dialogfeld "Benutzer an Empfänger anhängen"" auf Seite 362.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie über Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung auf das Dialogfeld zugreifen.
	Benutzer von ausgewählten Empfängern trennen. Trennt den aktuellen Empfänger vom entsprechenden (auf der Seite aufgelisteten) Benutzer. Es wird eine Bestätigungsmeldung angezeigt.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie über Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung auf das Dialogfeld zugreifen.
×	Den an Benutzer angehängten Empfänger löschen. Trennt den Empfänger vom Benutzer und löscht den Empfänger.
	Hinweis: Diese Schaltfläche wird nur angezeigt, wenn Sie über Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung auf das Dialogfeld zugreifen.
₩	E-Mail-Adresse der ausgewählten Empfänger aus LDAP aktualisieren. Dieses Symbol wird nur angezeigt, wenn LDAP mit der BSM-Applikation verbunden ist. Klicken Sie hier, um die Benutzerdaten zu synchronisieren, sodass die im Benutzerrepository für den jeweiligen Benutzer gespeicherten E-Mail-Informationen die E-Mail-Empfängerinformationen entsprechend dem mit dem Empfänger verknüpften Benutzer aktualisieren.

Elemente der Oberfläche	Beschreibung
EUM- Warnungsbenachrichtigungsvorlage	Wählen Sie die Vorlage, die Sie für die EUM- Warnungsbenachrichtigung verwenden wollen, oder eine bereits erstellte Vorlage aus.
	Hinweis: Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage in den Registerkarten für E-Mail, Pager oder SMS ändern, ändert sich der Zeitplan für Erhalt von Benachrichtigungen in Gemischter Wert. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite erneut ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen, und die Schaltfläche Gemischter Wert wird deaktiviert.
	Weitere Informationen zu EUM- Warnungsbenachrichtigungsvorlagen und zum Erstellen benutzerdefinierter Vorlagen finden Sie unter "Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 464.
	Hinweis: Dieses Feld ist nur für ereignisbasierte Warnungen relevant.
	Weitere Informationen zu Benachrichtigungsvorlagen und zum Erstellen benutzerdefinierter Vorlagen finden Sie unter "Seite "Benachrichtigungsvorlagen"" auf Seite 470.
	Hinweis:
	Der Standardwert lautet LONG.
	Weitere Informationen zu den in den jeweiligen Vorlagen angezeigten Parametern finden Sie unter "Registerkarte "Pager"" auf Seite 374.
	Das Feld listet die Standardvorlagen und benutzerdefinierten Vorlagen auf.
	Sie müssen die Warnungsbenachrichtigungsvorlage auswählen und einen Benachrichtigungszeitplan für Warnungsempfänger angeben. Sie müssen diese Verfahren nicht für Empfänger durchführen, die nur geplante Reports erhalten.

Elemente der Oberfläche	Beschreibung
Link zu Benutzer	Dieses Feld wird nur angezeigt, wenn Sie wie folgt auf diese Seite zugreifen:
	 Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung, wählen Sie in der Struktur einen Benutzer aus und klicken Sie auf die Registerkarte Empfänger. Admin > Persönliche Einstellungen > Empfänger.
Empfängername	Der Name des Empfängers.
	Wichtig: Darf 49 Zeichen nicht überschreiten.
	Syntaxausnahme: Folgende Zeichen werden nicht unterstützt: `~!@#\$%^&*-+[]{}\ /?"'<>

Elemente der Oberfläche	Beschreibung
Zeitplan für Erhalt von Benachrichtigungen	Aktiviert, wenn Sie die Zeitplanoption Pro Benachrichtigungsmethode für den Empfänger unter Zeitplan für Erhalt von Benachrichtigungen auf der Registerkarte Allgemein ausgewählt haben.
	Wählen Sie Folgendes aus:
	Gemischter Wert. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage in den Registerkarten für E-Mail, Pager oder SMS ändern, ändert sich der Zeitplan für Erhalt von Benachrichtigungen in Gemischter Wert. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite erneut ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen, und die Schaltfläche Gemischter Wert wird deaktiviert.
	Ganztägig. Wenn der Empfänger E-Mail- Nachrichten ganztägig erhalten soll.
	Von bis. Wenn der Empfänger E-Mail- Nachrichten während des angegebenen Zeitraums erhalten soll.
	Der Zeitraum wird auf der Grundlage des für den Empfänger ausgewählten GMT-Offsets berechnet.
	Geplante Reports werden nach dem Zeitplan gesendet, der auf der Seite Geplante Reports konfiguriert wurde, nicht nach dem Zeitplan, der für den Empfänger konfiguriert wurde. Weitere Informationen finden Sie unter "How to Schedule a Report" im BSM-Benutzerhandbuch.

Elemente der Oberfläche	Beschreibung
Zeitzone	Wählen Sie die Zeitzone für den Empfänger aus Business Service Management verwendet die Zeitzone zum Senden von Warnungsbenachrichtigungen und HP Software-as-a- Service-Benachrichtigungen an den ausgewählten Empfänger.
	Hinweis:
	Bei der für den Empfänger ausgewählten Zeitzone handelt es sich um die Zeitzone, die in den Warnungsbenachrichtigungen an den Empfänger enthalten ist. Wird beispielsweise irgendwo in der Welt eine Warnung ausgelöst und eine Benachrichtigung gesendet, werden Datum und Uhrzeit der Warnung in die Ortszeit des Empfängers konvertiert. Die Warnung gibt auch den GMT-Offset des Empfängers an.
	Wenn Sie einen Benachrichtigungszeitplan für den Empfänger definiert haben, entspricht die für den Empfänger ausgewählte Zeitzone auch der Zeitzone, die BSM zur Berechnung des Zeitpunkts verwendet, an dem die Empfängerbenachrichtigungen gesendet werden. Wenn Sie beispielsweise konfigurieren, dass ein Empfänger von 9:00 bis 21:00 Uhr Pager-Warnungen erhalten soll und einen GMT-Offset von -5 Stunden auswählen, erhält der Empfänger nur zwischen 9:00 und 21:00 Uhr ostamerikanischer Zeit (EST) Warnungen über einen Pager.
	Geplante Reports werden nach dem Zeitplan gesendet, der auf der Seite Geplante Reports konfiguriert wurde, nicht nach dem Zeitplan, der für den Empfänger konfiguriert wurde. Weitere Informationen finden Sie unter "How to Schedule a Report" im BSM-Benutzerhandbuch.
	Wenn Sie die Zeitzone des Benutzers ändern, dem der Empfänger zugewiesen wird, wird eine Bestätigungsnachrichtung ausgegeben, um zu überprüfen, ob Sie die Zeitzonenänderung auch an den GMT-Offset des Empfängers weitergeben wollen. Wenn Sie den GMT-Offset des Empfängers ändern, ist die Zeitzone des Benutzers, dem der Empfänger zugewiesen ist, nicht betroffen.

Bereich "Kommunikationsmethode"

Wichtiger Hinweis	Dieser Bereich umfasst die folgenden Registerkarten:	
	"Registerkarte "E-Mail""	
	"Registerkarte "SMS"" auf der nächsten Seite	
	"Registerkarte "Pager"" auf Seite 374	

Registerkarte "E-Mail"

Diese Registerkarte bietet Ihnen die Möglichkeit, mehrere E-Mail-Adressen für den Empfänger und den Benachrichtigungsvorlage festzulegen, die die auf globaler Ebene in der Seite ausgewählte Benachrichtigungsvorlage überschreibt. Des Weiteren können Sie den Zeitplan für das Senden von E-Mail-Benachrichtigungen und ggf. das Sicherheitszertifikat festlegen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung und in der Struktur einen Benutzer aus und klicken Sie auf die Registerkarte Empfänger. Klicken Sie im Bereich Kommunikationsmethode für den Benutzer auf die Registerkarte E-Mail.
Wichtiger Hinweis	Es können nur die Empfänger für den Empfang geplanter Reports ausgewählt werden, die für den Empfang von E-Mails konfiguriert wurden und beim Konfigurieren geplanter Reports unter Verfügbare Empfänger aufgeführt sind. Hinweis: Der in E-Mail-Nachrichten angezeigte Text darf nur aus lateinischen Zeichen bestehen, mit Ausnahme des Inhalts in Feldern, die vom Benutzer
	eingefügt wurden. Dieser kann aus jeder unterstützten und relevanten Sprache bestehen. Diese Felder können beispielsweise den Warnungsnamen, die Warnungsbeschreibung und den KPI-Namen enthalten.

Elemente der Oberfläche	Beschreibung
E-Mail-Adressen	Geben Sie eine oder mehrere E-Mail-Adressen ein. Mehrere Einträge werden durch ein Semikolon (;) getrennt.

Elemente der Oberfläche	Beschreibung
Sichere E-Mails aktivieren	Wählen Sie diese Option aus, wenn der Empfänger verschlüsselte E-Mail empfangen soll. Sie müssen den Inhalt des Zertifikats, das der Empfängern zum Sichern eingehender E-Mail-Nachrichten verwendet, dann in das Textfeld unterhalb dieser Option eingeben.
	Hinweis:
	Die Option für verschlüsselte E-Mail wird nur für Warnungen unterstützt. Verschlüsselte E-Mail wird nicht für geplante Reports oder Abonnement- Benachrichtigungen unterstützt (nur HP Software- as-a-Service-Kunden).
	Die Option für verschlüsselte E-Mail wird nur unterstützt, wenn der BSM- Datenverarbeitungsserver auf einem Windows- Computer installiert ist.
EUM- Warnungsbenachrichtigungsvorlage	Wählen Sie die Vorlage aus, die Sie verwenden möchten. Details finden Sie unter "Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 462.
	Hinweis: Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage in den Registerkarten für E-Mail, Pager oder SMS ändern, ändert sich der Zeitplan für Erhalt von Benachrichtigungen in Gemischter Wert. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite erneut ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen und die Option Gemischter Wert wird deaktiviert.
Zeitplan für Erhalt von E-Mail- Nachrichten	Wählen Sie den Zeitplan aus, den Sie für den Erhalt von E-Mails verwenden möchten. Details finden Sie unter Zeitplan für Erhalt von Benachrichtigungen unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"" auf Seite 364.

Registerkarte "SMS"

Diese Registerkarte bietet Ihnen die Möglichkeit, den SMS-Dienstanbieter (Short Message Service), die SMS-Nummern und den Typ der Benachrichtigungsvorlage festzulegen, die die auf

globaler Ebene in der Seite ausgewählte Benachrichtigungsvorlage überschreibt. Des Weiteren können Sie den Zeitplan für das Senden von Warnungsbenachrichtigungen per SMS definieren.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung und in der Struktur einen Benutzer aus und klicken Sie auf die Registerkarte Empfänger. Klicken Sie im Bereich Kommunikationsmethode für den Benutzer auf die Registerkarte SMS.
Wichtiger Hinweis	SMS ist ein Dienst zur Textübermittlung, der von den meisten Anbietern GSM- basierter Mobiltelefone bereitgestellt wird. SMS-Nachrichten sind nützlich, um mobile Mitarbeiter oder Mitarbeiter ohne E-Mail- oder Pager-Zugriff zu benachrichtigen. Beachten Sie, dass die maximale Länge von SMS- Textnachrichten im Allgemeinen 160 Zeichen beträgt.
	Hinweis: Sie können einen Pager- oder SMS-Dienstanbieter verwenden, der nicht in der Standardliste angezeigt wird. Details finden Sie unter "Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS" auf Seite 360.

Elemente der Oberfläche	Beschreibung
EUM- Warnungsbenachrichtigungsvorlage	Wählen Sie die Vorlage aus, die Sie verwenden möchten. Details finden Sie unter "Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 462.
	Hinweis: Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage in den Registerkarten für E-Mail, Pager oder SMS ändern, ändert sich der Zeitplan für Erhalt von Benachrichtigungen in Gemischter Wert. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite erneut ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen und die Option Gemischter Wert wird deaktiviert.

Elemente der Oberfläche	Beschreibung
Provider	Wählen Sie in der Liste einen SMS-Dienstanbieter aus:
	Genie-UK
	• Itineris
	SFR-France
	GoSMS-Israel
	MtnSMS-Global
	Hinweis: Wenn Ihr Anbieter in der Liste der Standardanbieter nicht aufgeführt ist und der Anbieter ein E-Mail-Gateway verwendet, können Sie Ihren Anbieter manuell zu BSM hinzufügen. Details finden Sie unter "Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS" auf Seite 360.
Zeitplan für Erhalt von SMS- Nachrichten	Wählen Sie den Zeitplan aus, den Sie für den Erhalt von SMS-Textnachrichten verwenden möchten. Details finden Sie unter Zeitplan für Erhalt von Benachrichtigungen unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten"" auf Seite 364.
SMS-Nummern	Geben Sie in das Feld eine oder mehrere Nummern für den SMS-Zugriff ein. Mehrere Einträge werden durch ein Semikolon (;) getrennt.

Registerkarte "Pager"

Diese Registerkarte bietet Ihnen die Möglichkeit, den Pager-Dienstanbieter, die Pager-Nummern und den Typ der Benachrichtigungsvorlage festzulegen, die die auf globaler Ebene in der Seite ausgewählte Benachrichtigungsvorlage überschreibt. Des Weiteren können Sie den Zeitplan für das Senden von Warnungsbenachrichtigungen per Pager definieren.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung und in der Struktur einen Benutzer aus und klicken Sie auf die Registerkarte Empfänger. Klicken Sie im Bereich Kommunikationsmethode für den Benutzer auf die Registerkarte Pager.
Wichtiger Hinweis	Sie können einen Pager verwenden, der nicht in der Standardliste angezeigt wird. Details finden Sie unter "Hinzufügen eines benutzerdefinierten Dienstanbieters für Pager oder SMS" auf Seite 360.
	Hinweis: Der in Pager-Nachrichten angezeigte Text darf nur aus lateinischen Zeichen bestehen, mit Ausnahme des Inhalts in Feldern, die vom Benutzer eingefügt wurden. Dieser kann aus jeder unterstützten und relevanten Sprache bestehen. Diese Felder können beispielsweise den Warnungsnamen, die Warnungsbeschreibung und den KPI-Namen enthalten.

Elemente der Oberfläche	Beschreibung
EUM- Warnungsbenachrichtigungsvorlage	Wählen Sie die Vorlage aus, die Sie verwenden möchten. Details finden Sie unter "Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 462.
	Hinweis: Wenn Sie die Auswahl im Feld EUM- Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen. Wenn Sie die Auswahl im Feld EUM-Warnungsbenachrichtigungsvorlage in den Registerkarten für E-Mail, Pager oder SMS ändern, ändert sich der Zeitplan für Erhalt von Benachrichtigungen in Gemischter Wert. Wenn Sie die Auswahl im Feld EUM- Warnungsbenachrichtigungsvorlage im oberen Bereich der Seite erneut ändern, werden die Änderungen in die Registerkarten für E-Mail, Pager und SMS auf derselben Seite übertragen und die Option Gemischter Wert wird deaktiviert.
Pager-Nummern	Geben Sie eine oder mehrere Pager-Zugriffsnummern ein. Mehrere Einträge werden durch ein Semikolon (;) getrennt.
	Hinweis: Falls Ihr Pager ausschließlich numerisch ist, können Sie beim Erstellen eines Warnungsschemas im Assistenten für Warnung nur eine numerische Benutzernachricht eingeben.
Zeitplan für Erhalt von Pager- Benachrichtigungen:	Wählen Sie den Zeitplan aus, den Sie für den Erhalt von Pager-Nachrichten verwenden möchten. Details finden Sie unter Zeitplan für Erhalt von Benachrichtigungen unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten" auf Seite 364.

Elemente der Oberfläche	Beschreibung
Тур	Wählen Sie den Pager-Dienstanbieter aus. Folgende Anbieter werden unterstützt:
	MetroCall
	• Arch
	AirTouch
	PageMci
	• SkyTel
	• PageNet
	• PageMart
	AmeriPage
	Nextel
	PageOne

Standardbenachrichtigungsvorlagen

Wichtiger Hinweis	Mit jeder Vorlage können Sie in der Benachrichtigung ausgewählte Informationen anzeigen, die den jeweiligen Parametern entspricht.
	Weitere Informationen zu den in den jeweiligen Vorlagen angezeigten Parametern finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf Seite 466.

Folgende Standardbenachrichtigungsvorlagen stehen zur Verfügung:

Elemente der Oberfläche	Beschreibung
DEFAULT_ LOG_ FORMAT	Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format für Reports erforderlich sind.
DEFAULT_ POSITIVE_ FORMAT	Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format für positive oder Nachverfolgungswarnungen erforderlich sind. Details zu Nachverfolgungswarnungen finden Sie unter "Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf Seite 465.
LONG	Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format erforderlich sind.
SHORT	Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im kurzen Format erforderlich sind.

Kapitel 20

Persönliche Einstellungen

Mit den persönlichen Einstellungen kann die Darstellung von Informationen in BSM je nach Benutzer angepasst werden.

Die Benutzer können ihre persönlichen Einstellungen konfigurieren, um das benutzerspezifische Verhalten von BSM anzupassen.

Auf der Registerkarte Persönliche Einstellungen stehen folgende Optionen zur Verfügung:

- Allgemeine Einstellungen. Details finden Sie unter "Benutzerkonto" unten.
- Menüanpassung. Details finden Sie unter "Menüanpassung" unten.

Benutzerkonto

Auf der Registerkarte **Allgemeine Einstellungen** können Sie folgende persönliche Einstellungen konfigurieren.

- Benutzername
- Benutzermodus
- Zeitzone f
 ür die Anzeige von Reports
- Kennwort
- · Aktualisierungsrate von Reports
- Benutzerdefinierte Menüelemente

Informationen zur Benutzeroberfläche zum Ändern des Kennworts und Aktualisieren anderer persönlicher Einstellungen finden Sie unter "Seite "Benutzerkonto" auf Seite 382.

Menüanpassung

Auf der Registerkarte **Menüanpassung** haben Sie folgende Möglichkeiten:

- Festlegen des Standardkontexts, der angezeigt wird, wenn Sie sich bei BSM anmelden
- Festlegen der ersten Seite, die in den verschiedenen Bereichen von BSM angezeigt wird
- Festlegen der Registerkarten und Optionen, die auf den Seiten in BSM zur Verfügung stehen

Durch das Anpassen der Eingangsseite, der Menüelemente und der Registerkarten können Sie die Benutzeroberfläche so einstellen, dass Sie nur die Bereiche von BSM sehen, die relevant für Sie sind. Weitere Informationen zur Benutzeroberfläche für Menüanpassungen finden Sie unter "Seite "Menüanpassung" auf Seite 383.

Anpassen der BSM-Menüs und -Seiten – Workflow

In dieser Aufgabe wird beschrieben, wie Sie die Seite anpassen, die beim Aufrufen von BSM angezeigt wird, und wie Sie die Menüelemente auswählen, die auf den Seiten von BSM zur Verfügung stehen sollen.

Tipp: Ein fallspezifisches Szenario für diese Aufgabe finden Sie unter "Anpassen der BSM-Menüs und -Seiten – Fallspezifisches Szenario" auf der nächsten Seite.

1. Zuweisen eines Standardkontexts

Wählen Sie aus dem Ausschnitt **Kontext** einen Kontext, der als standardmäßiger Eingangskontext angezeigt werden soll, wenn Sie sich bei BSM anmelden, und klicken Sie auf **Als standardmäßigen Eingangskontext festlegen**. Informationen zur Benutzeroberfläche finden Sie unter "Seite "Menüanpassung" auf Seite 383.

2. Auswählen von Kontextseiten und Registerkarten

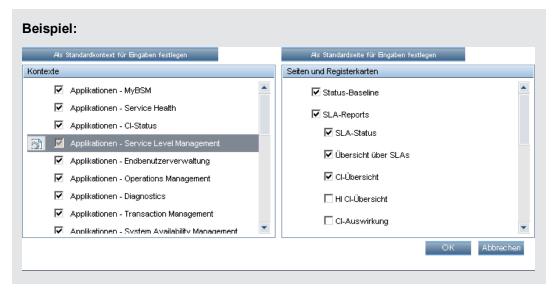
Wählen Sie im Ausschnitt **Seiten und Registerkarten** den Kontext der Seiten und Registerkarten aus, der im ausgewählten Kontext für den Benutzer sichtbar sein soll. Deaktivieren Sie die Kontrollkästchen der Seiten und Registerkarten, die dem Benutzer nicht angezeigt werden sollen.

3. Zuweisen einer standardmäßigen Eingangsseite

Wählen Sie eine Seite oder Registerkarte aus, die als standardmäßige Eingangsseite für den ausgewählten Kontext verwendet werden soll, und klicken Sie auf **Als standardmäßige Eingangsseite festlegen**.

4. Ergebnisse

Neben dem standardmäßigen Eingangskontext und der standardmäßigen Eingangsseite wird ein entsprechendes Symbol angezeigt. Die für den Benutzer sichtbaren Seiten und Registerkarten sind im Ausschnitt **Seiten und Registerkarten** ausgewählt. Die für den Benutzer nicht sichtbaren Seiten und Registerkarten sind im Ausschnitt **Seiten und Registerkarten** nicht ausgewählt.



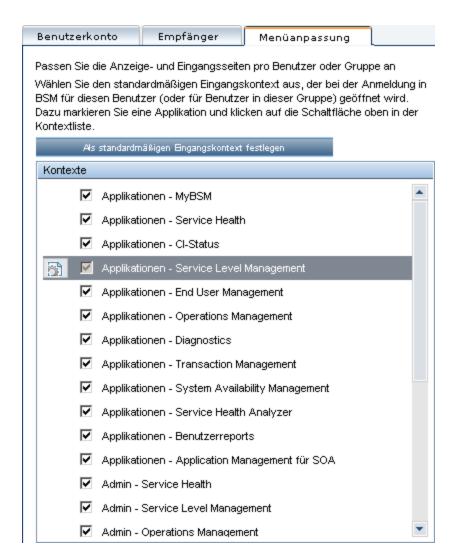
Anpassen der BSM-Menüs und -Seiten – Fallspezifisches Szenario

In diesem fallspezifischen Szenario wird beschrieben, wie Sie Benutzermenüs für einzelne Benutzer anpassen.

Hinweis: Eine Aufgabe für dieses Szenario finden Sie unter "Anpassen der BSM-Menüs und - Seiten – Workflow" auf der vorherigen Seite.

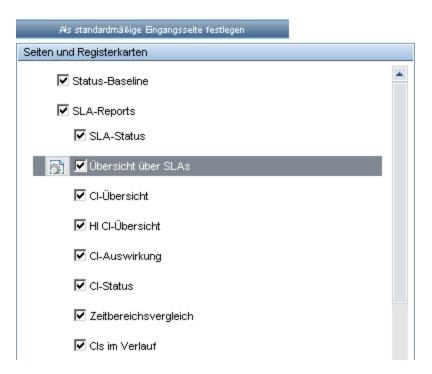
1. Zuweisen eines Standardkontexts

Karl Müller ist ein registrierter BSM-Benutzer des Versicherungsunternehmens ABC. Er möchte die Service Level Management-Applikationsoberfläche als Business Service Management-Standardkontext konfigurieren, der nach dem Anmelden angezeigt wird. Er navigiert zur Option Persönliche Einstellungen, indem er Admin > Persönliche Einstellungen auswählt, und wählt dann Menüanpassung, um die Seite Menüanpassung zu öffnen. Er wählt Applikationen – Service Level Management im Ausschnitt Kontexte aus und klickt auf Als standardmäßigen Eingangskontext festlegen. Die Option Applikationen – Service Level Management wird als standardmäßiger Eingangskontext angegeben:



2. Auswählen von Kontextseiten und Registerkarten

Karl Müller möchte nur die Seiten und Registerkarten angezeigt bekommen, die für seine Arbeit relevant sind, und er möchte den Report Übersicht über SLAs sofort nach dem Anmelden bei BSM sehen. Im Ausschnitt Seiten und Registerkarten deaktiviert er die Option SLA-Verwaltung, da die auf dieser Registerkarte angezeigten Informationen nicht relevant für seine Arbeit sind. Er wählt die Option Übersicht über SLAs aus und klickt auf Als standardmäßige Eingangsseite festlegen. Die Seite Übersicht über SLAs ist nun die standardmäßige Eingangsseite, die ihm nach dem Anmelden bei BSM angezeigt wird.



3. Ergebnisse

Der Kontext, der geöffnet wird, wenn Karl Müller sich bei BSM anmeldet, ist der Kontext **Service Level Management** im Menü **Applikationen**. Die Seite **Report mit SLA-Übersicht** wird auf der Registerkarte **SLA-Reports** angezeigt.



Persönliche Einstellungen – Benutzeroberfläche

Dieser Abschnitt umfasst die folgenden Themen:

- "Seite "Benutzerkonto"" unten
- "Seite "Menüanpassung"" auf der nächsten Seite
- "Registerkarte "Empfänger"" auf Seite 384

Seite "Benutzerkonto"

Auf dieser Seite können Sie den Benutzernamen, den Benutzermodus, die Zeitzone, das Kennwort und die Einstellungen der Aktualisierungsrate konfigurieren.

Zugriff	Wählen Sie Admin > Persönliche Einstellungen > Benutzerkonto.
	Hinweis: Auf die Registerkarte Persönliche Einstellungen können Sie auch zugreifen, indem Sie in der Standortübersicht auf Standardseite ändern klicken.
Wichtiger Hinweis	BSM speichert diese Einstellungen für den jeweils definierten Benutzer. Alle von Ihnen vorgenommenen Änderungen bleiben nur für diesen Benutzer für alle zukünftigen Websitzungen wirksam.
Siehe auch	"Persönliche Einstellungen" auf Seite 377

Elemente der Oberfläche	Beschreibung
Kennwort bestätigen	Geben Sie das Kennwort erneut ein, das Sie in das Feld Kennwort eingegeben haben.
Anmeldename	Der Name, der für die Anmeldung an BSM verwendet wird.
	Hinweis: Sie können die Eingabe in diesem Feld nicht ändern.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf BSM an.
Automatische Aktualisierungsrate auswählen	Wählen Sie die Rate aus, in der BSM den Browser automatisch aktualisieren und die neusten Daten aus der Datenbank laden soll. Hinweis: Diese Einstellung ist nur in der Zeitauflösung Vortag oder
	Letzte Stunde in Reports aktiv.
Zeitzone	Wählen Sie die entsprechende Zeitzone entsprechend dem Standort des Benutzers aus.

Elemente der Oberfläche	Beschreibung
Benutzermodus	Wählen Sie den Benutzermodus für den Benutzer aus den folgenden Optionen aus:
	Nicht angegeben. Der Benutzer befindet sich in keinem bestimmten Modus. Wählen Sie diese Option aus, wenn folgende Bedingungen erfüllt sind:
	 BSM arbeitet mit Benutzermodi und Sie möchten, dass dieser Benutzer KPIs für beide Modi in Service Health-Ansichten anzeigen können soll.
	 Ihr System arbeitet nicht mit Benutzermodi.
	Operationsbenutzer. Ermöglicht dem Benutzer das Anzeigen der Operationsversion von KPIs.
	Geschäftsbenutzer. Ermöglicht dem Benutzer das Anzeigen der Geschäftsversion von KPIs.
	Hinweis: Weitere Informationen zu Benutzermodi finden Sie unter "KPIs for User Modes" im BSM Application Administration Guide.
Benutzername	Der Benutzername für den Benutzer.
	Hinweise:
	Sie können maximal 50 Zeichen eingeben.
	• Zulässig sind alle Sonderzeichen außer den folgenden: "\/[]: <> +=;,?*% &

Seite "Menüanpassung"

Auf dieser Seite können Sie die Seiten für Anzeige und Eingang pro Benutzer anpassen. Sie können Folgendes festlegen:

- Den Standardkontext, der angezeigt wird, wenn Sie sich bei BSM anmelden
- Die erste Seite, die in den verschiedenen Bereichen von BSM angezeigt wird
- Die Registerkarten und Optionen, die auf den Seiten in BSM zur Verfügung stehen

Zugriff	Wählen Sie Admin > Persönliche Einstellungen > Menüanpassung
	Hinweis: Auf die Registerkarte Persönliche Einstellungen können Sie auch zugreifen, indem Sie in der Standortübersicht auf Standardseite ändern klicken.
Relevante Aufgaben	"Anpassen der BSM-Menüs und -Seiten – Workflow" auf Seite 378
Siehe auch	"Persönliche Einstellungen" auf Seite 377

Elemente der Oberfläche	Beschreibung
Kontexte	Wählen Sie einen BSM-Kontext aus. Sie können für den Kontext folgende Aktionen durchführen:
	Wählen Sie Seiten und Registerkarten im Bereich Seiten und Registerkarten aus, die für den angegebenen Benutzer sichtbar sein sollen.
	Klicken Sie auf die Schaltfläche Als standardmäßigen Eingangskontext festlegen, um den Kontext als Kontext festzulegen, der angezeigt wird, wenn sich der Benutzer bei BSM anmeldet.
Seiten und Registerkarten	Wählen Sie die Seiten und Registerkarten aus, die für den im Bereich Kontexte ausgewählten BSM-Kontext sichtbar sein sollen.
	Weisen Sie eine Seite oder Registerkarte als Standardseite zu, die für den im Bereich Kontexte ausgewählten Kontext geöffnet wird.
Als standardmäßigen Eingangskontext	Klicken Sie hier, um den im Bereich Kontexte ausgewählten Kontext als Eingangskontext festzulegen, der angezeigt wird, wenn sich der angegebene Benutzer bei BSM anmeldet.
festlegen	Hinweis: Das Symbol Standardmäßiger Eingangskontext wird neben dem angegebenen Kontext angezeigt.
Als standardmäßige Eingangsseite	Klicken Sie hier, um die angegebene Seite oder Registerkarte als Standardseite zuzuweisen, die für den im Bereich Kontexte ausgewählten Kontext geöffnet wird.
festlegen	Hinweis: Das Symbol Standardmäßige Eingangsseite wird neben der angegebenen Seite oder Registerkarte angezeigt.

Registerkarte "Empfänger"

Auf dieser Seite können Sie Empfänger, deren E-Mail-, Pager- und SMS-Informationen sowie die Vorlage definieren, die zum Senden von Warnungsbenachrichtigungen an diese Empfänger verwendet werden soll.

Informationen zur Benutzeroberfläche finden Sie unter "Dialogfeld "Neuer Empfänger/Empfänger bearbeiten" auf Seite 364.

Kapitel 21

Authentifizierungsstrategien

Die BSM-Authentifizierung basiert auf einem Konzept von Authentifizierungsstrategien. Bei jeder Strategie erfolgt die Authentifizierung über einen bestimmten Authentifizierungsdienst. Es kann jeweils nur ein Authentifizierungsdienst mit BSM konfiguriert werden.

Als Standardauthentifizierungsstrategie für die Anmeldung bei BSM wird der interne BSM-Authentifizierungsdienst verwendet. Sie geben Ihren Benutzernamen und Ihr Kennwort für BSM auf der Anmeldeseite ein. Ihre Anmeldeinformationen werden gespeichert und von der BSM-Datenbank überprüft. Eine Beschreibung des Authentifizierungsverfahrens in BSM finden Sie unter "BSM-Anmeldeablauf" auf Seite 26.

Sie können die Authentifizierung zur Verwendung von LDAP (Lightweight Directory Access Protocol) konfigurieren. BSM verwendet den LDAP-Server zum Überprüfen der Anmeldeinformationen eines Benutzers. Details zu LDAP finden Sie unter "LDAP-Authentifizierung und Zuordnung" auf Seite 417.

Die Authentifizierungsstrategien werden im Assistenten zur Verwaltung von Authentifizierungen konfiguriert. Weitere Informationen zum Assistenten zur Verwaltung von Authentifizierungen finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Einrichten einer Strategie für die SSO-Authentizierung

Bei SSO (Single Sign-On) handelt es sich um eine Methode zur Zugangskontrolle, bei der Benutzer nach einmaliger Anmeldung Zugriff auf die Ressourcen verschiedener Softwaresysteme erhalten, ohne dass sie sich erneut anmelden müssen. Die Applikationen innerhalb konfigurierten Gruppe von Softwaresystemen vertrauen der Authentifizierung und beim Wechsel von einer Applikation zu einer anderen ist keine weitere Authentifizierung mehr erforderlich.

Die Standardstrategie für die SSO-Authentifizierung für BSM ist Lightweight Single Sign-On (LW-SSO). LW-SSO ist in BSM eingebettet und erfordert keinen externen Computer für die Authentifizierung. Details zu LW-SSO finden Sie unter "LW-SSO-Strategie" auf Seite 404.

Wenn die außerhalb von BSM konfigurierten Applikationen LW-SSO nicht unterstützen oder Sie eine stärkere SSO-Implementierung wünschen, können Sie mit dem Assistenten für die Authentifizierungsverwaltung das Identity Management Single Sign-On (IDM-SSO) konfigurieren. Bei der Aktivierung als SSO-Strategie dient IDM-SSO auch als Authentifizierungsmechanismus. Anhand IDM-SSO authentifizierte Benutzer können sich bei BSM anmelden, sofern Sie die im Feld Benutzerfilter des Dialogfeldes LDAP-Anbieterattribute definierten Kriterien erfüllen. Details finden Sie unter "Dialogfeld "LDAP-Anbieterattribute" auf Seite 400.

Alle Anforderungen an Client-Applikationen werden der SSO-Authentifizierung unterzogen. Die unterstützten Applikationen müssen nur den Namen des authentifizierten Benutzers kennen.

Details zur IDM-SSO-Authentifizierungsstrategie finden Sie unter "Identity Management Single Sign-On-Authentifizierung" auf Seite 412.

Einrichten der LDAP-Authentifizierung

Bei LDAP (Lightweight Directory Access Protocol) handelt es sich um ein Internetprotokoll, das von E-Mail- und anderen Programmen für die Suche nach Informationen auf einem externen Server verwendet wird. Sie können LDAP auf folgende Weise mit BSM konfigurieren:

- Als Authentifizierungsmechanismus für Benutzer, die sich bei BSM anmelden.
- Zum Zuordnen von Gruppen und Synchronisieren von BSM-Benutzern mit Benutzern, die auf dem externen LDAP-Server konfiguriert sind, wodurch der Prozess der Benutzerverwaltung für BSM-Administratoren vereinfacht wird. Details finden Sie unter "Zuordnen der Gruppen und Synchronisieren von Benutzern" auf Seite 423.

Sie können LDAP mithilfe des Assistenten zur Verwaltung von Authentifizierungen aktivieren und deaktivieren. Details finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Authentifizierungsmodi in BSM

In der folgenden Tabelle wird der von BSM verwendete Authentifizierungsmodus angezeigt, je nach Single Sign-On-Modus oder LDAP-Modus, der im Assistenten zur Verwaltung von Authentifizierungen ausgewählt wurde:

Single Sign-On-Modus	LDAP-Modus	Authentifikator
Deaktiviert	Deaktiviert	BSM intern
	Aktiviert	LDAP
LW-SSO	Deaktiviert	BSM intern
	Aktiviert	LDAP
IDM-SSO	Deaktiviert	IDM-SSO
	Aktiviert	IDM-SSO

Authentifizierungsstrategie – Benutzeroberfläche

Dieser Abschnitt umfasst die folgenden Themen:

- "Seite "Authentifizierungsstrategie""
- "Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400
- "Assistent für die Authentifizierung" auf der nächsten Seite

Seite "Authentifizierungsstrategie"

Auf dieser Seite werden die aktuelle Authentifizierungsstrategie und die Single Sign-On-Konfiguration für die Anmeldung bei BSM angezeigt.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Authentifizierungsverwaltung aus.
Wichtiger Hinweis	Der Zugriff auf die Seite Authentifizierungsverwaltung ist von den folgenden Berechtigungsebenen abhängig:
	Ansicht. Ermöglicht die Anzeige der Seite Authentifizierungsverwaltung.
	 Änderung. Ermöglicht Ihnen den Zugriff auf den Assistenten zur Verwaltung von Authentifizierungen und das Ändern von Konfigurationen. Die Schaltfläche Konfiguration ist eingeblendet.
	Sie konfigurieren Berechtigungen unter Benutzer und Berechtigungen . Weitere Informationen finden Sie unter "Zuweisen von Berechtigungen" auf Seite 266.
Siehe auch	 "Authentifizierungsstrategien" auf Seite 385 "Infrastruktureinstellungen" auf Seite 103

Elemente der Oberfläche	Beschreibung
Konfigurieren	Klicken Sie auf die Schaltfläche, um den Assistenten für die Authentifizierung zu öffnen und konfigurieren Sie eine Authentifizierungsstrategie. Weitere Informationen zum Assistenten für die Authentifizierung finden Sie unter "Assistent für die Authentifizierung" auf der nächsten Seite.
	Die Parameter werden sowohl für Single Sign-On-Konfiguration und Lightweight Directory Access Protocol-Konfiguration mithilfe des Assistenten konfiguriert, indem Sie auf die Schaltfläche Konfigurieren klicken. Sie können die Parametereinstellung gleichzeitig oder getrennt vornehmen.

Elemente der Oberfläche	Beschreibung
Lightweight	Dieser Abschnitt zeigt Folgendes an:
Directory Access Protocol-	Name. Der Name des Parameters Lightweight Directory Access Protocol.
Konfiguration	Wert. Der Wert des Parameters Lightweight Directory Access Protocol gemäß der Konfiguration im Assistenten.
Single Sign-	Dieser Abschnitt zeigt Folgendes an:
On- Konfiguration	Name. Der Name des Single Sign-On-Parameters.
	Wert. Der aktuelle Wert des Single Sign-On-Parameters gemäß der Konfiguration im Assistenten.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Konfigurieren	Klicken Sie auf die Schaltfläche, um den Assistenten für die Authentifizierung zu öffnen und konfigurieren Sie eine Authentifizierungsstrategie. Weitere Informationen zum Assistenten für die Authentifizierung finden Sie unter "Assistent für die Authentifizierung".
Name	Der Name des Single Sign-On- oder Lightweight Directory Access Protocol- Parameters.
Wert	Der Wert des angegebenen Single Sign-On- oder Lightweight Directory Access Protocol-Parameters.

Assistent für die Authentifizierung

Dieser Assistent bietet Ihnen die Möglichkeit, eine Authentifizierungsstrategie für die Anmeldung bei BSM zu erstellen.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen >
	Authentifizierungsverwaltung aus und klicken Sie auf Konfigurieren.

Wichtiger Hinweis

Wenn die Benutzeroberfläche nach dem Upgrade der Version von BSM nicht richtig reagiert (beispielsweise wird die Seite nicht geladen oder eine Fehlermeldung wird angezeigt), löschen Sie den Java-Cache, indem Sie folgende Schritte auf dem Client-PC ausführen:

- 1. Navigieren Sie zu **Start > Systemsteuerung > Java**.
- 2. Klicken Sie im Abschnitt **Temporäre Internetdateien** auf **Einstellungen**.
- 3. Klicken Sie im Dialogfeld **Temporäre Internetdateien** auf **Dateien löschen**.

Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf der vorherigen Seite.

Aufbau des Assistenten

Dieser Assistent besteht aus folgenden Elementen:

Assistent für die Authentifizierung > "Seite "Single Sign-On"" unten > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > "Seite "LDAP - Allgemeine Konfiguration"" auf Seite 396 > ("Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400) > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf Seite 401 > "Seite "Übersicht"" auf Seite 402

Seite "Single Sign-On"

Mit diesem Assistenten können Sie eine Single Sign-On-Strategie konfigurieren. Die auf der Seite **Single Sign-On** angezeigten Elemente sind vom ausgewählten Single Sign-On-Modus abhängig.

Wichtiger Hinweis

- Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf der vorherigen Seite.
- Wenn ein Wert in einem der Assistentenfelder leer oder ungültig ist, wird das Fehlersymbol in der entsprechende Zelle angezeigt. Eine Beschreibung des Fehlers können Sie wie folgt anzeigen:
- Zeigen Sie mit der Maus auf das Fehlersymbol, um eine Quickinfo mit der Fehlermeldung anzuzeigen.
- Rufen Sie die Protokolldatei < HPBSM > /log/EJBContainer/login.log auf.

Aufbau des Assistenten

Der "Assistent für die Authentifizierung" auf der vorherigen Seite besteht aus folgenden Elementen:

"Assistent für die Authentifizierung" auf der vorherigen Seite > Seite "Single Sign-On" > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > "Seite "LDAP - Allgemeine Konfiguration"" auf Seite 396 > ("Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400) > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf Seite 401 > "Seite "Übersicht"" auf Seite 402

Elemente der Oberfläche	Beschreibung
Deaktiviert	Wählen Sie diese Option, um die Single Sign-On (SSO)- Authentifizierungsmethode zu deaktivieren.
Identity Management	Wählen Sie diese Option, um die Identity Management Single Sign-On (IDM-SSO)-Authentifizierungsmethode zu konfigurieren. Weitere Informationen zu den Elementen auf dieser Seite finden Sie unten. Weitere Informationen zu diesem Thema finden Sie unter "Identity Management Single Sign-On-Authentifizierung" auf Seite 412. Hinweis: Wenn Sie diese Option ausgewählt haben, kann LDAP nur für die Gruppenzuordnung und nicht für die Authentifizierung konfiguriert werden.
Lightweight	Wählen Sie diese Option, um die Lightweight Single Sign-On (LW-SSO)-Authentifizierungsmethode zu konfigurieren. Weitere Informationen zu den Elementen auf dieser Seite finden Sie unten. Weitere Informationen zu diesem Thema finden Sie unter "LW-SSO-Strategie" auf Seite 404.

Identity Management Single Sign-On (IDM-SSO)-Konfiguration

Elemente der	
Oberfläche	Beschreibung
×	Weist darauf hin, dass der Wert im angegebenen Feld leer oder ungültig ist.
	Zeigen Sie mit der Maus auf dieses Symbol, um eine Quickinfo mit einer Fehlerbeschreibung anzuzeigen.
Name des Headers	Geben Sie den Header-Namen für den durch Identity Management Single Sign-On übergebenen Token ein.
	Beispiel: sso_user
	Hinweis: Stellen Sie sicher, dass die BSM-Ressourcen mit der Identity Management Single Sign-On-Methode geschützt werden, bevor Sie diese Informationen eingeben.
URL für Abmeldung	Geben Sie hier die URL für eine alternative Abmeldungsseite ein, die statt der standardmäßigen Anmeldungsseite nach dem Abmelden von BSM angezeigt werden soll.
	Beispiel:\ <alternativeabmelde-url>.jsp</alternativeabmelde-url>
	Hinweis: Dieses Feld ist optional.

Lightweight Single Sign-On (LW-SSO)-Konfiguration

Elemente der Oberfläche	Beschreibung
×	Weist darauf hin, dass der Wert im angegebenen Feld leer oder ungültig ist.
	Zeigen Sie mit der Maus auf dieses Symbol, um eine Quickinfo mit einer Fehlerbeschreibung anzuzeigen.
Hinzufügen	Fügt den Host/die Domäne der Liste der geschützten Hosts/Domänen hinzu.
SAML2- Authentifizierungsschema aktivieren	Wählen Sie diese Option, um die Authentifizierung über das Security Assertion Markup Language 2.0-Protokoll zu aktivieren.
HP Business Service Management-Domäne	Geben Sie die BSM-Domäne ein, die für die Tokenerstellung verwendet werden soll. Dieses Feld ist für die Unterstützung mehrerer Domänen und normalisierter URLs erforderlich, wenn die Domäne nicht automatisch analysiert werden kann (z. B. bei der Verwendung von Aliasen).
	Beispiel: devlab.ad
Automatisch analysieren	Klicken Sie hierauf, um die BSM-Domäne automatisch analysieren zu lassen.
SAML2-Einstellungen	Klicken Sie hierauf, um Parameter im Dialogfeld SAML2-Konfiguration festzulegen.
Schlüssel für Tokenerstellung (initString)	Geben Sie einen initString-Wert für die Verschlüsselung und Entschlüsselung des LW-SSO-Token ein. Wenn Sie diesen Wert ändern, müssen Sie initString in allen HP-Produkten der LW-SSO-Integration auf den gleichen Wert festlegen. Beispiel: Xy6stqZ

Elemente der Oberfläche	Beschreibung
Vertrauenswürdige Hosts/Domänen	Zeigt die Liste der vertrauenswürdigen Hosts und Domänen an, die Teil einer LW-SSO-Integration sind.
	Die Liste der vertrauenswürdigen Hosts kann den DNS- Domänennamen (meineDomäne.com), den NetBIOS-Namen (meinServer), die IP-Adresse oder den vollqualifizierten Domänennamen für den spezifischen Server (meinServer.meineDomäne) enthalten.
	Um der Liste der vertrauenswürdigen Hosts/Domänen einen Host oder eine Domäne hinzuzufügen, klicken Sie auf das Symbol Hinzufügen, geben Sie den Namen des Hosts oder der Domäne in das Textfeld unter Vertrauenswürdige Hosts/Domänen ein, und wählen Sie den Typ des Hosts oder der Domäne aus dem Dropdownfeld Typ aus.
	Beispiele: mercury.global, emea.hpqcorp.net, devlab.ad
	Zum Entfernen eines Hosts oder einer Domäne aus der Liste vertrauenswürdiger Hosts/Domänen, wählen Sie diesen bzw.
	diese aus, und klicken Sie auf die Schaltfläche Entfernen .

Dialogfeld "SAML2-Konfiguration"

In diesem Dialogfeld können Sie die SAML-Authentifizierungsparameter für Ihre Lightweight Single Sign-On-Konfiguration ändern.

Zugriff	Navigieren Sie im Assistenten zur Verwaltung von Authentifizierungen zur Single Sign-On-Seite, wählen Sie Lightweight aus und aktivieren Sie dann das Kontrollkästchen SAML2-Authentifizierungsschema aktivieren . Klicken Sie auf SAML-Einstellungen , um das Dialogfeld SAML2-Konfiguration zu öffnen.
	Das Dialogfeld SAML2-Konfiguration umfasst die folgenden Bereiche:
	SAML2-Erstellung. Ändern Sie die SAML2-Authentifizierungsparameter zum Senden von SAML-Authentifizierungsanforderungen aus BSM.
	SAML2-Prüfung. Ändern Sie die SAML2-Authentifizierungsparameter zum Entschlüsseln von SAML-Anforderungen von BSM.
Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf Seite 390.
	SAML ist in BSM standardmäßig aktiviert. Wenn Sie die SAML- Authentifizierung deaktivieren wollen, deaktivieren Sie das Kontrollkästchen SAML2-Authentifizierungsschema aktivieren.

Aufbau des Assistenten	Der "Assistent für die Authentifizierung" auf Seite 390 besteht aus folgenden Elementen:
	"Assistent für die Authentifizierung" auf Seite 390 > "Seite "Single Sign-On"" auf Seite 391 > (Dialogfeld "SAML2-Konfiguration") > "Seite "LDAP - Allgemeine Konfiguration"" auf der nächsten Seite > ("Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400) > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf Seite 401 > "Seite "Übersicht"" auf Seite 402

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Wiederherstellen	Stellt die SAML2-Konfigurationsattribute wieder auf den Status bei der Anmeldung an die aktuelle Sitzung von BSM zurück.

Abschnitt "SAML2-Erstellung"

Elemente der Oberfläche	Beschreibung
Keystore- Dateiname	Der Dateiname des Keystore in BSM.
	Ist Nach Keystore in Klassenpfad suchen nicht ausgewählt, muss es sich bei diesem Wert um den vollständigen Pfad zum Speicherort des Keystore handeln. Beispiel: C: \mystore\java.keystore.
	Ist Nach Keystore in Klassenpfad suchen ausgewählt, muss es sich bei diesem Wert lediglich um den Dateinamen des Keystore handeln. Beispiel: java.keystore.
Keystore- Kennwort	Das Kennwort, das den Zugriff auf den Keystore ermöglicht, in dem sich der private Schlüssel für die Verschlüsselung während der SAML-Authentifizierungsanforderung befindet.
Nach Keystore in Klassenpfad suchen	Wählen Sie diese Option aus, wenn das LW-SSO-Framework im Klassenpfad nach dem Keystore suchen soll.
	Hinweis: Ist diese Option nicht ausgewählt, geben Sie nur den Namen der eigentlichen Keystore-Datei in das Feld Keystore-Dateiname ein.
Alias des privaten Schlüssels	Gibt den Alias des privaten Schlüssels an, der zur Verschlüsselung während der SAML-Authentifizierungsanforderung verwendet wird.
Kennwort des privaten Schlüssels	Gibt das Kennwort des privaten Schlüssels an, der zur Verschlüsselung während der SAML-Authentifizierungsanforderung verwendet wird.

Abschnitt "SAML2-Prüfung"

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
Nach Keystore in Klassenpfad suchen	Wählen Sie diese Option aus, wenn das LW-SSO-Framework im Klassenpfad nach dem Keystore suchen soll.
	Hinweis: Ist diese Option nicht ausgewählt, geben Sie nur den Namen der eigentlichen Keystore-Datei in das Feld Keystore-Dateiname ein.
Keystore- Dateiname	 Der Dateiname des Keystore in BSM. Ist Nach Keystore in Klassenpfad suchen nicht ausgewählt, muss es sich bei diesem Wert um den vollständigen Pfad zum Speicherort des Keystore handeln. Beispiel: C:\mystore\java.keystore. Ist Nach Keystore in Klassenpfad suchen ausgewählt, muss es sich bei diesem Wert lediglich um den Dateinamen des Keystore handeln. Beispiel: java.keystore.
Keystore- Kennwort	Gibt das Kennwort des öffentlichen Schlüssels an, der zur Verschlüsselung während der SAML-Authentifizierungsanforderung verwendet wird.

Seite "LDAP - Allgemeine Konfiguration"

Auf dieser Seite des Assistenten können Sie einen externen LDAP-Server zum Speichern der Authentifizierungsinformationen (Benutzernamen und Kennwörter) verwenden und die Benutzersynchronisierung zwischen LDAP-Benutzern und BSM-Benutzern aktivieren.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Authentifizierungsverwaltung aus und klicken Sie auf Konfigurieren. Navigieren Sie zur Seite LDAP - Allgemeine Konfiguration.
	Folgende LDAP-Modi sind verfügbar:
	Enabled
	Disabled
	Hinweis: LDAP kann nicht für die Authentifizierung verwendet werden, wenn Sie IdentityManagement auf der Seite Single Sign-On-Konfiguration des Assistenten ausgewählt haben.
Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf Seite 390.
	Wenn Sie beim Konfigurieren von LDAP-Parametern Hilfe benötigen, wenden Sie sich an Ihren LDAP-Administrator.

Aufbau des Assistenten	Der "Assistent für die Authentifizierung" auf Seite 390 besteht aus folgenden Elementen:
	"Assistent für die Authentifizierung" auf Seite 390 > "Seite "Single Sign-On"" auf Seite 391 > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > Seite "LDAP - Allgemeine Konfiguration" > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf Seite 401 > "Seite "Übersicht"" auf Seite 402

Ausschnitt "LDAP - Allgemeine Konfiguration"

Elemente der Oberfläche	Beschreibung
×	Weist darauf hin, dass der Wert im angegebenen Feld leer oder ungültig ist.
	Eine Beschreibung des Fehlers können Sie wie folgt anzeigen:
	Zeigen Sie mit der Maus auf das Fehlersymbol, um eine Quickinfo mit der Fehlermeldung anzuzeigen.
	Öffnen Sie die Protokolldatei < HPBSM- Stammverzeichnis>\log\EJBContainer\login.log.
Erweitert	Öffnet das Dialogfeld LDAP-Anbieterattribute , in dem Sie die Konfigurationen für den ausgewählten LDAP-Anbieter ändern können. Weitere Informationen finden Sie unter "Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400.
DN-Auflösung (Distinguished Name)	Wählen Sie diese Option aus, um die LDAP-Benutzerinformationen für die Suche einzugeben. Hinweis: Wenn für Ihr LDAP Benutzeranmeldeinformationen erforderlich sind, um die Verbindung zum LDAP-Server zu überprüfen, müssen Sie den Dienst users-remote-repository in der JMX-Konsole verwenden, um diese Informationen einzugeben, da Sie über die Benutzeroberfläche nicht ohne gültige Benutzeranmeldeinformationen auf die URL-Adresse des LDAP-Servers zugreifen können.
DN (Distinguished Name) für Benutzer mit Suchberechtigung	Definiert den Distinguished Name (DN) eines Benutzers mit Suchprivilegien auf dem LDAP-Verzeichnisserver. Hinweis: Lassen Sie dieses Feld für einen anonymen Benutzer leer.

Elemente der Oberfläche	Beschreibung
LDAP-Server-URL	Geben Sie die URL des LDAP-Servers ein (oder für Active Directory- Benutzer: Global Catalog [AD GC])
	Um verschiedene Verzweigungen in derselben Struktur darzustellen, geben Sie mehrere DNs ein, die Sie durch Semikola trennen.
	Um ein Failover zu ermöglichen, geben Sie mehrere LDAP (AD GC)- Server-URLs ein, die Sie durch Semikola trennen.
	Das erforderliche Format lautet: Idap://computername:port//bereich??sub
	Normalerweise verwenden LDAP-Server den Port 389 und AD GC- Server den Port 3268 oder den sicheren Port 3269.
	Mögliche Werte für den Bereich lauten sub , one oder base , wobei die Groß-/Kleinschreibung zu beachten ist.
	BSM ignoriert das Attribut zwischen zwei Fragezeichen, sofern vorhanden.
	Wenn die Portnummer und der Wert für den Bereich nicht angegeben werden, werden Standardwerte verwendet
	 Die Standardportnummer für die reguläre Kommunikation lautet: 389
	 Die Standardportnummer für die SSL-Kommunikation lautet: 636
	■ Standardwert für den Bereich: sub
	Beispiele:
	Einzelner DN, einzelner LDAP-Server: ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
	<pre>Mehrere DNs: ldap://my.ldap.server:389/ou=People, o=myOrg.com??sub; ldap://my.ldap.server:389/ou=Staff, o=my2ndOrg.net??sub</pre>

Elemente der Oberfläche	Beschreibung
	<pre>Mehrere LDAP-Server: ldap://my.ldap.server:389/ou=People, o=myOrg.com??sub; ldap://my.2ndldap.server:389/ou=People, o=myOrg.com??sub</pre>
	Hinweis: Wenn nach Eingabe der URL ein rotes X mit folgendem Popuptext angezeigt wird:
	FEHLER - sun.security.validator.ValidatorException: Fehler beim Erstellen des PKIX-Pfades: sun.security.provider.certpath.SunCertPathBuilderException: Gültiger Zertifizierungspfad zum angeforderten Ziel konnte nicht gefunden werden
	Dies bedeutet, dass Sie eine Vertrauensbeziehung mit dem LDAP- Server herstellen müssen. Details finden Sie unter "Sichern der Kommunikation zwischen LDAP-Server und BSM-Server über SSL" auf Seite 427.
LDAP-Anbietertyp	Geben Sie den verwendeten LDAP-Anbietertyp ein. Wählen Sie zwischen:
	Allgemeines LDAP
	Microsoft Active Directory
	Sonstiges
	Hinweis: Wenn Sie auf Erweitert klicken und die Attributeinstellungen für den LDAP-Anbieter ändern, wird der Wert in diesem Feld automatisch auf Sonstiges geändert.
Kennwort für Benutzer mit	Definiert das Kennwort des Benutzers mit Suchberechtigung für die Entitäten des LDAP-Servers nach Gruppen.
Suchberechtigung	Hinweis: Lassen Sie dieses Feld für einen anonymen Benutzer leer.

Abschnitt "DN-Auflösung testen"

Ermöglicht Ihnen eine Überprüfung der konfigurierten LDAP-Parameter und der Anmeldeinformationen eines bestimmten Benutzers auf Gültigkeit.

Elemente der Oberfläche	Beschreibung
Kennwort	Das Kennwort des Benutzers, dessen Anmeldeinformationen in das Feld UUID eingegeben werden.
	Hinweis: Dieses Feld ist optional. Wenn Sie keinen Eintrag vorgenommen haben, wird ein anonymer Benutzer verwendet.
Testen	Testet die LDAP-Konfiguration und die Benutzeranmeldeinformationen auf Gültigkeit. In einer Meldung wird angezeigt, ob die Überprüfung erfolgreich war.
UUID	Der tatsächliche Anmeldename (eindeutige Benutzer-ID) des LDAP-Benutzers, der überprüft werden soll.

Dialogfeld "LDAP-Anbieterattribute"

In diesem Dialogfeld können Sie die standardmäßigen LDAP-Einstellungen ändern, die sich auf den ausgewählten Hersteller beziehen.

Zugriff	Klicken Sie auf der Seite LDAP - Allgemeine Konfiguration des Assistenten zur Verwaltung von Authentifizierungen auf Erweitert .	
Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf Seite 390.	
	Wenn Sie die Einstellungen für die LDAP-Anbieterattribute ändern, wird der Wert des Felds LDAP-Anbietertyp auf der Seite LDAP - Allgemeine Konfiguration automatisch in Sonstiges geändert.	
Aufbau des Assistenten	ŭ v	
	"Assistent für die Authentifizierung" auf Seite 390 > "Seite "Single Sign-On"" auf Seite 391 > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > "Seite "LDAP - Allgemeine Konfiguration"" auf Seite 396 > (Dialogfeld "LDAP-Anbieterattribute") > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf der nächsten Seite > "Seite "Übersicht"" auf Seite 402	

Elemente der Oberfläche	Beschreibung
Gruppenklassenobjekt	Legt fest, welche LDAP-Entitäten als Gruppen auf dem LDAP- Server angesehen werden.
Gruppenmitgliedsattribut	Definiert das spezielle Attribut, mit dem festgelegt wird, welche Entitäten der LDAP-Gruppe als Mitglieder der LDAP-Gruppe angesehen werden.

Elemente der Oberfläche	Beschreibung
Wiederherstellen	Setzt die LDAP-Herstellerattribute wieder auf den Status der Anmeldung an die aktuelle Sitzung von BSM zurück.
Benutzerfilter	Definiert, welche LDAP-Benutzer sich bei BSM anmelden dürfen.
Benutzerobjektklasse	Legt fest, welche LDAP-Entitäten als Benutzer auf dem LDAP- Server angesehen werden.
UUID-Attribut	Das Attribut, mit dem Sie sich bei BSM anmelden, so wie es auf dem LDAP-Server angezeigt wird.
	Beispiel: uid, mail

Seite "LDAP-Benutzersynchronisierungskonfiguration"

Auf dieser Seite des Assistenten können Sie den LDAP-Server für die Synchronisierung von LDAP-Benutzern mit BSM-Benutzern konfigurieren.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Authentifizierungsstrategie und klicken Sie auf Konfigurieren. Navigieren Sie zur Seite LDAP-Benutzersynchronisierungskonfiguration.
Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf Seite 390.
	Diese Seite ist nur dann aktiviert, wenn die Seite LDAP - Allgemeine Konfiguration. richtig konfiguriert wurde.
Aufbau des Assistenten	Der "Assistent für die Authentifizierung" auf Seite 390 besteht aus folgenden Elementen:
	"Assistent für die Authentifizierung" auf Seite 390 > "Seite "Single Sign-On"" auf Seite 391 > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > "Seite "LDAP - Allgemeine Konfiguration"" auf Seite 396 > ("Dialogfeld "LDAP-Anbieterattribute"" auf der vorherigen Seite) > Seite "LDAP-Benutzersynchronisierungskonfiguration" > "Seite "Übersicht"" auf der nächsten Seite

Elemente der Oberfläche	Beschreibung
×	Weist darauf hin, dass der in das angegebene Feld eingegebene Wert ungültig ist.

Elemente der Oberfläche	Beschreibung
Benutzersynchronisierung aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Benutzersynchronisierung bei der Anmeldung an BSM zu aktivieren und LDAP-Benutzer mit BSM-Benutzern zu synchronisieren.
	Wichtig: Stellen Sie vor dem Aktivieren dieses Kontrollkästchens sicher, dass Sie LDAP-Gruppen und BSM einander zugeordnet haben. Wenn Sie keine Gruppenzuordnung durchgeführt haben, werden alle Benutzer unter der Stammgruppe geschachtelt und erhalten die Berechtigung Anzeigender Benutzer zugewiesen. Weitere Informationen zum Zuordnen von Gruppen finden Sie unter "Zuordnen der Gruppen und Synchronisieren von Benutzern" auf Seite 423.
Gruppen-Basis-DN	Der DN (Distinguished Name) der LDAP-Entität, aus der Sie die Gruppensuche starten wollen.
Gruppensuchfilter	Geben Sie die relevanten Parameter als Hinweis darauf ein, welche Attribute in der Gruppensuche verwendet werden sollen.
Basis-DN der Stammgruppe	Der DN (Distinguished Name) der LDAP-Gruppen, die in der hierarchischen Struktur der zugeordneten Gruppen an erster Stelle stehen. Bei dem Wert muss es sich um eine Untermenge der Gruppen-Basis-DN handeln.
Stammgruppenfilter	Geben Sie die Parameter ein, um zu bestimmen, welche LDAP- Entitäten die hierarchische Basis für die LDAP-Gruppen bilden sollen. Die angegebenen Entitäten stehen dann für die Zuordnung zu Gruppen in BSM zur Verfügung.
Testen	Prüft, ob die zur Definition der LDAP-Gruppenstruktur eingegebenen Parameter gültig sind.
Ausschnitt "Gruppenkonfiguration testen"	Zeigt die Gruppen, die für die Zuordnung mit BSM-gruppen verfügbar sind sowie die hierarchische Struktur der LDAP-Gruppen an. Die angezeigten Gruppen werden anhand der Parameter bestimmt, die in die Felder auf der Seite LDAP-Benutzersynchronisierungskonfiguration eingegeben wurden.

Seite "Übersicht"

Auf dieser Seite des Assistenten wird eine Übersicht über die Authentifizierungsstrategien angezeigt, die im Assistenten zur Verwaltung von Authentifizierungen konfiguriert wurden.

Zugriff	Wählen Sie Admin > Plattform > Benutzer und Berechtigungen >
	Authentifizierungsverwaltung aus und klicken Sie auf Konfigurieren. Geben
	Sie die Informationen auf den Seiten zu Single Sign-On und LDAP ein und navigieren Sie zur Seite Übersicht .

Wichtiger Hinweis	Allgemeine Informationen über diesen Assistenten finden Sie unter: "Assistent für die Authentifizierung" auf Seite 390.
Aufbau des Assistenten	Der "Assistent für die Authentifizierung" auf Seite 390 besteht aus folgenden Elementen:
	"Assistent für die Authentifizierung" auf Seite 390 > "Seite "Single Sign-On"" auf Seite 391 > ("Dialogfeld "SAML2-Konfiguration"" auf Seite 394) > "Seite "LDAP - Allgemeine Konfiguration"" auf Seite 396 > ("Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400) > "Seite "LDAP-Benutzersynchronisierungskonfiguration"" auf Seite 401 > Seite "Übersicht"

Elemente der Oberfläche	Beschreibung
LDAP - Allgemeine Konfiguration	Zeigt die Parameter zu LDAP - Allgemeine Konfiguration gemäß der Konfiguration auf der Seite LDAP - Allgemeine Konfiguration des Assistenten an.
LDAP- Benutzersynchronisierungskonfiguration	Zeigt die Parameter zu LDAP- Benutzersynchronisierungskonfiguration gemäß der Konfiguration auf der Seite LDAP- Benutzersynchronisierungskonfiguration des Assistenten an.
Single Sign-On-Konfiguration	Zeigt die Single Sign-On-Parameter gemäß der Konfiguration im Assistenten an.

Kapitel 22

LW-SSO-Strategie

Die Standardstrategie für die SSO-Authentifizierung für BSM ist Lightweight Single Sign-On (LW-SSO). LW-SSO ist in BSM eingebettet und erfordert keinen externen Computer für die Authentifizierung. BSM verwendet zur Zeit die Version 2.4 von LW-SSO.

Eine Übersicht über die Single Sign-On-Strategien finden Sie unter "Einrichten einer Strategie für die SSO-Authentizierung" auf Seite 386.

Sie können LW-SSO in BSM mithilfe des Assistenten für die Authentifizierung konfigurieren. Weitere Informationen zum Assistenten für die Authentifizierung finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

LW-SSO kann mithilfe der JMX-Konsole konfiguriert werden, um die Authentifizierung durch clientseitige Zertifikate zu akzeptieren. Sobald ein Zertifikat erkannt wird, erstellt LW-SSO den Token, der von anderen Applikationen verwendet werden kann. Weitere Informationen finden Sie unter "Sicherstellen des Benutzerzugriffs auf BSM mithilfe von clientseitigen Zertifikaten" auf Seite 408.

Weitere Informationen zu LW-SSO finden Sie unter "LW-SSO-Authentifizierung – Allgemeine Referenz" auf Seite 430.

LW-SSO-Konfiguration für Installationen mit mehreren und mit verschachtelten Domänen

Die LW-SSO-Konfiguration, die im Assistenten zur Verwaltung von Authentifizierungen festgelegt wird (weitere Informationen siehe "Assistent für die Authentifizierung" auf Seite 390), ist von der Architektur der BSM-Installation abhängig.

Wenn Sie sich über einen Man-in-the-Middle, z. B. Reverse Proxy, Load Balancer oder NAT, bei BSM anmelden, ist die BSM-Domäne die Domäne des Man-in-the-Middle.

Wenn Sie sich direkt beim BSM-Gateway anmelden, ist die BSM-Domäne die Domäne des BSM-Gateways.

Damit LW-SSO mit einer anderen Applikation in einer anderen Domäne als der BSM-Domäne verwendet werden kann, müssen all diese Domäne in der Liste **Vertrauenswürdige Hosts/Domänen** der LW-SSO-Konfiguration aufgeführt sein.

Befinden sich BSM-Domäne und integrierende Applikation in verschachtelten Domänen, sollte das Suffix der Domäne als LW-SSO-Domäne für beide Applikationen definiert sein. Außerdem sollten Sie die automatische Domänenberechnung (**Automatisch analysieren** im Assistenten zur Verwaltung von Authentifizierungen) deaktivieren und das Domänensuffix explizit angeben.

```
Beispiel 1:

BSM -Gateway-Server befindet sich in emea.hp.com

TransactionVision -Server befindet sich in cnd.hp.com

Deaktivieren Sie die automatische Domänenberechnung und legen Sie folgenden Domänennamen fest: hp.com

Beispiel 2:

BSM -Gateway-Server befindet sich in corp.ad.example.com

NNMi -Server befindet sich in sdc.example.com

Load Balancer befindet sich in example.com

Deaktivieren Sie die automatische Domänenberechnung und legen Sie
```

folgenden Domänennamen fest: example.com

Konfigurieren des Modus für die Verarbeitung unbekannter Benutzer

In dieser Aufgabe wird die Verarbeitung unbekannter Benutzer beschrieben, die versuchen, sich bei BSM anzumelden, d. h. Benutzer, die von der Host-Applikation authentifiziert wurden, im Repository der BSM-Benutzer jedoch nicht vorhanden sind.

So konfigurieren Sie den Modus zur Verarbeitung unbekannter Benutzer:

- 1. Wählen Sie Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen aus. Wählen Sie dann Foundation und Single Sign-On aus.
- 2. Navigieren Sie im Feld **Single Sign-On Lightweight (LW-SSO)** zu dem Eintrag **Modus zur Bearbeitung unbekannter Benutzer** und wählen Sie eine der folgenden Optionen aus:
 - IntegrationUser. Ein Benutzer mit dem Benutzernamen IntegrationUser wird anstelle des Benutzers erstellt, der die Anmeldung versucht hat. Dieser Benutzer besitzt die Berechtigung Systemanzeige.
 - Allow. Der Benutzer wird als neuer BSM-Benutzer erstellt und ihm wird der Zugriff auf das System gewährt. Dieser Benutzer besitzt die Berechtigung Systemanzeige und sein Standardkennwort ist der Anmeldename.
 - **Deny.** Dem Benutzer wird der Zugriff auf BSM verweigert und es wird die Anmeldeseite angezeigt.

Die Änderungen werden sofort wirksam.

Hinweis: Wenn zwischen BSM und dem LDAP-Server die Benutzersynchronisierung aktiviert ist, wird unbekannten Benutzern immer der Zugang zu BSM verweigert.

Ändern der LW-SSO-Parameter mithilfe der JMX-Konsole

In dieser Aufgabe wird beschrieben, wie die Optionen und Parameter geändert werden, die für LW-SSO über die JMX-Konsole verwendet werden.

Sie können die JMX-Konsole auch verwenden, wenn Sie keinen Zugriff auf BSM haben und die SSO-Parameter ändern müssen, um Zugriff zu erhalten.

So ändern Sie Lightweight Single Sign-On (LW-SSO)-Parameter mithilfe der JMX-Konsole:

- Geben Sie die URL der JMX-Konsole (http://<Servername>:8080/jmx-console/) in einem Webbrowser ein.
- 2. Geben Sie Anmeldeinformationen für die JMX-Konsole ein. Wenn Sie diese nicht kennen, wenden Sie sich an Ihren Systemadministrator.
- 3. Ermitteln Sie den Lightweight Single Sign-On-Kontext wie folgt:

a. Domänenname: Topaz

b. Service: LW-SSO-Konfiguration

4. Ändern Sie die Parameter wie gewünscht.

Die Änderungen werden sofort wirksam.

Sicherstellen des Benutzerzugriffs auf BSM mithilfe von clientseitigen Zertifikaten

Sie können den Benutzerzugriff auf BSM sicherstellen, indem Sie clientseitige Zertifikate verwenden. Sie konfigurieren LW-SSO, indem Sie die JMX-Konsole verwenden, um solche Zertifikate zu akzeptieren. Nachdem ein Zertifikat akzeptiert wurde, wird der Benutzer bei BSM angemeldet. Die Authentifizierung durch clientseitige Zertifikate bietet eine sichere Alternative für die Eingabe von Anmeldeinformationen in den Anmeldebildschirm.

So konfigurieren Sie LW-SSO für die Zusammenarbeit mit der Authentifizierung durch clientseitige Zertifikate:

- Legen Sie fest, welches Feld und welche Attribute des clientseitigen Zertifikats für die Authentifizierung verwendet werden sollen (Beispiel: EMAILADDRESS in SubjectDN).
 Zeigen Sie dazu die Details des Clientzertifikats an und suchen Sie die Felder Subject oder SubjectAlternativeName. Entscheiden Sie, welches Attribut verwendet werden soll.
- Geben Sie die URL der JMX-Konsole (http://<Name des Gateway- oder Datenverarbeitungsservers>:8080/jmx-console/) in einem Webbrowser ein.
- 3. Geben Sie Anmeldeinformationen für die JMX-Konsole ein.
- 4. Ermitteln Sie unter dem Domänennamen **Topaz** den Eintrag **service=LW-SSO Configuration**.
- 5. Zum Aktivieren der clientseitigen Authentifizierung setzen Sie das Attribut ClientCertificateInboundHandlerEnabled auf true.

Hinweis: Es wird dringend empfohlen, die clientseitige Authentifizierung nur zu aktivieren, wenn es erforderlich ist, und andernfalls den Wert explizit auf **false** zu setzen.

- 6. Sie definieren das Feld, das die Benutzerkennung enthält, indem Sie das Attribut ClientCertificateUserldentifierRetrieveField ermitteln und den Namen des Authentifizierungszertifikatfelds eingeben, in dem sich die Benutzerkennung befindet, beispielsweise SubjectDN oder SubjectAlternativeName.
- Sie definieren, wie die Benutzerkennung aus dem Feld abgerufen wird, indem Sie das Attribut ClientCertificateUserIdentifierRetrieveMode ermitteln und den entsprechenden Modus zum Abrufen der Benutzerkennung eingeben, entweder EntireField oder FieldPart.
- 8. Um den Teil des Felds User Identifier Retrieve, das die Benutzerkennung enthält, zu definieren, ermitteln Sie das Attribut ClientCertificateUserIdentifierRetrieveFieldPart und geben den Namen des Teils von User Identifier Retrieve ein, in dem sich die Benutzerkennung befindet, beispielsweise EMAILADDRESS.

Hinweis: Wird userIdentifierRetrieveMode als FieldPart eingestellt oder userIdentifierRetrieveField als SubjectAlternativeName, muss das Attribut ClientCertificateUserIdentifierRetrieveFieldPart angegeben werden. Andernfalls kann es leer bleiben.

Klicken Sie auf Änderungen anwenden.

- 10. Wählen Sie in der BSM-Benutzeroberfläche **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus. Klicken Sie auf **Foundation** und wählen Sie **Single Sign-On** aus der Dropdownliste aus.
- 11. Stellen Sie für **Modus zur Bearbeitung unbekannter Benutzer** den Wert für **Verweigert** ein.

Sicherstellen des Benutzerzugriffs auf BSM mithilfe eines externen Authentifizierungspunkts

LW-SSO 2.4 ermöglicht die Verwendung eines externen Authentifizierungspunkts, der den Benutzern gestattet, die eigene Anmeldeüberprüfung für die von ihnen gewünschte Authentifizierungstechnologie zu verwenden: LDAP, eine proprietäre Benutzer-/Kennwortdatenbank, eine benutzerdefinierte SSO-Lösung usw.

Bei einem externen Authentifizierungspunkt handelt es sich um eine externe URL, die die tatsächliche Benutzerauthentifizierung durchführt. Er enthält die Benutzeranmeldeinformationen (zumeist Benutzername und Kennwort, aber auch ein Klasse-B-Zertifikat des Benutzers oder ein proprietärer SSO-Token), überprüft diese Angaben und erstellt eine "Authentication Assertion" - einen Token, in dem festgelegt wird, wer der authentifizierte Benutzer ist, und in dem normalerweise auch Informationen über die Art der Authentifizierung des Benutzers enthalten sind.

So verwenden Sie eine externe Authentifizierungslösung mit LW-SSO 2.4:

- Wenn Sie LDAP verwenden, stellen Sie sicher, dass dasselbe Benutzerrepository von BSM und dem Authentifizierungsserver verwendet wird. Wenn Sie LDAP nicht verwenden, erstellen Sie die Benutzer manuell in BSM.
- Stellen Sie die LW-SSO-Konfiguration auf dem Authentifizierungsserver so ein, dass derselbe "initString" wie in BSM verwendet wird.
- 3. Verwenden Sie in der LW-SSO-Konfiguration auf dem BSM-Gateway-Server die JMX-Konsole für Folgendes:
 - a. Angeben des AuthenticationPointServer-URL
 - b. Einstellen von "validationPoint enabled = true"
 - c. Klicken Sie auf Änderungen anwenden.
 - d. Starten Sie den BSM-Gateway-Server neu.
- 4. Stellen Sie sicher, dass Sie die Anmeldung an BSM über den externen Authentifizierungspunkt vornehmen können. Wenn Sie sich nicht anmelden können, finden Sie weitere Informationen unter "Fehlerbehebung und Einschränkungen" auf der nächsten Seite.
- 5. Wenn bestimmte URLs diese Funktion nicht verwenden sollen, verwenden Sie die JMX-Konsole, um sie zur Liste der nicht sicheren URLs in der LW-SSO-Konfiguration aufzunehmen.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Fehlerbehebungen und Einschränkungen für LW-SSO (Lightweight Single Sign-On).

Zugriff auf BSM wegen geänderter LW-SSO-Parameter nicht möglich

Wenn der Zugriff auf BSM für Sie gesperrt ist, können Sie bestimmte LW-SSO-Parameter (Lightweight Single Sign-On) remote aktualisieren. Verwenden Sie dazu die JMX-Konsole auf dem in BSM eingebetteten Applikationsserver.

Weitere Informationen zum Ändern der LW-SSO-Parameter außerhalb der BSM-Benutzeroberfläche finden Sie unter "Ändern der LW-SSO-Parameter mithilfe der JMX-Konsole" auf Seite 407.

Synchronisieren von Benutzern bei Verwendung von LW-SSO

LW-SSO gewährleistet keine Benutzersynchronisierung zwischen integrierten Applikationen. Deshalb müssen Sie LDAP aktivieren und die Gruppenzuordnung für die integrierte Applikation zum Überwachen von Benutzern konfigurieren. Fehler bei der Gruppenzuordnung und Benutzersynchronisierung können zu Sicherheitslücken und fehlerhaftem Applikationsverhalten führen. Weitere Informationen zum Zuordnen von Benutzern zwischen Applikationen finden Sie unter "Zuordnen der Gruppen und Synchronisieren von Benutzern" auf Seite 423.

Anmeldung bei BSM bei Verwendung eines externen Authentifizierungspunkts nicht möglich

Wenn Sie einen externen Authentifizierungspunkt aktiviert haben und sich darüber nicht anmelden können, stellen Sie sicher, dass der Benutzer, dessen Anmeldeinformationen Sie eingeben, als Benutzer in BSM definiert ist.

Kapitel 23

Identity Management Single Sign-On-Authentifizierung

Sie binden Identity Management Single Sign-On (IDM-SSO) ein, wenn Sie eine sicherere Verbindung als die von LW-SSO benötigen oder wenn die Applikationen, die außerhalb von BSM konfiguriert wurden, LW-SSO nicht unterstützen. Der IDM-Server wird von einem einzigen zentralen Richtlinienserver überwacht und besteht aus einem Benutzerrepository, einem Richtlinienspeicher (beide können sich auf demselben Server befinden wie der Richtlinienserver) und einem Webserver-Agent, die auf dem jeweiligen Webserver der Applikation installiert wurden, die mit dem Richtlinienserver kommunizieren. Der IDM-Server steuert den Benutzerzugriff auf verschiedene Ressourcen der Organisation und schützt vertrauliche persönliche und geschäftliche Informationen vor nicht autorisierten Benutzern. Informationen hierzu finden Sie in der IDM-Dokumentation des Herstellers.

BSM verlangt vom IDM-Hersteller das Speichern von Benutzerinformationen, um sie als Header bei HTTP-Anforderungen zu übergeben. Sie konfigurieren sowohl den Header-Namen als auch die IDM-SSO-Strategie im Assistenten für die Authentifizierung. Weitere Informationen finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Bevor Sie IDM-SSO in BSM konfigurieren, stellen Sie sicher, dass der IDM-Anmeldebildschirm vor dem BSM-Anmeldebildschirm angezeigt wird.

Ist dies nicht der Fall, wenden Sie sich an den IDM-Administrator. Wurde in BSM dieselbe LDAP definiert wie die von IDM verwendete, sollten Sie die Authentifizierung über die IDM- und die BSM-Anmeldebildschirme mit denselben Anmeldeinformationen durchführen können. Wenn nicht, überprüfen Sie, ob die LDAP-Einstellungen in BSM denen in IDM entsprechen. Sie können nun die IDM-SSO in BSM konfigurieren. Wenn Sie beim Anzeigen der Header Hilfe brauchen, um den korrekten IDM-Header zu bestimmen, der in der Konfiguration verwendet werden soll, können Sie zum BSM-Anmeldebildschirm zurückkehren, ohne die Sitzung zu schließen, und /DumpSession.jsp an die Anmelde-URL anhängen. Suchen Sie Ihre Login-ID in der Ergebnisliste. Es sollte sich um den Header-Namen handeln, der von IDM bereitgestellt wird. Überprüfen Sie diesen, indem Sie http://<HPBSM-Server>/topaz/verifyIDM.jsp in derselben Benutzersitzung verwenden. Wurde dies überprüft, sollten Sie den Namen im Assistenten zur Verwaltung von Authentifizierungen verwenden können.

Sichern von BSM-Ressourcen unter IDM-SSO

Wird IDM-SSO als eine Single Sign-On-Strategie verwendet, könnnen BSM-Ressourcen mit Formular- oder Basisauthentifizierungsschemata geschützt werden oder ungeschützt bleiben.

Ressourcen, auf die von Applikationsbenutzern zugegriffen wird

Wenn Sie IDM-SSO verwenden möchten, um BSM-Ressourcen zu sichern, auf die von Applikationsbenutzern zugegriffen wird, verwenden Sie die **Formularauthentifizierung** für die folgenden Ressourcen:

- /filters/*
- /hpbsm/*
- /mam-images/*
- /mcrs/*
- /MercuryAM/*
- /odb/*
- /opal/*
- /opr-admin-server/*
- /opr-console/*
- /opr-gateway/*
- /opr-web/*
- /ovpm /*
- /topaz/*
- /topazSettings/*
- /tv/*
- /tvb/*
- /ucmdb-ui/*
- /uim/*
- /utility portlets/*
- /webinfra/*

Ressourcen, auf die von Daten-Collectoren zugegriffen wird

Wenn Sie IDM-SSO verwenden möchten, um BSM-Ressourcen zu sichem, auf die von Daten-Collectoren in der Kommunikation von Computer zu Computer zugegriffen wird, verwenden Sie eine Authentifizierungsmethode, die das Weitergeben von Anmeldeinformationen erlaubt, bzw. die Basisauthentifizierung.

Die folgenden Ressourcen werden von Daten-Collectoren verwendet:

- /ext/* verwendet von RUM
- /mam/* verwendet von RTSM
- /topaz/topaz_api/* verwendet von allen Daten-Collectoren zum Abrufen der BSM-Version, Serverzeit usw.

Ressourcen, auf die von Webservices zugegriffen wird (erforderlich)

Wenn Sie IDM-SSO mit BSM verwenden, müssen Sie die folgenden Ressourcen mithilfe der **Basisauthentifizierung** schützen, da sie von verschiedenen BSM-Webservices verwendet werden:

- /opr-admin-server/rest/*
- /opr-console/rest/*
- /opr-gateway/rest/*
- /topaz/bam/*
- /topaz/bsmservices/*
- /topaz/eumopenapi/*
- /topaz/servicehealth/*
- /topaz/slm/*

Zusätzliche Ressourcen, die mit Basisauthentifizierung geschützt werden müssen

- /topaz/rfw/directAccess.do verwendet mit veröffentlichtem URL für einen Report
- /topaz/sitescope/* verwendet für die SAM-Verwaltung eingebunden in BSM-Benutzeroberfläche

Ungeschützte Ressourcen

Die folgenden Ressourcen bleiben ungeschützt:

- /mam-collectors
- /topaz/Charts
- /topaz/images
- /topaz/Imgs/chartTemp
- /topaz/js
- /topaz/rfw/static
- /topaz/services/technical/time
- /topaz/static
- /topaz/stylesheets

BSM-Plattformverwaltungshandbuch

Kapitel 23: Identity Management Single Sign-On-Authentifizierung

- /tvb/rest
- /ucmdb-api

Wenn Sie einen Load Balancer verwenden, sollten auch die folgenden Ressourcen auf **ungeschützt** eingestellt werden.

- /topaz/topaz_api/loadBalancerVerify_core.jsp
- /topaz/topaz_api/loadBalancerVerify_centers.jsp

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Hinweise zur Fehlerbehebung bei IDM-SSO.

Fehler bei der Eingabe des IDM-SSO-Headers in den Assistenten für die Authentifizierung

Vergewissern Sie sich, dass der richtige Header verwendet wird. Wenden Sie sich an den Siteminder-Administrator, um alle Header abzubilden und um einen passenden für Ihre Zwecke zu finden. Wenn Sie beispielsweise eine E-Mail-Adresse als Anmeldenamen verwenden möchten, suchen Sie nach einem Feld, das nur eine E-Mail-Adresse enthält. Oder wenn er z. B. aussieht wie HTTP_SEA, entfernen Sie HTTP_ aus dem Namen und geben Sie sea als Header-Namen ein.

Überprüfen der richtigen Benutzer-ID

Sie überprüfen, ob Sie die richtige Benutzer-ID mit dem verwendeten Header bekommen haben, indem Sie zu https://<HPBSM-Server>/topaz/verifyIDM.jsp?headerName=sea wechseln (wenn sea Ihr Header ist).

Kapitel 24

LDAP-Authentifizierung und Zuordnung

Sie können die Benutzerinformationen (Benutzernamen und Kennwörter) für die Authentifizierung auf einem externen LDAP-Server speichern, anstatt den internen BSM-Service zu verwenden. Sie können den LDAP-Server auch zum Synchronisieren von BSM- und LDAP-Benutzern verwenden. Für eine optimale Leistung sollte sich der LDAP-Server im gleichen Subnetz wie der Rest der BSM-Server befinden. Für eine optimale Sicherheit sollte entweder eine SSL-Verbindung zwischen dem BSM-Gatewayserver und dem LDAP-Server konfiguriert werden, oder die BSM- und LDAP-Server sollten sich im gleichen sicheren internen Netzwerksegment befinden.

Die Authentifizierung wird vom LDAP-Server vorgenommen, und die Autorisierung wird vom BSM-Server übernommen.

Sie können den LDAP-Server mit dem Authentifizierungs-Assistenten für die Authentifizierung und die Benutzersynchronisierung konfigurieren. Weitere Informationen zum Assistenten für die Authentifizierung finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

Weitere Informationen zur Sicherung der Kommunikation zwischen einem LDAP-Server und Ihrem BSM-Server über SSL finden Sie unter "Sichern der Kommunikation zwischen LDAP-Server und BSM-Server über SSL" auf Seite 427.

Zuordnen von Gruppen

Sie ordnen Gruppen zu, um die Benutzersynchronisierung zwischen LDAP-Benutzern und BSM-Benutzern zu ermöglichen. Sie können auf die Funktion für die Gruppenzuordnung zugreifen, indem Sie in der Oberfläche von **Benutzer und Berechtigungen** auf die Schaltfläche **LDAP-**

Synchronisierung klicken und **Gruppenzuordnungen** auswählen. Diese Schaltfläche ist nur aktiviert, wenn die folgenden Bedingungen zutreffen:

- Die Option LDAP-Modus auf der Seite Authentifizierungsstrategie ist auf Enabled gesetzt.
- Der Benutzer verfügt über Administratorberechtigungen.

Wenn die Benutzersynchronisierung aktiviert ist, gelten für die Oberfläche der Benutzerverwaltung folgende Einschränkungen:

- Sie können keinen Benutzer erstellen.
- Die Felder Benutzername und Anmeldename sind für einzelne Benutzer deaktiviert.
- Das Feld Kennwort wird nicht angezeigt.
- Sie können Benutzer nicht manuell über die Registerkarte Hierarchie Gruppen zuweisen.

Hinweis: Benutzer, die keiner Gruppe zugewiesen sind, werden auf der Stammebene (Alle) angezeigt und ihre Rolle in Automatisch erstellte Benutzerrollen in Infrastruktureinstellungen unter LDAP-Konfiguration definiert. Falls Sie mehr Kontrolle über Benutzerberechtigungen benötigen, finden Sie weitere Informationen unter "Präzises Steuern der Zuweisung von standardmäßigen Benutzerberechtigungen" auf Seite 422.

Hinweis: Einigen Kunden gefällt das Konzept der automatischen Benutzererstellung, doch bevorzugen sie es, Benutzer manuell den entsprechenden BSM-Gruppen zuzuweisen. Wie jedoch zuvor angemerkt, ist die manuelle Gruppenzuweisung in BSM deaktiviert, wenn die Benutzersynchronisierung aktiviert ist.

Gehen Sie wie folgt vor, um Benutzer manuell der entsprechenden BSM-Gruppe zuzuweisen, wenn die LDAP-Benutzersynchronisierung aktiviert ist:

- 1) Deaktivieren Sie die Benutzersynchronisierung in **Gruppenzuordnungen**.
- 2) Weisen Sie Benutzer manuell über die Registerkarte Hierarchie Gruppen zu.
- 3) Reaktivieren Sie die Benutzersynchronisierung in **Gruppenzuordnungen**.

Sie können wahlweise eine LDAP-Gruppe mehreren BSM-Gruppen oder mehrere LDAP-Gruppen einer BSM-Gruppe zuordnen.

Beim Aktivieren der Funktion für die Gruppenzuordnung können Sie sich mit einem eindeutigen Benutzerattribut, das nur auf dem LDAP-Server vorhanden ist (z. B. eine E-Mail-Adresse), bei BSM anmelden. Weitere Informationen finden Sie unter "Ändern des zur Anmeldung bei BSM verwendeten Attributs" auf Seite 426.

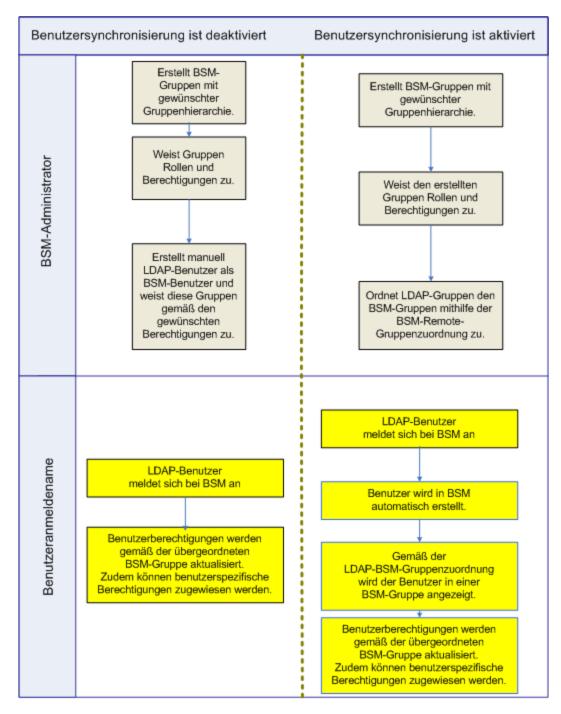
Synchronisieren von Benutzern

Mit der Funktion zur Benutzersynchronisierung werden Benutzer auf einem LDAP-Server Benutzern in BSM zugeordnet. Auf diese Weise wird der Prozess der Benutzerverwaltung für BSM-Administratoren vereinfacht, da alle Benutzerverwaltungsfunktionen über den LDAP-Server durchgeführt werden. Sie sollten Berechtigungen auf Gruppenebene in BSM erteilen und die Benutzer anschließend je nach gewünschter Berechtigungsebene in Gruppen verschachteln. Beim Verschieben von Benutzern zwischen LDAP-Gruppen werden diese nach der Anmeldung bei BSM zwischen den entsprechenden zugeordneten Gruppen auf dem BSM-Server verschoben.

LDAP-Benutzer, die in BSM nicht vorhanden sind und sich anmelden, werden als BSM-Benutzer erstellt. Ihr Status wird wie folgt bestimmt:

- Gehören Benutzer zu einer zugeordneten LDAP-Gruppe, werden sie automatisch der BSM-Gruppe zugewiesen, die ihrer LDAP-Gruppe zugeordnet ist.
- Ist ihre Gruppe keiner BSM-Gruppe zugewiesen oder gehören sie keiner LDAP-Gruppe an, werden sie unter der Gruppe **Stamm** verschachtelt und als BSM-Benutzer mit der Berechtigung **Systemanzeige** erstellt. Ihre Berechtigungen und ihre Benutzerhierarchie können über die Benutzerverwaltungsoberfläche geändert werden.

Das folgende Ablaufdiagramm zeigt den Prozess der Benutzerverwaltung bei Aktivierung von LDAP, wie er vom BSM-Administrator und von BSM bei Anmeldung des Benutzers durchgeführt wird:



Damit ein LDAP-Benutzer sich bei BSM anmelden kann, muss er mit den im Feld **Benutzerfilter** des Dialogfelds **LDAP - Allgemeine Konfiguration** im Assistenten zur Verwaltung von Authentifizierungen definierten Kriterien übereinstimmen. Weitere Informationen zur Seite **LDAP - Allgemeine Konfiguration** finden Sie unter "Dialogfeld "LDAP-Anbieterattribute"" auf Seite 400.

Hinweis: Beachten Sie, dass jeder neue LDAP-Benutzer, der dem Benutzerfilter entspricht, bei der ersten Anmeldung als BSM-Benutzer erstellt wird. Wenden Sie sich an Ihren LDAP-Administrator, um die Filterdefinition so einzugrenzen, dass nur entsprechende Benutzer Zugriff auf BSM erhalten.

Benutzer, die vom LDAP-Server entfernt wurden, werden weiterhin als BSM-Benutzer angezeigt, auch wenn sie nicht länger als LDAP-Benutzer registriert sind und sich nicht bei BSM anmelden können. Diese Benutzer werden als **Veraltete Benutzer** bezeichnet. Weitere Informationen zum Entfernen veralteter Benutzer aus BSM finden Sie unter "Löschen von veralteten Benutzern" auf Seite 428.

Weitere Informationen zum Synchronisieren von LDAP-Benutzern mit BSM-Benutzern finden Sie unter "Zuordnen der Gruppen und Synchronisieren von Benutzern" auf Seite 423.

Weitere Informationen zum Synchronisieren von Gruppen nach der Aktualisierung von einer vorherigen Version von BSM finden Sie unter "Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version von BSM".

Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version von BSM

Beim Durchführen eines Upgrades von einer früheren Version von BSM ist die Einstellung Benutzersynchronisierung aktivieren in den Infrastruktureinstellungen standardmäßig auf False eingestellt. Dies ermöglicht die Zuweisung von LDAP-Gruppen zu Gruppen in BSM über die Schaltfläche LDAP-Konfiguration in der Oberfläche Benutzer und Berechtigungen. Wenn Sie die Gruppen nicht zu diesem Zeitpunkt zuweisen, werden alle BSM-Gruppen unter dem Stammverzeichnis verschachtelt angeordnet.

Nach dem Zuweisen von LDAP- und BSM-Gruppen müssen Sie die Einstellung **Benutzersynchronisierung aktivieren** in den Infrastruktureinstellungen auf **True** festlegen, damit die Benutzer beim Anmelden bei BSM synchronisiert werden.

Weitere Informationen zum Durchführen dieser Aufgabe finden Sie unter "Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version von BSM" auf Seite 425.

Präzises Steuern der Zuweisung von standardmäßigen Benutzerberechtigungen

Wenn Sie eine standardmäßige Gruppenzuordnung für alle Benutzer benötigen, die nicht in eine der aktuell zugewiesenen Gruppen passen, und die BSM-Standardbenutzerrolle (wie für die Infrastruktureinstellung **Automatisch erstellte Benutzerrollen** unter **LDAP-Konfiguration** angegeben) nicht präzise genug ist, verwenden Sie die Funktion für die dynamische LDAP-Gruppe in BSM.

Bitten Sie den LDAP-Serveradministrator Ihres Unternehmens, dass er eine dynamische LDAP-Gruppe basierend auf demselben Benutzerfilter erstellt, den Sie in der LDAP-Konfiguration von BSM angegeben haben.

Dieser Benutzerfilter nimmt automatisch Mitglieder der dynamischen Gruppe in das LDAP Ihres Unternehmens auf.

Erstellen Sie in BSM eine lokale Gruppe mit den Rollen und Berechtigungen, die Sie standardmäßig benötigen. Ordnen Sie die dynamische Gruppe, die Sie in dem LDAP Ihres Unternehmens erstellt haben, der lokalen BSM-Gruppe zu. Jeder Benutzer, der sich bei BSM anmelden darf, aber nicht zu einer anderen zugewiesenen Gruppe gehört, wird der Standardgruppe zugeordnet. Ohne diese Standardgruppe müssten die Benutzer auf Stammebene in der Struktur **Benutzerverwaltung** erstellt werden und ihre Berechtigungen müssten individuell gehandhabt werden.

Um dynamische LDAP-Gruppen in BSM zu aktivieren, wechseln Sie zu Infrastruktureinstellungen, wählen den Kontext LDAP-Einstellungen aus und setzen Dynamische Gruppen aktivieren auf true. Die Änderung wird sofort wirksam.

Vor dem Aktivieren von dynamischen Gruppen werden mit **Benutzer auflisten** im Dialogfeld **Gruppenzuordnungen** unter **Benutzer und Berechtigungen** keine Mitglieder der dynamischen Gruppe angezeigt.

Hinweis: Da die LDAP-Gruppen des Unternehmens sehr groß sein können, werden mit **Benutzer auflisten** nur die ersten 100 Benutzer angezeigt. Um die vollständige Benutzerliste anzuzeigen oder nach bestimmten Benutzem zu suchen, verwenden Sie einen Standard-LDAP-Browser.

Zuordnen der Gruppen und Synchronisieren von Benutzern

In dieser Aufgabe wird beschrieben, wie LDAP-Gruppen zu BSM-Gruppen zugeordnet werden und wie LDAP-Benutzer mit BSM-Benutzern synchronisiert werden:

1. Konfigurieren des LDAP-Servers für das Zuordnen von Gruppen

Sie können den LDAP-Server mit dem Assistenten für die Authentifizierung für die Gruppenzuordnung aktivieren. Details zu Aufgaben finden Sie unter "Assistent für die Authentifizierung" auf Seite 390.

2. Erstellen von BSM-Gruppen und -Hierarchien

Sie erstellen lokale Gruppen in BSM mit den entsprechenden Rollen für die Verschachtelung von Benutzern, wobei die Benutzer die Berechtigungsebene der Gruppe übernehmen, in der sie verschachtelt sind. Weitere Informationen zu dieser Aufgabe finden Sie unter "Ausschnitt "Gruppen/Benutzer" auf Seite 352.

3. Zuordnen von LDAP-Gruppen zu BSM-Gruppen

Sie ordnen Benutzergruppen auf dem LDAP-Server zu Gruppen in BSM zu.

Achtung: Administratoren müssen eine der folgenden Maßnahmen ergreifen, um nicht in BSM gesperrt zu werden, wenn sie sich nach dem Aktivieren des LDAP-Servers, aber vor dem Konfigurieren der Gruppenzuordnung und Benutzersynchronisierung abmelden:

- Sicherstellen, dass die eigene Gruppe zugeordnet wurde, um das Anmelden an BSM zu ermöglichen, nachdem die Synchronisierung aktiviert wurde.
- Erstellen eines Kontos mit Superuser-Berechtigungen in BSM.
- a. Navigieren Sie im Fenster Benutzer und Berechtigungen zum Ausschnitt
 Gruppen/Benutzer, klicken Sie auf die Schaltfläche LDAP-Konfiguration , und

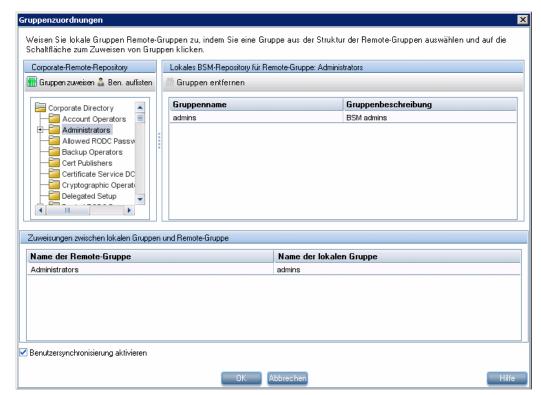
wählen Sie **Gruppenzuordnungen** aus, um das Dialogfeld **Gruppenzuordnungen** zu öffnen.

b. Wählen Sie im Ausschnitt **<Name des Repositorys>-Remote-Repository** eine Remote-LDAP-Servergruppe aus und klicken Sie auf **Gruppen zuweisen**.

Die BSM-Gruppen, die zur ausgewählten LDAP-Gruppe zugeordnet wurden, werden im Ausschnitt Lokales BSM-Repository für Remote-Gruppe: <Gruppenname> angezeigt.

Die bestehende Zuordnung aller LDAP-Gruppen wird im Ausschnitt **Zuweisungen zwischen lokalen Gruppen und Remote-Gruppe** angezeigt.

Kapitel 24: LDAP-Authentifizierung und Zuordnung



Zuordnen von lokalen Gruppen zu Remote-Gruppen:

4. Benutzersynchronisierung aktivieren

Sie aktivieren Sie Synchronisierung von Benutzergruppen auf dem LDAP-Server mit Benutzergruppen in BSM, indem Sie die relevanten Einstellungen auf der Seite **LDAP-Benutzersynchronisierungskonfiguration** im Assistenten für die Authentifizierung vornehmen.

- Bevor Sie die Benutzersynchronisierung aktivieren, stellen Sie sicher, dass Sie entweder ein Superuser-Konto in BSM erstellt haben, das Ihrer eigenen LDAP-Benutzeranmeldung entspricht, oder dass Sie eine entsprechende LDAP-Gruppe zu einer BSM-Gruppe zugeordnet haben, der die Rolle superuser zugewiesen wurde. Falls Sie nicht so vorgehen und sich von BSM abmelden, nachdem Sie LDAP aktiviert haben und bevor die Gruppenzuordnung und Benutzersynchronisierung durchgeführt wurde, wird das unter BSM festgelegte Superuser-Konto für BSM gesperrt.
- Sie deaktivieren die Benutzersynchronisierung und aktivieren die Verwaltung von Benutzern über das Fenster Benutzerverwaltung in BSM, indem Sie das Kontrollkästchen Benutzersynchronisierung aktivieren auf der Seite LDAP-Benutzersynchronisierungskonfiguration unter Benutzerverwaltung > LDAP > Gruppenzuordnungen deaktivieren.

Weitere Informationen zum Synchronisieren von Benutzern über den Assistenten für die Authentifizierung finden Sie unter "Seite "LDAP-Benutzersynchronisierungskonfiguration" auf Seite 401.

Synchronisieren von Benutzern nach dem Upgrade von einer früheren Version von BSM

So synchronisieren Sie LDAP- und BSM-Benutzer nach der Aktualisierung von einer vorherigen Version von BSM:

- Wenn Sie ein Upgrade von einer früheren Version als BSM 7.50 vorgenommen haben, stellen Sie sicher, dass das Kontrollkästchen Benutzersynchronisierung aktivieren auf der Seite LDAP-Benutzersynchronisierungskonfiguration des Assistenten zur Verwaltung von Authentifizierungen deaktiviert ist.
- 2. Stellen Sie sicher, dass LDAP-Gruppen BSM-Gruppen zugeordnet wurden. Weitere Informationen zum Durchführen dieser Aufgabe finden Sie unter "Zuordnen der Gruppen und Synchronisieren von Benutzern" auf Seite 423.
- Navigieren Sie im Assistenten zur Verwaltung von Authentifizierungen zur Seite LDAP-Benutzersynchronisierungskonfiguration und aktivieren Sie das Kontrollkästchen Benutzersynchronisierung aktivieren.

Ändern des zur Anmeldung bei BSM verwendeten Attributs

In dieser Aufgabe wird beschrieben, wie Sie das LDAP-Attribut ändern, mit dem Sie sich bei BSM anmelden.

So ändern Sie das LDAP-Attribut, mit dem Sie sich bei BSM anmelden:

- Navigieren Sie zu Admin > Plattform > Benutzer und Berechtigungen > Authentifizierungsstrategie.
- 2. Klicken Sie auf die Schaltfläche **Konfigurieren**, um den Assistenten zur Verwaltung von Authentifizierungen zu aktivieren.
- 3. Navigieren Sie zur Seite **LDAP Allgemeine Konfiguration** und klicken Sie auf die Schaltfläche **Erweitert**.
- 4. Ändern Sie das **UUID-Attribut** in das Attribut, mit dem Sie sich anmelden wollen, so, wie es auf dem LDAP-Server angezeigt wird.

Sichern der Kommunikation zwischen LDAP-Server und BSM-Server über SSL

- 1. Führen Sie folgende Schritte aus, wenn der LDAP-Server eine sichere Verbindung erfordert:
 - a. Rufen Sie das CA-Stammzertifikat von der Zertifizierungsstelle ab, von der das LDAP-Serverzertifikat ausgegeben wurde.
 - b. Importieren Sie es auf jedem BSM-Gateway (für JRE und JRE64) in den Trust Store der
 - c. Starten Sie die BSM-Gateway-Server neu.

Beispiel:

cd C:\HPBSM\JRE64\bin

keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -keystore ..\lib\security\cacerts cd C:\HPBSM\JRE\bin

keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -keystore ..\lib\security\cacerts :

- Stellen Sie sicher, dass die Kommunikation zwischen dem LDAP-Server und dem BSM-Server über SSL gültig ist. Verwenden Sie dazu den Assistenten zur Verwaltung von Authentifizierungen wie folgt:
 - a. Navigieren Sie zum Assistenten zur Verwaltung von Authentifizierungen, indem Sie
 Admin > Plattform > Benutzer und Berechtigungen > Authentifizierungsverwaltung auswählen, auf Konfigurieren klicken und zur Seite LDAP Allgemein navigieren.
 - b. Geben Sie die URL des LDAP-Servers mit der folgenden Syntax ein: ldaps://computername:port/<bereich>??sub.
 - Stellen Sie sicher, dass es sich bei dem Protokoll um "Idaps://" handelt und die Portnummer gemäß SSL-Port konfiguriert ist, so, wie auf dem LDAP-Server konfiguriert (Standardeinstellung: 636).
 - c. Testen Sie Ihre Konfiguration auf der Seite **LDAP Allgemeine Konfiguration**, indem Sie die UUID und das Kennwort eines bekannten LDAP-Benutzers in die entsprechenden Felder eingeben. Klicken Sie auf **Testen**, um den Benutzer zu authentifizieren. Weitere Informationen finden Sie unter "Seite "LDAP Allgemeine Konfiguration" auf Seite 396.

Löschen von veralteten Benutzern

In dieser Aufgabe wird beschrieben, wie BSM-Benutzer gelöscht werden, die nicht mehr auf dem LDAP-Server vorhanden sind.

Diese Option ist nur aktiviert, wenn die folgenden Bedingungen zutreffen:

- Die Option Repository-Modus für Remote-Benutzer auf der Seite Authentifizierungsstrategie wird auf Enabled gesetzt.
- Der Benutzer verfügt über Berechtigungen zum Löschen.

So löschen Sie veraltete Benutzer:

- Wählen Sie Admin > Plattform > Benutzer und Berechtigungen aus, klicken Sie im Ausschnitt Gruppen/Benutzer auf die Schaltfläche LDAP-Konfiguration , und wählen Sie Veraltete Benutzer löschen aus.
- 2. Wählen Sie den Benutzer aus, den Sie löschen möchten.

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden die Fehlerbehebung und Einschränkungen für die LDAP-Authentifizierung (Lightweight Directory Access Protocol) beschrieben.

- Beim Einrichten des LDAP-Server-URLs: Wenn Sie ein rotes Kreuz mit einer Fehlermeldung wie dieser sehen:
 - FEHLER sun.security.validator.ValidatorException: Fehler beim Erstellen des PKIX-Pfades: sun.security.provider.certpath.SunCertPathBuilderException: Gültiger Zertifizierungspfad zum angeforderten Ziel konnte nicht gefunden werden
 - Sie haben noch keine sichere Verbindung zum LDAP-Server konfiguriert. Weitere Informationen zur Durchführung dieser Aufgabe finden Sie unter "Securing Communication Between an LDAP Server and BSM Server Over SSL" in der PDF-Datei "HP Business Service Management Hardening Guide".
- Wenn BSM mit einer Oracle-Datenbank installiert und die Benutzersynchronisierung mit einem LDAP-Active Directory-Server aktiviert ist, stellen Sie sicher, dass Sie bei der Anmeldung bei BSM die UID mit der richtigen Groß- und Kleinschreibung verwenden, so, wie auf dem LDAP-Server konfiguriert. Dies ist deshalb erforderlich, weil bei der Oracle-Datenbank die Groß-/Kleinschreibung beachtet wird, während sie beim LDAP-Active Directory nicht beachtet wird, sodass die Anmeldung ohne Berücksichtigung der richtigen Groß-/Kleinschreibung zu unerwünschten Resultaten führen kann.

Wenn sich beispielsweise ein auf dem LDAP-Active Directory-Server vorhandener Benutzer namens **testuser** bei BSM anmeldet, wird er automatisch als BSM-Benutzer **testuser** erstellt, dem in der Oberfläche der BSM-Benutzerverwaltung Berechtigungen zugewiesen werden können. Wenn Sie sich dann bei BSM als **Testuser** anmelden, sendet der LDAP-Active Directory-Server eine Bestätigung, dass der Benutzer vorhanden ist (weil Active Directory die Groß-/Kleinschreibung nicht berücksichtigt) und dieser erhält dann Zugang zu BSM. Da die Oracle-Datenbank diesen Benutzer jedoch nicht als **testuser** erkennt (da die Oracle-Datenbank die Groß-/Kleinschreibung berücksichtigt, wird der Benutzer **Testuser** als neuer Benutzer behandelt, ohne die Berechtigungen, die **testuser** zugewiesen wurden.

Kapitel 25

LW-SSO-Authentifizierung – Allgemeine Referenz

Bei LW-SSO handelt es sich um eine Methode der Zugangskontrolle, bei der Benutzer nach einmaliger Anmeldung Zugriff auf die Ressourcen verschiedener Softwaresysteme erhalten, ohne dass sie sich erneut anmelden müssen. Die Anwendungen der konfigurierten Gruppe von Softwaresystemen vertrauen der Authentifizierung und beim Wechsel von einer Anwendung zu einer anderen ist keine weitere Authentifizierung mehr erforderlich.

Die in diesem Kapitel enthaltenen Informationen beziehen sich auf die LW-SSO-Version 2.4.

LW-SSO-Token-Ablaufdatum

Der Ablaufwert des LW-SSO-Tokens bestimmt die Gültigkeit der Applikationssitzung. Aus diesem Grund sollte der Ablaufwert mindestens so hoch gewählt werden, wie der Ablaufwert der Applikationssitzung.

Empfohlene Konfiguration des LW-SSO-Token-Ablaufs

Jede Applikation, die LW-SSO verwendet, muss den Token-Ablauf konfigurieren. Der Standardwert ist 60 Minuten. Für Applikationen, die keine hohe Sicherheitsstufe erfordern, kann auch ein Wert von 300 Minuten gewählt werden.

GMT-Zeit

Alle Applikationen, die Teil einer LW-SSO-Integration sind, müssen dieselbe GMT-Zeit mit einer maximalen Abweichung von 15 Minuten verwenden.

Mehrdomänen-Funktionalität

Die Mehrdomänen-Funktionalität erfordert, dass alle Applikationen einer LW-SSO-Integration die **trustedHosts**-Einstellungen (oder die **protectedDomains**-Einstellungen) konfigurieren, wenn eine Integration mit Applikationen in verschiedenen DNS-Domänen erforderlich ist. Zudem muss im **Iwsso**-Element der Konfiguration die richtige Domäne hinzugefügt werden.

Abruf des SecurityToken für URL-Funktionalität

Um die Informationen empfangen zu können, die von anderen Applikationen als SecurityToken für eine URL gesendet werden, muss die Host-Applikation die richtige Domäne im Iwsso-Element der Konfiguration konfigurieren.

LW-SSO-Systemanforderungen

Die folgende Tabelle enthält die Anforderungen für eine LW-SSO-Konfiguration:

Applikation	Version	Kommentare
Java	1.5 und höher	
HTTP-Servlets-API	2.1 und höher	
Internet Explorer	6.0 und höher	Der Browser muss den HTTP-Sitzungs-Cookie und die HTTP 302 Redirect-Funktionalität aktivieren
FireFox	2.0 und höher	Der Browser muss den HTTP-Sitzungs-Cookie und die HTTP 302 Redirect-Funktionalität aktivieren
JBoss-	JBoss 4.0.3	
Authentifizierungen	JBoss 4.3.0	
Tomcat- Authentifizierungen	Standalone Tomcat 6.0.29	
	Standalone Tomcat 5.0.28	
	Standalone Tomcat 5.5.20	
Acegi-	Acegi 0.9.0	
Authentifizierungen	Acegi 1.0.4	
Spring Security- Authentifizierungen	Spring Security 2.0.4	
Webdienste-	Axis 1 - 1.4	
Engines	Axis 2 - 1,2	
	JAX-WS-RI 2.1.1	

LW-SSO-Sicherheitswarnungen

Dieser Abschnitt beschreibt die Sicherheitswarnungen einer LWSSO-Konfiguration:

 Vertraulicher InitString-Parameter in LW-SSO. LW-SSO verwendet Symmetric Encryption zum Validieren und Erstellen eines LW-SSO-Token. Der initString-Parameter innerhalb der Konfiguration wird für die Initialisierung des Sicherheitsschlüssels verwendet. Eine Applikation erstellt ein Token und jede Applikation, die denselben initString-Parameter verwendet, validiert das Token.

Achtung:

- LW-SSO kann nicht ohne das Festlegen des initString-Parameters verwendet werden.
- Der initString-Parameter enthält vertrauliche Informationen und muss als solche in Bezug auf Veröffentlichung, Transport und Persistenz behandelt werden.
- Der initString-Parameter darf nur zwischen Applikationen ausgetauscht werden, die Teil einer LW-SSO-Integration sind.
- Der initString-Parameter sollte mindestens 12 Zeichen umfassen.
- Authentifizierungssicherheitsstufe. Die Applikation, die das unsicherste Authentifizierungs-Framework verwendet, und ein LW-SSO-Token ausgibt, dem andere integrierte Applikationen vertrauen, legt die Authentifizierungssicherheitsstufe für alle Applikationen fest.

Sie sollten die Umgebung so einrichten, dass nur Applikationen mit einem sehr sicheren Authentifizierungs-Framework LW-SSO-Token ausgeben.

- Symmetrische Verschlüsselungsimplikationen. LW-SSO verwendet die symmetrische
 Kryptografie für die Ausgabe und Validierung von LW-SSO-Token. Aus diesem Grund kann jede
 Applikation, die LW-SSO verwendet, ein Token ausgeben, dem von allen Applikationen vertraut
 wird, die denselben initString-Parameter verwenden. Dieses potentielle Risiko entsteht, wenn
 sich eine Applikation, die einen gemeinsamen initString verwendet, an einem unsicheren
 Speicherort befindet oder auf diese Applikation von einen unsicheren Speicherort zugegriffen
 werden kann.
- Benutzerzuordnung (Synchronisation). Das LW-SSO-Framework stellt nicht die Benutzerzuordnung zwischen den integrierten Applikationen sicher. Aus diesem Grund muss die integrierte Applikation die Benutzerzuordnung überwachen. Wir empfehlen, dass Sie dieselbe Benutzerregistrierung (wie LDAP/AD) für alle integrierte Applikationen verwenden.

Fehler bei der Benutzerzuordnung können zu Sicherheitslücken und fehlerhaftem Applikationsverhalten führen. So kann zum Beispiel derselbe Benutzername unterschiedlichen real existierenden Benutzern in verschiedenen Anwendungen zugewiesen sein.

Zudem kann es in Fällen, bei denen sich ein Benutzer an einer Applikation (AppA) anmeldet und dann auf eine zweite Applikation (AppB), die Container- oder Applikationsauthentifizierung verwendet, zugreift, sein, dass sich der Benutzer aufgrund eines Zuordnungsfehlers manuell an AppB anmelden und dabei seinen Benutzernamen eingeben muss. Verwendet der Benutzer dann einen anderen Benutzernamen als den Benutzernamen, mit dem er sich an AppA angemeldet hat, kann folgendes Verhalten auftreten: Meldet sich der Benutzer über die AppA oder AppB an einer

weiteren Applikation (AppC) an, wird der Zugriff auf AppC mit dem Benutzernamen, der für AppA oder AppB entsprechend verwendet wurde, hergestellt.

• Identity Management. Dieser Manager wird für Authentifizierungszwecke verwendet. Alle nicht geschützten Ressourcen in diesem Manager müssen mit der Einstellung nonsecureURLs in der LW-SSO-Konfigurationsdatei konfiguriert werden.

Fehlerbehebung und Einschränkungen

Bekannte Probleme

In diesem Abschnitt werden die bei der LW-SSO-Authentifizierung bekannten Probleme beschrieben.

 Sicherheitskontext. Der LW-SSO-Sicherheitskontext unterstützt nur einen Attributwert pro Attributname.

Aus diesem Grund wird von dem LW-SSO-Framework nur ein Name angenommen, wenn das SAML2-Token mehrere Werte für denselben Attributnamen sendet.

Gleiches gilt, wenn das IdM-Token so konfiguriert ist, dass es mehrere Werte für denselben Attributnamen sendet: Das LW-SSO-Framework nimmt nur einen Namen an.

 Mehrdomänen-Abmelde-Funktionalität bei der Verwendung von Internet Explorer 7. Bei der Mehrdomänen-Abmelde-Funktionalität kann es bei der Verwendung von Internet Explorer 7 zu Fehlern kommen. Dabei ruft die Anwendung mehr als 3 aufeinanderfolgende HTTP 302-Redirect-Verben in der Abmeldeprozedur auf.

In diesem Fall ist es möglich, dass Internet Explorer 7 die HTTP 302-Redirect-Antwort falsch interpretiert und stattdessen die Fehlerseite **Die Webseite kann nicht angezeigt werden.** anzeigt.

Als Umgehungslösung sollten Sie die Anzahl der Befehle für die Applikationsweiterleitung in der Abmeldebefehlsfolge verringern, sofern dies möglich ist.

Einschränkungen

Beachten Sie die folgenden Einschränkungen bei der Verwendung der LW-SSO-Authentifizierung:

Client-Zugriff auf die Applikation.

Wenn in der LW-SSO-Konfiguration eine Domäne definiert ist:

- Die Applikationsclients müssen unter Verwendung des vollständig qualifizierten Domänennamens (FQDN) in der Anmelde-URL auf die Applikation zugreifen. Beispiel: http://MeinServer.Unternehmensdomäne.com/WebApp.
- LW-SSO unterstützt keine URLs mit einer IP-Adresse. Beispiel: http://192.168.12.13/WebApp.
- LW-SSO unterstützt keine URLs ohne Domäne. Beispiel: http://MeinServer/WebApp.

Wenn in der LW-SSO-Konfiguration keine Domäne definiert ist: Der Client kann ohne die Verwendung der FQDN in der Anmelde-URL auf die Applikation zugreifen. In diesem Fall wird ein für den Computer spezifisches LW-SSO-Sitzungs-Cookie ohne Domäneninformation erstellt. Aus diesem Grund wird der Cookie nicht von einem Browser an einen anderen delegiert und nicht an andere Computer in derselben DNS-Domäne weitergegeben. Dies bedeutet, dass LW-SSO innerhalb derselben Domäne nicht funktioniert.

- LW-SSO-Framework-Integration. Applikationen können die LW-SSO-Funktionalität nur nutzen und erweitern, wenn sie zuvor in das LW-SSO-Framework integriert wurden.
- Mehrdomänen-Funktionalität.

- Die Mehrdomänen-Funktionalität basiert auf HTTP-Referenzen. Aus diesem Grund unterstützt LW-SSO Links von einer Applikation zu einer anderen, jedoch nicht die Eingabe einer URL in ein Browserfenster, sofern sich beide Applikationen nicht in derselben Domäne befinden.
- HTTP POST wird nicht unterstützt, wenn es im ersten Link über Domänengrenzen verwendet wird.

Die Mehrdomänen-Funktionalität unterstützt nicht die erste HTTP POST-Anfrage an eine zweite Applikation (es wird nur die HTTP GET-Anfrage unterstützt). Enthält Ihre Applikation beispielsweise einen HTTP-Link zu einer zweiten Applikation wird eine HTTP GET-Anfrage unterstützt; eine HTTP FORM-Anfrage jedoch nicht. Nach der ersten Anfrage können alle weiteren Anfragen entweder HTTP POST- oder HTTP GET-Anfragen sein.

■ LW-SSO-Token-Größe:

Die Größe der Informationen, die LW-SSO von einer Applikation in einer Domäne an eine andere Applikation in einer anderen Domäne übertragen kann, ist auf 15 Gruppen/Rollen/Attribute begrenzt (jedes Objekt kann dabei etwa 15 Zeichen lang sein).

■ Links von einer geschützten (HTTPS) zu einer ungeschützten (HTTP) Seite in einem Mehrdomänenszenario:

Die Mehrdomänen-Funktionalität kann nicht verwendet werden für Links von einer geschützten (HTTPS) zu einer ungeschützten (HTTP) Seite. Hierbei handelt es sich um eine Browsereinschränkung, die verhindert, dass der Referenz-Header bei Links von einer geschützten (HTTPS) zu einer ungeschützten (HTTP) Ressource gesendet wird.

Verhalten von Cookies anderer Domänen in Internet Explorer:

Microsoft Internet Explorer 6 enthält ein Modul, welches das "Platform for Privacy Preferences (P3P) Project" unterstützt. Dies bedeutet, dass Cookies, die von einer anderen Domäne kommen, standardmäßig in der Sicherheitszone **Internet** blockiert werden. Sitzungs-Cookies werden durch den Internet Explorer ebenfalls als Cookies aus anderen Domänen behandelt und aus diesem Grund blockiert, weswegen LW-SSO nicht funktioniert.

Um dieses Problem zu vermeiden, müssen Sie die aufgerufene Anwendung (oder eine Untergruppe der DNS-Domäne als *.MeineDomäne.com) zur Zone **Lokales Intranet** oder **Vertrauenswürdige Sites** auf Ihrem Computer hinzufügen (wählen Sie beispielsweise in Microsoft Internet Explorer **Menü > Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites > Erweitert**). Anschließend wird das Cookie angenommen.

Achtung: Der LW-SSO-Sitzungs-Cookie ist nur ein Cookie von mehreren Cookies, die von der blockierten Drittanbieterapplikation verwendet werden.

SAML2-Token.

■ Abmelde-Funktionalität wird nicht bei Verwendung des SAML2-Token unterstützt.

Aus diesem Grund wird ein Benutzer, der sich bei der Verwendung des SAML2-Token (für den Zugriff auf eine zweite Applikation) von der ersten Applikation abmeldet, nicht von der zweiten Applikation abgemeldet.

■ Der SAML2-Token-Ablauf wird nicht in der Sitzungsverwaltung der Applikation verwaltet.

Aus diesem Grund wird bei der Verwendung des SAML2-Token für den Zugriff auf die zweite Applikation die Sitzungsverwaltung jeder Applikation getrennt geführt.

- JAAS-Realm. Der JAAS-Realm in Tomcat wird nicht unterstützt.
- Verwenden von Leerzeichen in Tomcat-Verzeichnissen. Das Verwenden von Leerzeichen in Tomcat-Verzeichnissen wird nicht unterstützt.
 - LW-SSO kann nicht verwendet werden, wenn ein Tomcat-Installationspfad (Ordner) Leerzeichen enthält (Beispiel: Program Files) und sich die LW-SSO-Konfigurationsdatei im Tomcat-Ordner **common\classes** befindet.
- Load Balancer-Konfiguration. Ein Load Balancer, der über LW-SSO bereitgestellt wird, muss für die Verwendung von Sticky-Sitzungen konfiguriert werden.

Teil 5

Reports und Warnungsverwaltung

Kapitel 26

Report Schedule Manager

Benutzer mit Administratorberechtigungen können geplante Reports im Report Schedule Manager bearbeiten, löschen, wiederaufnehmen oder anhalten. Sie planen Filter-FavoritenBenutzerreports (benutzerdefinierte Reports, Trend-Reports, Service-Reports) und Filter-Favoriten im Report Manager, um zu ermöglichen, dass bestimmte Empfänger in bestimmten festgelegten Intervallen den angegebenen Report automatisch per E-Mail erhalten. Weitere Informationen zum Planen von Benutzer-Reports finden Sie unter How to Create and Manage User Reports Using Report Manager im BSM-Benutzerhandbuch.

Manager "Report-Planung" - Hauptseite

Auf dieser Seite können Sie Zeitpläne für Filter-Favoriten in der Report-Planung verwalten.

Zugriff	Wählen Sie Admin > Plattform > Report-Planung aus.
Wichtiger Hinweis	Sie können auf der Hauptseite der Report-Planung keinen neuen Zeitplan erstellen. Weitere Informationen zum Erstellen von Zeitplänen finden Sie unter "How to Create and Manage User Reports Using Report Manager" im BSM-Benutzerhandbuch.
Relevante Aufgaben	"How to Create and Manage User Reports Using Report Manager" im BSM-Benutzerhandbuch.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Element der	
Oberfläche	Beschreibung
0	Klicken Sie hier, um das Dialogfeld Zeitplan bearbeiten zu öffnen und die Zeitplankonfiguration zu bearbeiten. Details finden Sie unter Create New Schedule Dialog Box.
&	Öffnet das Dialogfeld Zeitplan bearbeiten für <report-name></report-name> , in dem Sie den ausgewählten Zeitplan bearbeiten können. Weitere Informationen finden Sie unter "Create New Schedule Dialog Box" im BSM-Benutzerhandbuch.
	Hinweis: In diesem Dialogfeld können Sie lediglich vorhandene Zeitpläne bearbeiten – neue Zeitpläne werden über die Report-Planung-Benutzeroberfläche erstellt. Weitere Informationen finden Sie unter "Create New Schedule Dialog Box" im BSM-Benutzerhandbuch.
®	Löscht den ausgewählten Zeitplan.
0	Nimmt den ausgewählten Zeitplan wieder auf.
6	Hält den ausgewählten Zeitplan an.
Ф	Aktualisiert die Seite der Report-Planung.
000	Setzt die Breite der Spalten auf die Standardeinstellung zurück.
	Ermöglicht die Auswahl der Spalten, die in der Tabelle angezeigt werden sollen.
Zeitpunkt der Erstellung	Der Zeitpunkt (in der angegebenen Zeitzone), zu der der Zeitplan generiert werden soll.

Element der Oberfläche	Beschreibung
Empfänger	Die in der Report-Planung konfigurierten Personen, die den Report bzw. das Reportelement in den geplanten Intervallen erhalten sollen. Weitere Informationen zum Konfigurieren von Zeitplänen finden Sie unter "Creating a New Schedule Dialog Box" im BSM-Benutzerhandbuch.
Serie	Das Serien-Pattern für den ausgewählten Zeitplan.
Report- Name	Der Name des Reports, für den der Zeitplan konfiguriert ist.
Report- Typ	Der Typ des Reports, für den der Zeitplan konfiguriert ist.
Status	Der Status des Zeitplans. Mögliche Werte:
	Aktiv
	Ausgesetzt

Kapitel 27

Einrichten eines Bereitstellungssystems für Warnungen

BSM informiert Sie durch die Auslösung von Warnungen proaktiv, wenn vordefinierte Leistungslimits überschritten werden.

Details zu Aufgaben finden Sie unter "Einrichten eines Bereitstellungssystems für Warnungen" auf Seite 445.

Dieser Abschnitt umfasst die folgenden Themen:

- "Empfänger von Warnungen"
- "Benachrichtigungsvorlage"
- "Warnungsschemata"
- "Öffnen von Ereignissen in OM" auf der nächsten Seite
- "Warnungshistorie" auf der nächsten Seite
- "Übermittlung von Warnungen" auf der nächsten Seite

Empfänger von Warnungen

Warnungen können so konfiguriert werden, dass Benachrichtigungen an bestimmte Empfänger gesendet werden. Details zu Aufgaben zum Konfigurieren von Empfängern finden Sie unter "Empfängerverwaltung" auf Seite 358.

Benachrichtigungsvorlage

Für jeden Empfänger können eine Benachrichtigungsmethode (eine beliebige Kombination von E-Mail, Pager und/oder SMS) sowie die Vorlage für die Warnungsbenachrichtigung festgelegt werden. Es ist auch möglich, einen Benachrichtigungszeitplan für die Warnungen zu erstellen. Weitere Informationen finden Sie unter "Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 464.

Warnungsschemata

In jedem Warnungsschema definieren Sie einen eindeutigen Satz an Eigenschaften. Nach der Erstellung eines Warnungsschemas können Sie dieses in der entsprechenden Benutzeroberfläche für Warnungen anzeigen und bearbeiten. Detaillierte Tipps und Richtlinien finden Sie unter "Planen von effektiven Warnungsschemata" auf Seite 444.

Für folgende Elemente können Warnungen konfiguriert und Empfänger zu Warnungen zugewiesen werden:

• Cls in einer Ansicht. Cl-Status-Warnungen werden von einer vordefinierten Statusänderung für das ausgewählte Konfigurationselement (Cl, Configuration Item) ausgelöst, die von der Business Logic Engine ermittelt wurde. Weitere Informationen finden Sie unter "Cl Status Alerts Administration" im BSM-Benutzerhandbuch.

- HP Service Manager öffnet automatisch Vorfälle, sobald eine CI-Status-Warnung in BSM ausgelöst wird. Weitere Informationen finden Sie unter HP Service Manager im Abschnitt zur BSM-Plattform auf der HP Software Integrations-Website.
- SLAs. Warnungen zum SLA-Status werden durch Statusänderungen an einem zentralen Leistungsindikator von SLA ausgelöst. Weitere Informationen finden Sie unter "SLA Alerts Administration" im BSM-Benutzerhandbuch.
- EUM-Warnungen. EUM-Warnungen werden ausgelöst, wenn vordefinierte Bedingungen wie beispielsweise Transaktionsantwortzeit, Verfügbarkeit, Erfolg bzw. Fehlschlagen oder die Fertigstellungszeit erreicht werden. Weitere Informationen finden Sie unter "End User Management Alerts Administration" im BSM-Benutzerhandbuch.

Öffnen von Ereignissen in OM

Ereignisse können in OM automatisch geöffnet werden, wenn eine CI-Status-Warnung, eine SLA-Warnung oder eine EUM-Warnung in BSM ausgelöst werden. Weitere Informationen finden Sie unter "Operations Manager" im Abschnitt zur BSM-Plattform auf der HP Software Integrations-Website.

Warnungshistorie

Sie können die Historie der Warnungen an den folgenden Stellen anzeigen:

- Registerkarte "Report für CI-Status-Warnungen". Ermöglicht Ihnen das Auflisten aller CI-Status-Warnungen, die während des angegebenen Zeitbereichs ausgelöst wurden. Weitere Informationen finden Sie unter "Report "CI-Status-Warnungen" im BSM-Benutzerhandbuch.
- Registerkarte "Report für SLA-Warnungen". Ermöglicht Ihnen das Auflisten aller Service Level Management-Warnungen, die während des angegebenen Zeitbereichs ausgelöst wurden. Weitere Informationen finden Sie unter "Report "Warnungsprotokoll" im BSM-Benutzerhandbuch.
- Registerkarte "Report für EUM-Warnungen". Ermöglicht den Zugriff auf die folgenden Reports:
- Report zum Warnungsprotokoll. Ermöglicht Ihnen das Nachvollziehen aller Einzelheiten für EUM-Warnungen, die von BSM während des angegebenen Zeitbereichs gesendet wurden. Weitere Informationen finden Sie unter "Report "Warnungsprotokoll" im BSM-Benutzerhandbuch.
- Report zur Warnungsanzahl im Verlauf. Ermöglicht Ihnen die Anzeige einer Übersicht über die Häufigkeit von Warnungen. Weitere Informationen finden Sie unter "Report "Warnungsanzahl im Verlauf" im BSM-Benutzerhandbuch.

Übermittlung von Warnungen

Falls die Onlinekomponenten ausfallen sollten, stellt die Applikation **Warnungen** sicher, dass die Daten standardmäßig für die Dauer einer Stunde im Bus gespeichert werden. Wenn die Komponenten wieder online sind, erzeugt die Warn-Engine Warnungen aus den Daten im Bus.

Warnungen und Ausfallzeiten

Beim Konfigurieren einer CI-Status-Warnung sollten Sie bedenken, dass sich Ausfallzeiten auf die CIs auswirken und deren Daten verzerren können.

Wenn Sie ein EUM-Warnungsschema für CIs konfigurieren, deren Status auf Daten aus Business Process Monitor- oder SiteScope-Datenquellen basiert, sollten Sie ebenfalls bedenken, dass sich Ausfallzeiten auf die CIs auswirken und die CI-Daten verzerren können.

Sie können entscheiden, in Ausfallzeiten eine CI-Statuswarnung oder eine EUM-Warnung auszulösen. Ausführliche Informationen zu dem Themenbereich Ausfallzeiten finden Sie unter "Ausfallzeitenverwaltung" auf Seite 221.

Um anzugeben, wie CI-Statuswarnungen und EUM-Warnungen in Ausfallzeiten gehandhabt werden sollen, wählen Sie **Admin > Plattform > Ausfallverwaltung** aus und legen eine der folgenden Optionen fest:

- Keine Aktion
- Warnungen unterdrücken und Ereignisse schließen
- Ausfallzeit für KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen
- Ausfallzeit für Reports und KPI-Berechnungen erzwingen; Warnungen unterdrücken und Ereignisse schließen
- Aktive Überwachung beenden (BPM & SiteScope); Ausfallzeit für Reports und KPI-Berechnungen erzwingen, Warnungen unterdrücken und Ereignisse schließen (wirkt sich auf alle zugehörigen SLAs aus)

Wenn bei CIs eine geplante Ausfallzeit vorliegt, werden bei keiner der oben genannten Optionen mit Ausnahme von **Keine Aktion** CI-Status- oder EUM-Warnungen gesendet.

CI-Warnungen werden auch dann gesendet, wenn eine der oben genannten Optionen (mit Ausnahme von **Keine Aktion**) ausgewählt ist, sofern Sie die Warnungen so konfiguriert haben, dass sie bei einer Änderung des CI-Status in **Ausfallzeit** gesendet wird. Informationen zur Benutzeroberfläche finden Sie unter "General Page" im Handbuch BSM-Benutzerhandbuch.

Details zu Aufgaben finden Sie unter "Einrichten eines Bereitstellungssystems für Warnungen" auf Seite 445.

Informationen zur Benutzeroberfläche finden Sie unter "Seite "Ausfallzeitenverwaltung" auf Seite 229.

Planen von effektiven Warnungsschemata

Vor dem Erstellen von Warnungsschemata sollten Sie sich überlegen, wie Benutzer am wirkungsvollsten bei Leistungsproblemen gewarnt werden können. Die weiter unten beschriebenen Verfahren können Ihnen bei der effektiven Warnungsplanung behilflich sein.

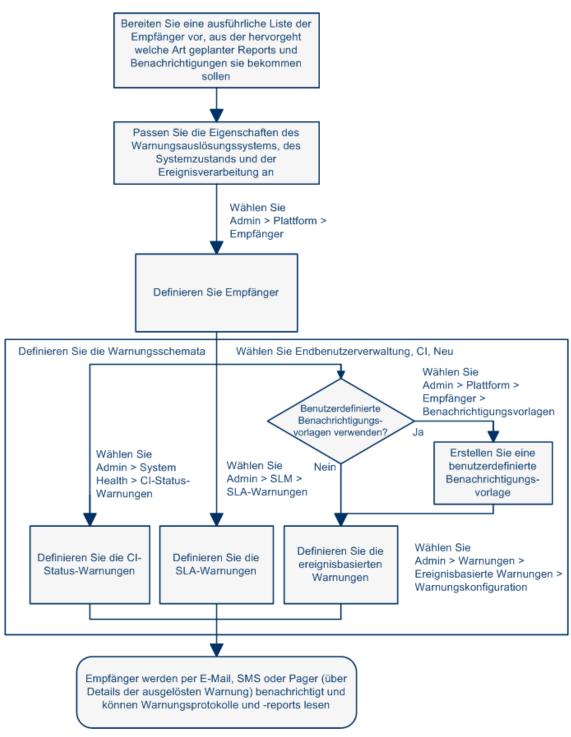
Hinweis: HP Professional Services bietet Beratung zu den bewährten Methoden im Hinblick auf dieses Thema. Informationen dazu, wie Sie diesen Service erhalten, bekommen Sie von Ihrem HP-Vertreter.

- Beim Erstellen von Warnungsschemata teilen Sie die Warnungen nach Schweregrad ein.
 Erstellen Sie kritische Warnungen für Ereignisse, die eine sofortige Korrektur erfordern
 (beispielsweise Transaktionsfehler oder exzessive Antwortzeiten für kritische Transaktionen).
 Erstellen Sie nichtkritische Warnungen für Ereignisse, die eine frühe Benachrichtigung erfordern
 (beispielsweise langsame Antwortzeiten).
- Legen Sie die Benutzer fest, die die verschiedenen Warnungstypen erhalten sollen, und wählen Sie die Sendemethode, die am besten zu dem jeweiligen Warnungstyp passt. Beispielsweise ist das Senden über Pager möglicherweise bei kritischen Warnungen besser geeignet als die E-Mail-Methode. Beim Festlegen der Sendemethode sollten Sie auch die Tageszeit in Betracht ziehen. Eine E-Mail-Warnung ist möglicherweise außerhalb der Bürozeiten wenig nützlich.
- Richten Sie BSM für die Warnung bei wiederkehrenden Problemen ein und nicht für einmalige Ereignisse. Wiederkehrende Warnungen sind der genaueste Hinweis auf Probleme mit Ihrer Applikation. Als Faustregel sollten Sie die Anzahl der wiederkehrenden Warnungen mit der Anzahl der Business Process Monitor-Standorte vergleichen, von denen aus Sie eine Überwachung durchführen. Wenn beispielsweise drei Fehler aufgetreten sind und Sie die Überwachung von 100 Standorten aus durchführen, ist das nicht so kritisch wie bei fünf Fehlern in fünf Standorten.

Einrichten eines Bereitstellungssystems für Warnungen

In dieser Aufgabe und dem verbundenen Prozessdiagramm wird die Einrichtung eines Systems für die Bereitstellung von Warnungen für Empfänger beschrieben.

Einrichten eines Bereitstellungssystems für Warnungen – Flussdiagramm



1. Planen der Anforderungen für Warnungsempfänger

Folgendes wird empfohlen:

- Listen Sie die erforderlichen Empfänger von Warnungen auf, einschließlich Kontaktinformationen und die erforderliche Sendemethode für den Empfänger (E-Mail, SMS, Pager). Vorschläge zur Vorgehensweise finden Sie unter "Planen von effektiven Warnungsschemata" auf Seite 444.
- Legen Sie die Typen von Warnungen fest, die Sie bereitstellen möchten. Details zu den unterschiedlichen Warnungstypen finden Sie unter "Einrichten eines Bereitstellungssystems für Warnungen" auf der vorherigen Seite..

2. Festlegen der entsprechenden Benutzerberechtigungen

Legen Sie die entsprechenden Benutzerberechtigungen fest für:

- EUM-Warnungen.
- Sie k\u00f6nnen f\u00fcr jede Applikation festlegen, ob ein Benutzer die Berechtigung Anzeigen oder Vollzugriff haben soll. W\u00e4hlen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, erstellen/bearbeiten Sie einen Benutzer, klicken Sie im Kontext End User Management auf Berechtigungen und w\u00e4hlen Sie den Kontext Business Service Management > Applikationen > <\u00e4pplikation> > Warnungen aus.
- Sie müssen auch die Berechtigung für die CEM-Ereignisvorlage auswählen. Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, erstellen/bearbeiten Sie einen Benutzer, klicken Sie im Kontext End User Management auf Berechtigungen und wählen Sie Warnung - Benachrichtigungsvorlage aus.
- CI-Status-Warnungen. Sie können für jede Ansicht festlegen, ob ein Benutzer die Berechtigung Ändern, Anzeigen, Löschen oder Vollzugriff haben soll. Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, erstellen/bearbeiten Sie einen Benutzer, klicken Sie im Kontext RTSM auf Berechtigungen und wählen Sie den Kontext Business Service Management > Ansichten > <ansicht_name> aus.
- SLA-Warnungen. Sie können pro SLA festlegen, ob ein Benutzer die Berechtigung Hinzufügen, Ändern, Anzeigen, Löschen oder Vollzugriff haben soll. Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, erstellen/bearbeiten Sie einen Benutzer, klicken Sie im Kontext Service Level Management auf Berechtigungen und wählen Sie den Kontext Business Service Management > SLAs > <sla_name> aus.
- Externe Aktionen für Warnungen (Ausführbare Datei ausführen, SNMP-Trap senden oder In Ereignisanzeige protokollieren). Sie können auf globaler Ebene festlegen, ob ein Benutzer die Berechtigung Ändern oder Vollzugriff haben soll. Wählen Sie Admin > Plattform > Benutzer und Berechtigungen > Benutzerverwaltung aus, erstellen/bearbeiten Sie einen Benutzer, klicken Sie im Kontext Plattform auf Berechtigungen und wählen Sie separat voneinander die Kontexte Business Service Management > Ausführbare Datei ausführen, SNMP-Trap senden oder In Ereignisanzeige protokollieren aus.

■ Die Benachrichtigungsvorlage, die Sie für die Warnungen festlegen können. Sie können für die Vorlage festlegen, ob ein Benutzer die Berechtigung Hinzufügen, Ändern, Anzeigen, Löschen oder Vollzugriff haben soll. Wählen Sie hierzu Admin > Plattform > Benutzer und Berechtigungen> Benutzerverwaltung, erstellen/bearbeiten Sie einen Benutzer und klicken Sie auf Berechtigungen. Wählen Sie im Kontext End User Management den Kontext Business Service Management > Systemempfänger-Vorlage aus. Diese Berechtigungen werden auf globaler Ebene definiert.

Informationen zur Benutzeroberfläche finden Sie unter "Operationen" auf Seite 252.

3. Festlegen der Warnungsauslösung während Ausfallzeiten

Wenn Sie eine CI-Statuswarnung oder ein EUM-Warnungsschema für CIs konfigurieren, deren bzw. dessen Status auf Daten aus Business Process Monitor- oder SiteScope-Datenquellen basiert, können sich Ausfallzeiten auf die CIs auswirken und die CI-Daten verzerren.

Sie können entscheiden, in Ausfallzeiten eine CI-Statuswarnung oder eine EUM-Warnung auszulösen. Um anzugeben, wie CI-Statuswarnungen und EUM-Warnungen in Ausfallzeiten gehandhabt werden sollen, wählen Sie **Admin > Plattform > Ausfallzeit** aus und legen eine der verfügbaren Optionen fest.

Details zum Konzept finden Sie unter "Warnungen und Ausfallzeiten" auf Seite 443.

Informationen zur Benutzeroberfläche finden Sie unter "Seite "Ausfallzeitenverwaltung"" auf Seite 229.

4. Anpassen der Eigenschaften des Warnungsauslösungssystems, des Warnungssystemzustands und der Ereignisverarbeitung – optional

Passen Sie die Eigenschaften des Warnungsauslösungssystems, des Systemzustands und der Ereignisverarbeitung an. Weitere Informationen finden Sie unter "Anpassen von Warnungen" auf Seite 449.

5. Definieren von Empfängern

Auf der Seite **Empfänger** definieren Sie die Empfänger von Warnungen (außer SiteScope-Warnungen). Sie können E-Mail, SMS oder Pager als Sendemethoden festlegen. Geben Sie bei Bedarf spezifische Zeitpläne für das Senden von Warnungen ein (zum Beispiel Empfänger, die während der Geschäftszeiten oder nur am Abend oder an Wochenenden Warnungen erhalten sollen). Weitere Informationen finden Sie unter "Registerkarte "Empfänger" (Benutzerverwaltung)" auf Seite 344.

6. Erstellen benutzerdefinierter Benachrichtigungsvorlagen – optional

Bei Bedarf haben Sie bei der Definition von EUM-Warnungen die Möglichkeit, benutzerdefinierte Benachrichtigungsvorlagen zu erstellen, die das Format und die in Warnungs-E-Mails enthaltenen Informationen anpassen. Weitere Informationen finden Sie unter "Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 464.

 Festlegen, dass in Operations Manager und in Operationenverwaltung bei der Auslösung einer Warnung in BSM ein Ereignis geöffnet werden soll

Sie können festlegen, dass in Operations Manager und Operations Management Ereignisse geöffnet werden sollen, wenn in BSM eine Warnung ausgelöst wird. Weitere Informationen

finden Sie unter Operations Manager im Abschnitt zur BSM-Plattform auf der HP Software Integrations-Website.

8. Ergebnis – Definieren der Warnungsschemata

Sie haben die Warnungsschemata geplant, die entsprechenden Empfänger eingerichtet, die allgemeinen Warnungseinstellungen und die Benachrichtigungsvorlagen angepasst. Jetzt können Sie die erforderlichen Warnungsschemata definieren:

- CI-Status-Warnungen. Definieren Sie nach Bedarf CI-Status-Warnungen, um Empfänger über KPI-Statusänderungen für bestimmte CIs und KPIs zu informieren, die in Service Health überwacht werden. Weitere Informationen finden Sie unter "How to Create a CI Status Alert Scheme and Attach it to a CI" im BSM-Benutzerhandbuch.
- SLA-Warnungen. Definieren Sie nach Bedarf SLA-Warnungen, um Empfänger mit Warnungen über Änderungen am aktuellen und prognostizierten Status von Servicevereinbarungen zu informieren. Weitere Informationen finden Sie unter "How to Define an SLA Alert Scheme" im BSM-Benutzerhandbuch.
- **EUM-Warnungen.** Definieren Sie nach Bedarf EUM-Warnungen, um Empfänger mit Warnungen über Leistungsabweichungen bei Real User Monitor-Entitäten oder Business Process Monitor-Transaktionen zu informieren. Weitere Informationen finden Sie unter "How to Create EUM Alert Schemes" im BSM-Benutzerhandbuch.

Anpassen von Warnungen

Hinweis: Alle Schritte in dieser Aufgabe sind optional und können in beliebiger Reihenfolge ausgeführt werden.

Diese Aufgabe beschreibt die Anpassungen, die Sie für Warnungen der Typen CI-Status, SLA und EUM durchführen können.

Ändern der Verarbeitung von Ereignissen

Um die Verarbeitung von Ereignissen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Warnungen.
- Lokalisieren und ändern Sie in der Tabelle Warnungen Ereignisverarbeitung die folgenden Parameter:
 - Akzeptable Ereignisverzögerung (Minuten). Wird verwendet, um für Warnungen die Standardverzögerung festzulegen. Ändern Sie die Standardverzögerung (60 Minuten), nach deren Ablauf Warnungen verworfen werden.
 - Berechnungspersistenz. Wird verwendet, um die Berechnungspersistenz zu aktivieren/zu deaktivieren. Wenn die Berechnungspersistenz aktiviert ist, werden die berechneten Daten, die vor dem Herunterfahren des Systems vorhanden waren, nach dem Hochfahren des Systems für Datenberechnungen verwendet. Wählen Sie false aus, um die Berechnungspersistenz zu deaktivieren. Wählen Sie true aus, um die Berechnungspersistenz zu aktivieren.

Ändern der Systemzustandsparameter für Warnungen

Um die Verarbeitung von Ereignissen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Warnungen.
- Lokalisieren und ändern Sie in der Tabelle Warnungen Systemzustandsmonitore die folgenden Parameter:
 - Fehlerschwellenwert für Benachrichtigungswarteschlangen-Monitor. Wird verwendet, um festzulegen, wann der Status der Benachrichtigungswarteschlange in Fehler wechselt. Geben Sie die maximale Anzahl der Meldungen ein, die in der Warnungswarteschlange des Benachrichtigungswarteschlangen-Monitors warten können. Wenn der Maximalwert erreicht ist, wechselt der Status des Benachrichtigungswarteschlangen-Monitors in Fehler.
 - Warnungsschwellenwert für Benachrichtigungswarteschlangen-Monitor. Wird verwendet, um festzulegen, wann der Status der Benachrichtigungswarteschlange in Warnung wechselt. Geben Sie die maximale Anzahl der Meldungen ein, die in der Warnungswarteschlange des Benachrichtigungswarteschlangen-Monitors warten können. Wenn der Maximalwert erreicht ist, wechselt der Status des Benachrichtigungswarteschlangen-Monitors in Warnung.

- Fehlerschwellenwert für Warnungswarteschlangen-Monitor. Wird verwendet, um festzulegen, wann der Status der Warnungswarteschlange in Fehler wechselt. Geben Sie die maximale Anzahl der Meldungen ein, die in der Warnungswarteschlange des Warnungswarteschlangen-Monitors warten können. Wenn der Maximalwert erreicht ist, wechselt der Status des Warnungswarteschlangen-Monitors in Fehler.
- Warnungsschwellenwert für Warnungswarteschlangen-Monitor. Wird verwendet, um festzulegen, wann der Status der Warnungswarteschlange in Warnung wechselt. Geben Sie die maximale Anzahl der Meldungen ein, die in der Warnungswarteschlange des Warnungswarteschlangen-Monitors warten können. Wenn der Maximalwert erreicht ist, wechselt der Status des Warnungswarteschlangen-Monitors in Warnung.

Ändern der Standardeinstellungen für die Warnungsauslösung

Um die Verarbeitung von Ereignissen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Warnungen.
- Lokalisieren und ändern Sie in der Tabelle Warnungen Ausgelöste Warnungen die folgenden Parameter:
 - Zeitüberschreitung für Befehlszeilenausführung (Sekunden). Sie können die standardmäßige Zeitüberschreitung für eine Aktion (30 Sekunden) ändern, nach der eine Befehlszeilen-Warnungsaktion nicht ausgeführt wird.
 - Standard-SNMP-Zieladresse oder Standard-SNMP-Port. Sie k\u00f6nnen die standardm\u00e4\u00df\u00e4\u00dfe SnMP-Trap-Hostadresse durch Angeben der IP-Adresse oder des Servernamens im Parameter Standard-SNMP-Zieladresse und der Portnummer im Parameter Standard-SNMP-Port \u00e4ndern.

Hinweis: Sie können nur eine SNMP-Zieladresse angeben. Die Standard-Hostadresse des SNMP-Traps wird im Dialogfeld zum Erstellen eines neuen SNMP-Traps und zum Ändern eines vorhandenen SNMP-Traps im Feld zum Eingeben des Hostziels automatisch angezeigt. Details finden Sie unter "Create New/Edit SNMP Trap Dialog Box" im BSM Application Administration Guide oder unter "Create SNMP Trap/Edit SNMP Trap Dialog Box" im BSM Application Administration Guide. Wenn Sie beim Erstellen oder Bearbeiten eines SNMP-Traps die Standard-Hostadresse auswählen und diese in den Infrastruktureinstellungen anschließend ändern, wird die Adresse in allen erstellten SNMP-Traps mit dem neuen Standardwert aktualisiert. Jede gesendete Warnung führt dazu, dass der SNMP-Trap an die neue Standardadresse gesendet wird.

Hinweis für HP Software-as-a-Service-Kunden: Sie können die Standard-Hostadresse pro Kunde festlegen, indem Sie bei der Anmeldung einen Kunden auswählen. Die aktualisierte Hostadresse wird nur für den jeweiligen Kunden definiert. Sie können auch eine globale Hostadresse definieren.

■ Ersatzpaare für die Befehlszeile. Wenn Sie in der Aktion Ausführbare Dateien einer EUM-Warnung einen Befehl angeben, können Sie spezielle Token verwenden, die bei der Vorbereitung der Befehlsausführung durch tatsächliche Werte ersetzt werden. Diese Werte können doppelte Anführungszeichen (") oder andere Token enthalten, die bewirken, dass die

resultierende Befehlszeile vom Betriebssystem nicht richtig interpretiert wird. Um diese falsche Interpretation zu vermeiden, können Sie den Standardwert der Infrastruktureinstellungen **Ersatzpaare für die Befehlszeile** wie folgt ändern:

- Jedes Paar wird im Format |a|b| geschrieben.
- Das Zeichen a wird durch b ersetzt.
- Mehrere Paare werden durch ein Komma (,) voneinander getrennt.
 Beispiel: |a|b|, |c|d|, |e|f|.
- Warnungsabhängigkeiten zwischen Cls aktivieren. Wird verwendet, um Warnungsabhängigkeiten zwischen Cls zu aktivieren. Wählen Sie Folgendes aus:
 - false. (Standard) Warnungsabhängigkeiten zwischen CIs sind nicht zulässig.
 - o true. Warnungsabhängigkeiten zwischen CIs sind zulässig.
- Zurücksetzen des Warnungs-Timers aktivieren. Wird verwendet, um den Timer für die Benachrichtigungshäufigkeit zurückzusetzen. Wählen Sie Folgendes aus:
 - false. (Standard) Eine Warnung wird durch eine bestimmte Bedingung ausgelöst. Danach liegt die Bedingung, die die Warnung ausgelöst hat, nicht mehr vor. Wenn die Bedingung, die die Warnung ausgelöst hat, vor Ablauf des im Parameter Akzeptable Ereignisverzögerung angegebenen Zeitraums erneut auftritt, wird die Warnung nicht gesendet.
 - true. Eine Warnung wird durch eine bestimmte Bedingung ausgelöst. Danach liegt die Bedingung, die die Warnung ausgelöst hat, nicht mehr vor. Wenn die Bedingung, die die Warnung ausgelöst hat, vor Ablauf des im Parameter Akzeptable Ereignisverzögerung angegebenen Zeitraums erneut auftritt, wird die Warnung gesendet, weil die Auslösebedingung den Timer für die Benachrichtigungshäufigkeit zurückgesetzt hat.
- **Protokollierung in DB aktivieren.** Aktiviert die Protokollierung von Warnungen und Benachrichtigungen in der Datenbank. Diese Anpassung steht nur für EUM-Warnungen zur Verfügung. Wählen Sie Folgendes aus:
 - **true.** (Standard) Warnungen und Benachrichtigungen werden in der Profildatenbank protokolliert.
 - false. Warnungen und Benachrichtigungen werden nicht in der Profildatenbank protokolliert.

Details zu Protokollen finden Sie unter "Warnungsprotokolle" auf Seite 457.

- Benachrichtigungen und Aktionen aktivieren. Aktiviert die Warn-Engine, sodass Aktionen ausgeführt und Benachrichtigungen gesendet werden. Diese Anpassung steht nur für EUM-Warnungen zur Verfügung. Wählen Sie Folgendes aus:
 - true. (Standard) Die Warn-Engine führt Aktionen aus und sendet Benachrichtigungen.
 - false. Es werden keine Aktionen ausgeführt und keine Benachrichtigungen an den Benutzer gesendet.
- Alte SNMP-Zieladresse oder Alter SNMP-Port. Wird verwendet, um die standardmäßige SNMP-Trap-Hostadresse für EUM-Warnungen zu ändern. Sie können die standardmäßige SNMP-Trap-Hostadresse durch Angeben der IP-Adresse oder des Servernamens im Parameter Standard-SNMP-Zieladresse und der Portnummer im Parameter Standard-

SNMP-Port ändern.

Hinweis: Sie können nur eine SNMP-Zieladresse angeben. Die Standard-Hostadresse des SNMP-Traps wird im Dialogfeld zum Erstellen eines neuen SNMP-Traps und zum Ändern eines vorhandenen SNMP-Traps im Feld zum Eingeben des Hostziels automatisch angezeigt. Details finden Sie unter "Create New/Edit SNMP Trap Dialog Box" im BSM Application Administration Guide oder unter "Create SNMP Trap/Edit SNMP Trap Dialog Box" im BSM Application Administration Guide. Wenn Sie beim Erstellen oder Bearbeiten eines SNMP-Traps die Standard-Hostadresse auswählen und diese in den Infrastruktureinstellungen anschließend ändern, wird die Adresse in allen erstellten SNMP-Traps mit dem neuen Standardwert aktualisiert. Jede gesendete Warnung führt dazu, dass der SNMP-Trap an die neue Standardadresse gesendet wird.

Hinweis für HP Software-as-a-Service-Kunden: Sie können die Standard-Hostadresse pro Kunde festlegen, indem Sie bei der Anmeldung einen Kunden auswählen. Die aktualisierte Hostadresse wird nur für den jeweiligen Kunden definiert. Sie können auch eine globale Hostadresse definieren.

- Wiederholungsversuche für Benachrichtigung. Wird verwendet, um die Anzahl der Wiederholungsversuche für eine Benachrichtigung festzulegen. Diese Anpassung steht nur für EUM-Warnungen zur Verfügung. Standardmäßig wird eine Benachrichtigung einmal gesendet. Sie können die Standardeinstellung mit dem Parameter Wiederholungsversuche für Benachrichtigung ändern. Die Anzahl der durchgeführten Wiederholungsversuche entspricht der angegebenen Zahl plus 1.
- Benachrichtigungs-URL. Wird verwendet, um die in Benachrichtigungen eingebettete URL anzupassen.
- Zeitüberschreitung für Symphony-Anforderungen (Sekunden). Wird verwendet, um die Anzahl der Sekunden festzulegen, nach deren Ablauf eine Zeitüberschreitung für eine Warnungsaktion eintritt.
- Warteintervall zwischen Wiederholungen (Sekunden). Wird verwendet, um die Anzahl der Sekunden zwischen jedem Versuch einer Benachrichtigungsausführung festzulegen.
- **EXE-Standardpfad.** Wird verwendet, um den Standardpfad zur standardmäßigen ausführbaren Datei für EUM-Warnungen anzugeben.
- **Standard-URL.** Wird verwendet, um die URL-Standardadresse für EUM-Warnungen anzugeben.
- Format der Empfängerinformationen in der Vorlage. Wird verwendet, um die Anzeige der Empfängerliste in E-Mail- oder SMS-Nachrichten zu ändern. Sie können die folgenden Werte zuweisen:
 - Adresse. Wird verwendet, um die vollständige E-Mail der Empfänger im Feld An von E-Mail- und SMS-Nachrichten anzuzeigen. Wenn Sie beispielsweise für Format der Empfängerinformationen in der Vorlage den Wert Adresse festlegen und die Vorlage die folgenden Parameter enthält: An:<<Empfänger>>, Profilname: <<Pro>rofilname>>, Schweregrad: <<Schweregrad>>, lautet die E-Mail wie folgt:

An:gaz@devlab.ad;shifv@devlab.ad;aahhh.hhheee@hp.com

Profilname: forAlert Schweregrad: Wichtig

 Logischer Name. Wird verwendet, um den logischen Namen der Empfänger im Feld An von E-Mail- und SMS-Nachrichten anzuzeigen. Wenn Sie beispielsweise für Format der Empfängerinformationen in der Vorlage den Wert Logischer Name festlegen und die Vorlage dieselben Parameter wie im obigen Beispiel enthält, lautet die E-Mail wie folgt:

An:aa;bac admins Profilname: forAlert Schweregrad: Wichtig

Ändern der Optionen für das Senden von Warnungen per E-Mail

Um die Verarbeitung von E-Mail-Warnungen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Plattformverwaltung aus.
- Lokalisieren und ändern Sie in der Tabelle Plattformverwaltung E-Mail-Einstellungen für Warnungen die folgenden Parameter:
 - **Kennwort für autorisierten E-Mail-Versand.** Wird verwendet, um das Standardkennwort für das autorisierte Senden von E-Mail-Warnungen zu ändern.
 - SMTP-Server (nur Windows). Wird verwendet, um den verwendeten primären SMTP-Server anzugeben. Legen Sie diesen Parameter unter Windows NT als <SMTPSVC> fest, wenn das Senden mit dem SMTP-Service erfolgen soll.
 - SMTP-Server-Port (nur Windows). Wird verwendet, um den SMTP-Server-Port anzugeben.
 - Benutzer für autorisierten E-Mail-Versand. Wird verwendet, um den Standardbenutzer für das autorisierte Senden von E-Mail-Warnungen zu ändern. Wird dieser Parameter nicht festgelegt, werden E-Mail-Warnungen ohne Autorisierung gesendet.

Ändern der Optionen für das Senden von Warnungen per Pager

Um die Verarbeitung von Pager-Warnungen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Plattformverwaltung aus.
- Lokalisieren und ändern Sie in der Tabelle Plattformverwaltung Pager-Einstellungen für Warnungen die folgenden Parameter:
 - **Kennwort für autorisierten Pager-Versand.** Wird verwendet, um das Standardkennwort für das autorisierte Senden von Pager-Warnungen zu ändern.
 - SMTP-Server (nur Windows). Wird verwendet, um den verwendeten primären SMTP-Server anzugeben. Legen Sie diesen Parameter unter Windows NT als <SMTPSVC> fest, wenn das Senden mit dem SMTP-Service erfolgen soll.

- SMTP-Server-Port (nur Windows). Wird verwendet, um den SMTP-Server-Port anzugeben.
- Benutzer für autorisierten Pager-Versand. Wird verwendet, um den Standardbenutzer für das autorisierte Senden von Pager-Warnungen zu ändern. Wird dieser Parameter nicht festgelegt, werden Pager-Warnungen ohne Autorisierung gesendet.

Ändern der Optionen für das Senden von Warnungen per SMS

Um die Verarbeitung von SMS-Warnungen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Plattformverwaltung aus.
- Lokalisieren und ändern Sie in der Tabelle Plattformverwaltung SMS-Einstellungen für Warnungen die folgenden Parameter:
 - **Kennwort für autorisierten SMS-Versand.** Wird verwendet, um das Standardkennwort für das autorisierte Senden von SMS-Warnungen zu ändern.
 - SMTP-Server (nur Windows). Wird verwendet, um den verwendeten primären SMTP-Server anzugeben. Legen Sie diesen Parameter unter Windows NT als <SMTPSVC> fest, wenn das Senden mit dem SMTP-Service erfolgen soll.
 - **SMTP-Server-Port (nur Windows).** Wird verwendet, um den SMTP-Server-Port anzugeben.
 - Benutzer für autorisierten SMS-Versand. Wird verwendet, um den Standardbenutzer für das autorisierte Senden von SMS-Warnungen zu ändern. Wird dieser Parameter nicht festgelegt, werden SMS-Warnungen ohne Autorisierung gesendet.

Ändern der Verarbeitung von Benachrichtigungen

Um die Verarbeitung von Benachrichtigungen zu ändern, wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus:

- Wählen Sie Foundation aus.
- Wählen Sie Plattformverwaltung aus.
- Lokalisieren und ändern Sie in der Tabelle Plattformverwaltung -Empfängerbenachrichtigungsservice die folgenden Parameter:
- E-Mail-Absenderadresse von Warnungen. Wird verwendet, um die E-Mail-Adresse des in E-Mails verwendeten Standardabsenders zu ändern. Sie verwenden diesen Parameter, um den Standardwert (HP_BSM_Alert_Manager) zu ändern, der im Feld Von angezeigt wird, wenn BSM bei der Installation des Datenverarbeitungsservers Warnungen sendet.
- "Alternativer SMTP-Server-Port (nur Windows)" und "Alternativer SMTP-Server (nur Windows)". Wird verwendet, um den alternativen SMTP-Server zu ändern:
- Ein benannter Server mit einer definierten Port-Nummer. Geben Sie einen Servernamen für das Senden von SMTP-E-Mails als Wert in das Feld Alternativer SMTP-Server ein.
 Geben Sie außerdem eine Port-Nummer für den Server in das Feld Alternativer SMTP-Server ein.
- Microsoft SMTP-Services. Geben Sie < SMTPSVC > als Wert in das Feld SMTP-Server oder

Alternativer SMTP-Server ein.

Einschränkung: Die folgenden Zeichen sind ungültig: _ . -

- Zeichensatz für E-Mail-Benachrichtigungen. Wird eine Warnung ausgelöst, können die Empfänger der generierten Warnung per E-Mail, SMS oder Pager benachrichtigt werden. Sie können einen der folgenden Zeichensätze auswählen:
 - UTF-8. Der Standardzeichensatz.
 - ISO-2022-JP.

Hinweis für HP Software-as-a-Service-Kunden: Die in diesem Abschnitt beschriebenen Einstellungen gelten pro Kunde.

- **E-Mail-Absender.** Wird verwendet, um den Namen des Absenders von Warn-E-Mails anzugeben.
- Empfängerbenachrichtigungen aktivieren. Legen Sie false fest, um das Senden von Benachrichtigungen an Empfänger zu verhindern. Legen Sie true fest, um Benachrichtigungen an Empfänger zu senden.
- Zeichensatz für Pager-Benachrichtigungen. Legt den beim Senden von Pager-Benachrichtigungen verwendeten Zeichensatz fest. Sie können einen der folgenden Zeichensätze auswählen:
- **UTF-8.** Der Standardzeichensatz.
- ISO-2022-JP.

Hinweis für HP Software-as-a-Service-Kunden: Die in diesem Abschnitt beschriebenen Einstellungen gelten pro Kunde.

- Kennwort für autorisierten Nachrichtenversand. Verwenden Sie diesen Parameter, um ein Standardkennwort für den autorisierten Nachrichtenversand anzugeben. Wird dieser Parameter nicht festgelegt, werden Nachrichten ohne Autorisierung gesendet.
- Zeichensatz für SMS-Benachrichtigungen. Legt den beim Senden von SMS-Benachrichtigungen verwendeten Zeichensatz fest Sie können einen der folgenden Zeichensätze auswählen:
- UTF-8. Der Standardzeichensatz.
- ISO-2022-JP.

Hinweis für HP Software-as-a-Service-Kunden: Die in diesem Abschnitt beschriebenen Einstellungen gelten pro Kunde.

- SMTP-Server (nur Windows). Wird verwendet, um den verwendeten primären SMTP-Server anzugeben. Legen Sie diesen Parameter unter Windows NT als <SMTPSVC> fest, wenn das Senden mit dem SMTP-Service erfolgen soll.
- SMTP-Server-Port (nur Windows). Wird verwendet, um den SMTP-Server-Port anzugeben.
- Zeitüberschreitung in Sekunden bei SMTP-Server-Socket-Verbindung (nur Windows).

Verwenden Sie diesen Parameter, um die Standardzeitüberschreitung (60 Sekunden) zu ändern, nach deren Ablauf die Verbindung eines SMTP-Server-Sockets getrennt wird.

Hinweis: Dieser Parameter wird nur für Windows-Betriebssysteme verwendet.

■ Benutzer für autorisierten Nachrichtenversand. Verwenden Sie diesen Parameter, um einen Standardbenutzer für den autorisierten Nachrichtenversand anzugeben. Wird dieser Parameter nicht festgelegt, erfolgt das Senden von Nachrichten ohne Autorisierung.

Warnungsprotokolle

Die folgenden Protokolle können Sie zum Debuggen der CI-Status-, SLA- und EUM-Warnungen verwenden.

Warnungstyp	Pfad zum Protokoll und zur Eigenschaftendatei für die Einrichtung der Protokollebene	Beschreibung
Alle Warnungen	Protokoll: <bsm- Datenverarbeitungsserver>\log\alerts\ alerts.ejb.log</bsm- 	Verarbeitung von Warnungen und Benachrichtigungen im MercuryAs- Prozess
	Setup: <bsm- datenverarbeitungsserver="">\conf\ core\Tools\log4j\EJB\ alerts.properties</bsm->	
	Protokoll: <bsm- Gatewayserver>\log\alerts\ alerts.reports.log</bsm- 	Für alle Warnungs-Reports
	Setup: <bsm- Gatewayserver>\conf\core\ Tools\log4j\EJB\ alerts.properties</bsm- 	
CI-Status- Warnungen und SLA-Warnungen	Protokoll: <bsm- Datenverarbeitungsserver>\log\ marble_worker_1\status.alerts.log</bsm- 	Warnungsinitialisierung und Berechnung im MAR Business Logic Engine-Arbeitsprozess
	Setup: <bsm- datenverarbeitungsserver="">\conf\ core\Tools\log4j\marble_worker\ cialerts.properties</bsm->	
	Protokoll: <bsm- datenverarbeitungsserver="">\log\ marble_worker_ 1\status.alerts.downtime.log</bsm->	Verarbeitung von Warnungen/Ausfallzeiten im MAR Business Logic Engine- Arbeitsprozess
	Setup: <bsm- datenverarbeitungsserver="">\conf\ core\Tools\log4j\marble_worker\ acialerts.properties</bsm->	
	Protokoll: <bsm- Gatewayserver>\log\alerts\ alertui.log</bsm- 	Warnungsverwaltung
	Setup: <bsm- Gatewayserver>\conf\core\ Tools\log4j\EJB\ alerts.properties</bsm- 	

Warnungstyp	Pfad zum Protokoll und zur Eigenschaftendatei für die Einrichtung der Protokollebene	Beschreibung
EUM-Warnungen	Protokoll: <bsm- Datenverarbeitungsserver>\log\alerts\ alert.rules.log</bsm- 	Warnungsberechnung im MAR Business Logic Engine- Arbeitsprozess
	Setup: <bsm- datenverarbeitungsserver="">\conf\core\ Tools\log4j\marble_worker\ alerts-rules.properties</bsm->	
	Protokoll: <bsm- Datenverarbeitungsserver>\log\alerts\ alerts.rules.init.log</bsm- 	Warnungsinitialisierung im MAR Business Logic Engine- Arbeitsprozess
	Setup: <bsm- datenverarbeitungsserver="">\conf\core\ Tools\log4j\marble_worker\ alerts-rules.properties</bsm->	
	Protokoll: <bsm- Datenverarbeitungsserver>\log\alerts\ alerts.downtime.log</bsm- 	Verarbeitung von Warnungen/Ausfallzeiten im MAR Business Logic Engine-
	Setup: <bsm- Datenverarbeitungsserver>\conf\ core\Tools\log4j\marble_worker\ alerts-rules.properties</bsm- 	Arbeitsprozess

Hinweis: Wenn Sie eine Datei mit Protokolleigenschaften auf einem der BSM-Verarbeitungsserver ändern, wirkt sich die Änderung nur auf die Protokolle auf diesem BSM-Verarbeitungsserver aus.

Report zu Warnungsdetails

Dieser Report zeigt die Auslöseinformationen an, die für die Warnung verfügbar sind, einschließlich der tatsächlichen Bedingungen zum Zeitpunkt der Warnung.

Nachfolgend wird ein Beispiel für den Report zu Warnungsdetails dargestellt.





Klicken Sie auf die Schaltfläche auf der Seite CI-Status-Warnungen, Warnungen zum SLA-Status oder in den Reports zum Warnungsprotokoll.

Wichtiger Hinweis

Weitere Informationen zu CI-Status-Warnungen finden Sie in den Einzelheiten zur Seite **Warnungsdetails** unter "Configuration Item Status Alert Notifications Report" im BSM-Benutzerhandbuch.

Weitere Informationen zu Warnungen zum SLA-Status finden Sie in den Einzelheiten zur Seite **Warnungsdetails** unter "SLA Status Alert Notifications Report" im BSM-Benutzerhandbuch.

Weitere Informationen zu EUM-Warnungen finden Sie in den Einzelheiten zur Seite **Warnungsdetails** unter "Alert Details" im BSM-Benutzerhandbuch.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Fehlerbehebungen und Einschränkungen für Warnungen.

Es wurden keine E-Mails empfangen, obwohl eine Warnung hätte ausgelöst werden sollen

Wenn die Empfänger keine E-Mails erhalten, überprüfen Sie die folgenden Möglichkeiten:

- Die Warnungsdefinition lautet nicht wie erwartet. Überprüfen Sie die Warnungsdefinition in der entsprechenden Warnungsverwaltung.
- Die Daten verhalten sich nicht wie erwartet, sodass die Auslösebedingung für die Warnung nicht besteht. Überprüfen Sie das Protokoll zur Warnungsberechnung oder überprüfen Sie die spezifischen Protokolle und Reports zum Datenursprung. Weitere Informationen finden Sie unter "Warnungsprotokolle" auf Seite 457.
- Möglicherweise liegt ein Verbindungsproblem mit dem E-Mail-Server von SMTP vor. Um die Funktion des Servers zu überprüfen, führen Sie folgenden Befehl aus: telnet <smtp_server_ host_name_or_IP_nbr> 25.
- Die E-Mail-Adresse des Empfängers ist möglicherweise ungültig. Überprüfen Sie die Empfängerdefinition in der Benutzeroberfläche und senden Sie manuell eine E-Mail an den Empfänger, um die Gültigkeit der Adresse zu überprüfen.
- Der Empfänger beurteilt die Warnung als Spam. Bitten Sie den Administrator des Empfängers, den Spamfilter neu zu konfigurieren.

Kapitel 28

Benachrichtigungsvorlagen für EUM-Warnungen

Um den Inhalt und die Anzeige von EUM-Warnungsbenachrichtigungen festzulegen, können Sie vordefinierte Vorlagen auswählen oder eigene Vorlagen für Benachrichtigungen festlegen.

Benachrichtigungsvorlagen für Warnungen geben die Informationen an, die von BSM aufgenommen werden, wenn die unterschiedlichen Benachrichtigungstypen gesendet werden. Die verfügbaren Standardvorlagen sind mit ausgewählten Parametern für jeden Abschnitt der Benachrichtigung vorkonfiguriert. Weitere Informationen zu den Informationen, die in die Standardvorlagen aufgenommen werden, finden Sie unter "Seite "Benachrichtigungsvorlagen" auf Seite 470.

Sie haben auch die Möglichkeit, benutzerdefinierte Vorlagen zu erstellen. Sie können verschiedene Vorlagen für die unterschiedlichen Sendemethoden für die Warnungsbenachrichtigungen (E-Mail, Pager, SMS) oder die unterschiedlichen Empfänger erstellen. Eine benutzerdefinierte Vorlage wird auf der Seite **Eigenschaften der Benachrichtigungsvorlage** definiert. In den Abschnitten der Warnungsbenachrichtigungen ist eine Liste mit Parametern enthalten, die Sie auswählen können. Weitere Informationen zu den Informationen, die in eine benutzerdefinierte Vorlage aufgenommen werden, finden Sie unter "Seite "Benachrichtigungsvorlagen"" auf Seite 470.

Hinweis für HP Software-as-a-Service-Kunden: Ihre Liste der Benachrichtigungsvorlagen beinhaltet die Standardbenachrichtigungsvorlagen, die Benachrichtigungsvorlagen, die Ihnen von HP Software-as-a-Service-Kundendienstvertretern bereitgestellt wurden und die von Ihrer Organisation erstellten Vorlagen.

Benachrichtigungsvorlagen für die Aufhebung des Warnungszustands

Beim Konfigurieren von Warnungsschemata können Sie ein Warnungsschema einrichten, durch das automatische Benachrichtigungen über die Aufhebung des Warnungszustands gesendet werden. Weitere Informationen zum Auswählen dieser Option beim Erstellen des Warnungsschemas finden Sie unter "How to Create EUM Alert Schemes".

Die Standardvorlage für Benachrichtigungen über die Aufhebung des Warnungszustands wird von BSM automatisch verwendet. Wenn BSM nicht die Standardvorlage verwenden soll, können Sie Ihre eigene Vorlage für die Benachrichtigung über die Aufhebung des Warnungszustands erstellen. Diese Vorlage muss auf einer bestehenden Benachrichtigungsvorlage basieren. BSM verwendet die von Ihnen erstellte Benachrichtigungsvorlage für die Aufhebung des Warnungszustands in folgenden Situationen:

- Eine Warnung wurde ausgelöst.
- Die Benachrichtigung wird basierend auf einer bestehenden Vorlage (Standardvorlage oder benutzerdefinierte Vorlage) an einen Empfänger gesendet.
- Das Warnungsschema wurde für das Senden von Benachrichtigungen über die Aufhebung des Warnungszustands konfiguriert.

Weitere Informationen zum Konfigurieren einer Benachrichtigungsvorlage für die Aufhebung des Warnungszustands finden Sie unter "Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf Seite 465.

Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen

Sie können vordefinierte Vorlagen auswählen, bestehende Vorlagen verändern oder Ihre eigenen Benachrichtigungsvorlagen erstellen, um die Inhalte und das Erscheinungsbild von Warnungsbenachrichtigungen festzulegen. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter "Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 462.

Erstellen von benutzerdefinierten Vorlagen

BSM ermöglicht Ihnen das flexible Erstellen von verschiedenen Benachrichtigungsvorlagen für die unterschiedlichen Warnungsschemata und Empfänger, die für Ihre Plattform definiert wurden.

Jede Vorlage ist in Abschnitte unterteilt. Sie geben die Informationen an, die in den jeweiligen Abschnitten angezeigt werden sollen. Weitere Informationen finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage" auf Seite 466.

Verwalten von bestehenden Vorlagen

Im Laufe der Zeit kann es notwendig werden, die von Ihnen erstellten Benachrichtigungsvorlagen zu ändern, da sich organisatorische Änderungen, neue Benachrichtigungsrichtlinien oder Änderungen an Servicelevelverträgen usw. ergeben haben. Sie verwenden die Seite **Benachrichtigungsvorlagen** zum Bearbeiten, Klonen und Löschen von Benachrichtigungsvorlagen, die in BSM definiert wurden. Weitere Informationen finden Sie unter "Seite "Benachrichtigungsvorlagen" auf Seite 470.

Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands

Sie können vordefinierte Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands auswählen, bestehende Vorlagen verändern oder Ihre eigenen Benachrichtigungsvorlagen erstellen, um die Inhalte und das Erscheinungsbild der Benachrichtigungen selbst festzulegen. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter "Benachrichtigungsvorlagen für die Aufhebung des Warnungszustands" auf Seite 463.

Hinweis: Als Benachrichtigungsvorlage für den Empfänger wird die Vorlage für die Aufhebung des Warnungszustands auf Grundlage des Namens der Benachrichtigungsvorlage ausgewählt. Weitere Informationen zum Benennen einer Vorlage für die Aufhebung des Warnungszustands finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf der nächsten Seite. Weitere Informationen zu Aufhebungen des Warnungszustands finden Sie unter "Advanced Settings Tab" im BSM-Benutzerhandbuch.

Informationen zum Erstellen, Ändern oder Verwalten von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands finden Sie unter "Seite "Benachrichtigungsvorlagen" auf Seite 470.

Benachrichtigungsvorlagen für EUM-Warnungen – Benutzeroberfläche

Dieser Abschnitt umfasst die folgenden Themen:

- "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" unten
- "Seite "Benachrichtigungsvorlagen"" auf Seite 470

Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"

In diesem Dialogfeld können Sie eine neue Benachrichtigungsvorlage für Warnungen definieren.

Zugriff

- So erstellen Sie eine neue Vorlage: Klicken Sie auf der Seite Benachrichtigungsvorlagen auf die Schaltfläche Neue Vorlage.
- So bearbeiten Sie eine vorhandene Vorlage: Klicken Sie auf der Seite Benachrichtigungsvorlagen auf eine vorhandene Vorlage und klicken Sie dann auf

Wichtiger Hinweis

Benachrichtigungen über die Aufhebung des Warnzustands: Wählen Sie zum Einrichten einer Benachrichtigung über die Aufhebung des Warnzustands die Benachrichtigungsvorlage aus, die Sie als Grundlage für Ihre Benachrichtigung verwenden wollen, und duplizieren Sie diese. Treffen Sie Ihre Wahl nach der Benachrichtigungsvorlage, die für Benutzer ausgewählt wurde, die am ehesten eine Benachrichtigung über die Aufhebung des Warnzustands erhalten. Ändern Sie den Namen der Vorlage, indem Sie Kopie von löschen und Followup (in Großbuchstaben, ein Wort) hinzufügen. Bearbeiten Sie die erforderlichen Vorlagendetails. Sie sollten in den Betreff einer E-Mail über die Aufhebung des Warnzustands die Kopfzeile, die warnungsspezifischen Informationen oder beides einschließen.

Beispiel: Wenn Sie eine Vorlage für Benachrichtigungen über die Aufhebung des Warnzustands auf der Grundlage der Standardvorlage **LONG** erstellen, würde die Benachrichtigungsvorlage **LONG_FOLLOWUP** genannt. Wenn die Vorlage für Benachrichtigungen über die Aufhebung des Warnzustands auf einer benutzerdefinierten Vorlage namens **MyTemplate** basiert, nennen Sie die Vorlage **MyTemplate_FOLLOWUP**.

Standard: Die Zeichenfolge **_FOLLOWUP** ist die Standardvorlage, die von BSM als Vorlagenname für eine Benachrichtigung über die Aufhebung des Warnzustands erkannt wird.

Anpassung: Sie können die Zeichenfolge **_FOLLOWUP** anpassen. Details finden Sie unter "Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf der vorherigen Seite.

Relevante Aufgaben

"Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf der vorherigen Seite

Bereich "Allgemeine Informationen"

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der Oberfläche	Beschreibung
<einfügen></einfügen>	Wählen Sie einen Parameter aus, um diesen dem Abschnitt hinzuzufügen. Wiederholen Sie diesen Schritt, um die gewünschten Textparameter aus der Liste hinzuzufügen.
	Fügen Sie vor oder hinter den Textparametern freien Text hinzu. Für diesen Abschnitt stehen folgende Textparameter zur Verfügung:
	Alert Name. Der Name der Warnung, wie im Warnungsschema definiert.
	Severity. Der Schweregrad, der der Warnung im Warnungsschema zugewiesen wurde.
	HP BSM URL. Die URL der BSM-Website.
	Entity Name. Der Name des mit der Warnung verbundenen CI.
	Entity Type. Der Typ des mit der Warnung verbundenen CI.
	Alert User Description. Die von Ihnen im Warnungsschema angegebene Beschreibung.
	Actions Result. Eine Beschreibung der Ergebnisse der im Warnungsschema angegebenen Warnungsaktionen.
Message format	Wählen Sie das Format für die Nachricht aus: Text oder HTML .
Name	Geben Sie einen Namen für die Vorlage ein.
	Verwenden Sie möglichst einen beschreibenden Namen, der Informationen zum Warnungstyp (E-Mail, Pager, SMS) enthält, für den Sie die Vorlage verwenden wollen, oder zu den Empfängern, die Warnungen über diese Vorlage erhalten.
Betreff	Geben Sie die Informationen an, die BSM in den Betreff der E-Mail, Pager- Nachricht oder SMS-Mitteilung einschließen soll.
	Verwenden Sie die <liste betreff="" einfügen="" fußzeile="" für="" kopfzeile="" zum=""></liste> , um Parameter und freien Text hinzuzufügen und einen benutzerdefinierten Betreff zu erstellen. Sie können so viele Parameter aus der Liste hinzufügen, wie Sie möchten.

Bereich "Kopfzeile"

In diesem Bereich können Sie die Informationen angeben, die oben in der Warnungsbenachrichtigung angezeigt werden sollen. Wählen Sie Parameter aus der Liste **<Einfügen>** und freien Text aus, um eine benutzerdefinierte Kopfzeile zu erstellen. Sie können so viele Parameter aus der Liste hinzufügen, wie Sie möchten.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der	
Oberfläche	Beschreibung
<einfügen></einfügen>	Wählen Sie einen Parameter aus, um diesen dem Abschnitt hinzuzufügen. Wiederholen Sie diesen Schritt, um die gewünschten Textparameter aus der Liste hinzuzufügen.
	Fügen Sie vor oder hinter den Textparametern freien Text hinzu. Für diesen Abschnitt stehen folgende Textparameter zur Verfügung:
	Alert Name. Der Name der Warnung, wie im Warnungsschema definiert.
	Severity. Der Schweregrad, der der Warnung im Warnungsschema zugewiesen wurde.
	HP BSM-URL. Die URL der BSM-Website.
	Entity Name. Der Name des mit der Warnung verbundenen CI.
	Entity Type. Der Typ des mit der Warnung verbundenen CI.
	Alert User Description. Die von Ihnen im Warnungsschema angegebene Beschreibung.
	Actions Result. Eine Beschreibung der Ergebnisse der im Warnungsschema angegebenen Warnungsaktionen.
	Entity ID. Der Typ des mit der Warnung verbundenen CI.

Bereich "Warnungsspezifische Informationen"

In diesem Bereich können Sie der Benachrichtigung Warnungsinformationen hinzufügen.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der Oberfläche	Beschreibung
<liste einfügen<br="" zum="">für warnungsspezifische Informationen></liste>	Wählen Sie einen Textparameter aus, um diesen dem Abschnitt hinzuzufügen. Wiederholen Sie diesen Schritt, um die gewünschten Textparameter aus der Liste hinzuzufügen. • Trigger Cause. Eine Beschreibung der im Warnungsschema angegebenen Bedingungen für die Warnungsauslösung.
	Actual Details. Eine Beschreibung der tatsächlichen Bedingungen zum Zeitpunkt der Warnung.

Bereich "Transaktion"

In diesem Bereich können Sie die BMP-Transaktionsdetails angeben, die nur für den BPM-Warnungstyp relevant sind.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der	
Oberfläche	Beschreibung
<einfügen></einfügen>	Wählen Sie einen Parameter aus, um diesen dem Abschnitt hinzuzufügen. Wiederholen Sie diesen Schritt, um die gewünschten Textparameter aus der Liste hinzuzufügen. Fügen Sie vor oder hinter den Textparametern freien Text hinzu. Für diesen Abschnitt stehen folgende Textparameter zur Verfügung:
	Data Collector Name. Der Name der Datenerfassung, die von der zur Warnung gehörenden Transaktion ausgeführt wird.
	Script Name. Der Name des Skripts, das die zur Warnung gehörende Transaktion enthält.
	Transaction Time. Datum und Uhrzeit der Warnung.
	Transaction Description. Eine Beschreibung der Transaktion, falls diese in System Availability Management definiert wurde.
	Transaction Name. Der Name der mit der Warnung verbundenen Transaktion.
	Transaction Error. Die Fehlermeldung, die von der Datenerfassung für die Transaktion generiert wird, falls zum Zeitpunkt der Warnung ein Transaktionsfehler aufgetreten ist.
	Location Name. Der Speicherort der Datenerfassung, die von der zur Warnung gehörenden Transaktion ausgeführt wird.

Bereich "Fußzeile"

In diesem Bereich können Sie die Informationen angeben, die unten in der Warnungsbenachrichtigung angezeigt werden sollen. Wählen Sie Parameter aus der Liste **<Einfügen>** und freien Text aus, um eine benutzerdefinierte Fußzeile zu erstellen. Sie können so viele Parameter aus der Liste hinzufügen, wie Sie möchten.

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben (nicht benannte Elemente werden in spitzen Klammern angegeben):

Elemente der Oberfläche	Beschreibung
<einfügen></einfügen>	Wählen Sie einen Parameter aus, um diesen dem Abschnitt hinzuzufügen. Wiederholen Sie diesen Schritt, um die gewünschten Textparameter aus der Liste hinzuzufügen.
	Fügen Sie vor oder hinter den Textparametern freien Text hinzu. Für diesen Abschnitt stehen folgende Textparameter zur Verfügung:
	Alert Name. Der Name der Warnung, wie im Warnungsschema definiert.
	Severity. Der Schweregrad, der der Warnung im Warnungsschema zugewiesen wurde.
	HP BSM-URL. Die URL der BSM-Website.
	Entity Name. Der Name des mit der Warnung verbundenen CI.
	Entity Type. Der Typ des mit der Warnung verbundenen CI.
	Alert User Description. Die von Ihnen im Warnungsschema angegebene Beschreibung.
	Actions Result. Eine Beschreibung der Ergebnisse der im Warnungsschema angegebenen Warnungsaktionen.
	Entity ID. Der Typ des mit der Warnung verbundenen CI.

Seite "Benachrichtigungsvorlagen"

Auf dieser Seite finden Sie eine Liste der Standardvorlagen und aller benutzerdefinierten Vorlagen, die definiert wurden. Sie können Standard- und benutzerdefinierte Vorlagen verwalten und neue Vorlagen erstellen oder Benachrichtigungsvorlagen für die Aufhebung von Warnungszuständen bearbeiten.

Zugriff	Admin > Plattform > Empfänger > Warnungsbenachrichtigungsvorlagen des
	End User Managements

Wichtiger Hinweis

Beim Konfigurieren von Warnungsschemata können Sie BSM anweisen, durch das Senden einer Benachrichtigung über die Aufhebung des Warnungszustands automatisch auf die Warnung zu reagieren. Weitere Informationen zum Auswählen dieser Option beim Erstellen des Warnungsschemas finden Sie unter "Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf Seite 465.

Die Standardvorlage für Benachrichtigungen über die Aufhebung des Warnungszustands wird von BSM automatisch verwendet. Wenn Sie keine Standardvorlage verwenden wollen, können Sie eine eigene Vorlage für die Benachrichtigung über die Aufhebung des Warnungszustands erstellen. Sie sollten eine vorhandene Benachrichtigungsvorlage duplizieren und die duplizierte Vorlage dann ändern.

BSM verwendet die von Ihnen erstellte Benachrichtigungsvorlage für die Aufhebung des Warnungszustands in folgenden Situationen:

- Eine Warnung wurde ausgelöst.
- Die Benachrichtigung wird basierend auf einer bestehenden Vorlage (Standardvorlage oder benutzerdefinierte Vorlage) an einen Empfänger gesendet.
- Das Warnungsschema wurde für das Senden von Benachrichtigungen über die Aufhebung des Warnungszustands konfiguriert.
- Als Benachrichtigungsvorlage (DEFAULT_POSITIVE_FORMAT) für den Empfänger wird die Vorlage für die Aufhebung des Warnungszustands auf Grundlage des Namens der Benachrichtigungsvorlage ausgewählt.

Relevante Aufgaben

"Konfigurieren von Benachrichtigungsvorlagen für EUM-Warnungen" auf Seite 464

Die Elemente der Benutzeroberfläche werden im Folgenden beschrieben:

Elemente der Oberfläche	Beschreibung
	Klicken Sie hier, um Benachrichtigungsvorlagen zu duplizieren. Dupliziert die ausgewählte Benachrichtigungsvorlage. Das Dialogfeld Eigenschaften der Benachrichtigungsvorlage wird geöffnet, in dem Sie die duplizierte Benachrichtigung bearbeiten können. Weitere Informationen finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf Seite 466.
Ø.	Klicken Sie hier, um Eigenschaften von Benachrichtigungsvorlagen zu ändern. Klicken Sie hier, um die ausgewählte Vorlage zu bearbeiten. Details finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf Seite 466.

Elemente der Oberfläche	Beschreibung
×	Klicken Sie hier, um Benachrichtigungsvorlagen zu löschen. Löschen Sie die ausgewählten Vorlagen gleichzeitig.
	Zum gleichzeitigen Löschen mehrerer Vorlagen aktivieren Sie die jeweiligen Kontrollkästchen und klicken Sie auf die Schaltfläche unter der Vorlagenliste.
Neue Vorlage	Klicken Sie auf die Schaltfläche Neue Vorlage, um das Dialogfeld Eigenschaften der Benachrichtigungsvorlage zu öffnen. Details finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf Seite 466.
Name der Benachrichtigungsvorlage	Listet die Standardvorlagen und benutzerdefinierten Vorlagen auf. Die Standardvorlagen sind:
	DEFAULT_LOG_FORMAT. Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format für Reports erforderlich sind.
	DEFAULT_POSITIVE_FORMAT. Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format für positive Warnungen oder Warnungen über das Löschen eines Protokolls erforderlich sind. Weitere Informationen zu Benachrichtigungen über die Aufhebung von Warnungszuständen finden Sie unter "Konfigurieren von Vorlagen für Benachrichtigungen über die Aufhebung des Warnungszustands" auf Seite 465.
	LONG. Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im langen Format erforderlich sind.
	SHORT. Enthält alle Elemente, die zum Erstellen einer Standardbenachrichtigung im kurzen Format erforderlich sind.
	Hinweis: Weitere Informationen zu den in den jeweiligen Vorlagen angezeigten Parametern finden Sie unter "Dialogfeld "Eigenschaften der Benachrichtigungsvorlage"" auf Seite 466.

Teil 6

Fehlerbehebung

Kapitel 29

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden Probleme beschrieben, die im Bereich **Plattformverwaltung** von BSM häufig auftreten können.

Weitere Informationen zur Fehlerbehebung finden Sie in der HP-Wissensdatenbank zum Lösen von Softwareproblemen (h20230.www2.hp.com/selfsolve/documents).

Dieser Abschnitt umfasst die folgenden Themen:

- "Das Kennwort muss geändert werden, damit Daten-Collectoren (RUM, TV, BPI, Diagnostics) auf RTSM zugreifen können" auf der nächsten Seite
- "Die Seiten der RTSM-Verwaltung werden nicht geladen" auf der nächsten Seite
- "Fehlerbehebung und Einschränkungen" oben
- "Java-Applets werden nicht geladen" auf der nächsten Seite
- "Wiederkehrende Probleme mit der Benutzeroberfläche, nachdem eine Verbindung über einen Load Balancer hergestellt wurde" auf der nächsten Seite
- "Die BSM-Anmeldeseite wird nicht angezeigt, wenn die Verbindung über einen Load Balancer hergestellt wurde" auf Seite 476
- "BSM-Dialogfelder und -Applets wie der Authentifizierungs-Assistent werden nicht richtig geladen" auf Seite 476
- "BSM wurde installiert, die Seite für Downloads ist jedoch leer" auf Seite 476
- "Allgemeine Verbindungsprobleme im Zusammenhang mit Ports" auf Seite 476
- "Die BSM-Verbindungen wurden unterbrochen, aber die Servlet-Engine von Tomcat sowie JBoss Application Server scheinen zu funktionieren" auf Seite 477
- "Eine Anmeldung bei BSM ist nicht möglich, und JBoss Application Server wird nicht initialisiert" auf Seite 477
- "Der Browser erreicht BSM nicht und ein Fehler zu unzureichendem Heap-Speicher tritt auf" auf Seite 477
- "Der Browser erreicht BSM nicht oder der JSP-Quellcode wird im Browserfenster angezeigt" auf Seite 478
- "BSM befindet sich hinter einem Proxy und der Servername wird vom Proxy nicht erkannt" auf Seite 479
- "Hostnamen des Gateway-Servers oder des Servers für die Datenverarbeitung wurden geändert" auf Seite 479
- "Prozesse werden nach einem automatischen Failover nicht automatisch neu gestartet" auf Seite 479

Das Kennwort muss geändert werden, damit Daten-Collectoren (RUM, TV, BPI, Diagnostics) auf RTSM zugreifen können

Während der Bereitstellung können Sie optional ein **Zugriff auf RTSM-Kennwort festlegen**, um die Kommunikation zwischen BSM-Daten-Collectoren (wie Real User Monitor, Business Process Insight und TransactionVision) und Run-time Service Model zu sichern. Dieses Kennwort kann später über die JMX-Konsole geändert werden.

So ändern Sie das Kennwort für den RTSM-Zugriff über die JMX-Konsole:

- Geben Sie die URL der JMX-Konsole (http://<Name des Gateway- oder Datenverarbeitungsservers>:8080/jmx-console/) in einem Webbrowser ein. (Ausführliche Anweisungen finden Sie unter "Verwenden der JMX-Konsole" auf Seite 25.)
- 2. Geben Sie Anmeldeinformationen für die JMX-Konsole ein. Wenn Sie diese nicht kennen, wenden Sie sich an Ihren Systemadministrator.
- 3. Wählen Sie in der Domäne Foundations den Kennwort-Manager des RTSM-Diensts.
- Ändern Sie changeDataCollectorsOdbAccessPwd. Bei der Operation werden die Kunden-ID und das neue Kennwort als Parameter abgerufen und alle Kennwörter der Daten-Collectoren in das neue geändert.

Die Seiten der RTSM-Verwaltung werden nicht geladen

Wenn die Links der RTSM-Verwaltung nicht funktionieren, kann dies folgende Gründe haben:

- Der BSM-Gateway-Server kann keine Verbindung zur URL des virtuellen Gateway-Servers für Applikationsbenutzer herstellen. Diese URL finden Sie unter Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen. Wählen Sie im Feld Foundation die Option Plattformverwaltung aus. Die URL befindet sich in der Tabelle Host-Konfiguration.
- Sie verwenden einen Reverse-Proxy oder einen Load Balancer und haben sich nicht über die oben angegebene URL angemeldet.

Beim Laden von Java-Applets tritt der Fehler "Klasse nicht gefunden" auf

Stellen Sie sicher, dass Sie eine Profildatenbank erstellt haben. Diese Datenbank muss manuell in der Plattformverwaltung erstellt werden. Weitere Informationen finden Sie unter "Datenbankverwaltung" auf Seite 76.

Java-Applets werden nicht geladen

Öffnen Sie **Systemsteuerung > Java > Temporäre Internetdateien > Einstellungen**, und stellen Sie sicher, dass **Temporäre Dateien auf Computer belassen** aktiviert ist. Falls das Problem weiterhin besteht, leeren Sie den Java-Cache, indem Sie im selben Dialogfeld auf **Dateien löschen** klicken.

Wiederkehrende Probleme mit der Benutzeroberfläche, nachdem eine Verbindung über einen Load Balancer hergestellt wurde

Für BSM sind Sticky-Sitzungen für Benutzer erforderlich. Stellen Sie sicher, dass die Persistenz auf **stickiness by session enabled** oder **Destination Address Affinity** festgelegt ist (je nach Load Balancer).

Die BSM-Anmeldeseite wird nicht angezeigt, wenn die Verbindung über einen Load Balancer hergestellt wurde

- Prüfen Sie die KeepAlive-URIs. Weitere Informationen finden Sie unter dem Themenbereich "Load Balancer für den Gateway-Server".
- Virtuelle Hosts und Load Balancer sollten mit einem vollqualifizierten Domänennamen (und nicht über die IP-Adresse) konfiguriert werden, damit LW-SSO funktioniert.

BSM-Dialogfelder und -Applets wie der Authentifizierungs-Assistent werden nicht richtig geladen

Mögliche Ursache:

Alte Java-Dateien auf dem Client-PC.

Lösung:

Löschen Sie mit den folgenden Schritten den Java-Cache:

- Navigieren Sie zu Start > Systemsteuerung > Java.
- Klicken Sie im Abschnitt Temporäre Internetdateien auf Einstellungen.
- Klicken Sie im Dialogfeld Temporäre Internetdateien auf Dateien löschen.

BSM wurde installiert, die Seite für Downloads ist jedoch leer

Mögliche Ursache:

Die Setupdateien von Komponenten wurden nicht auf der Seite für Downloads installiert.

Lösung:

Installieren Sie die Setupdateien von Komponenten auf der Seite für Downloads. Details zur Installation von Setupdateien für Komponenten auf einer Windows-Plattform finden Sie unter "Installieren der Setupdateien von Komponenten".

Allgemeine Verbindungsprobleme im Zusammenhang mit Ports

Stellen Sie sicher, dass alle für BSM-Server erforderlichen Ports nicht von anderen Applikationen auf demselben Computer verwendet werden. Öffnen Sie dazu ein Eingabeaufforderungsfenster und führen Sie **netstat** aus (oder verwenden Sie ein Dienstprogramm, mit dem Sie Portinformationen anzeigen können). Suchen Sie nach den erforderlichen Ports.

Details zu den für BSM erforderlichen Ports finden Sie unter "Port Usage" im Handbuch BSM Hardening Guide.

Tipp: Sie können Probleme mit der Portverwendung beheben, indem Sie ein Dienstprogramm verwenden, mit dem alle verwendeten Ports und die jeweiligen Applikationen aufgelistet werden.

Die BSM-Verbindungen wurden unterbrochen, aber die Servlet-Engine von Tomcat sowie JBoss Application Server scheinen zu funktionieren

Zu den Verbindungsproblemen gehört, dass eine Anmeldung bei BSM nicht möglich ist und dass Business Process Monitor keine Verbindung mit dem Gateway-Server herstellen kann.

Mögliche Ursache:

Dies kann eintreten, wenn die Datei TopazInfra.ini leer oder beschädigt ist.

So überprüfen Sie, ob dies das Problem ist:

1. Geben Sie im Browser http://<Gateway-Server>:8080/web-console ein, um eine Verbindung mit der JMX-Konsole herzustellen.

Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).

- 2. Wählen Sie unter **System > JMX MBeans > Topaz** die Option **Topaz:service=Connection Pool Information** aus.
- 3. Klicken Sie unten auf der Seite auf die Schaltfläche showConfigurationSummaryInvoke. Ist die Seite Operation Result leer, ist die Datei TopazInfra.ini leer oder beschädigt.

Lösung:

Sie können dieses Problem lösen, indem Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration erneut ausführen und die Verbindung mit der vorhandenen Verwaltungsdatenbank erneut herstellen oder eine neue Verwaltungsdatenbank definieren. Wenn Sie kein Problem mit der Datei **TopazInfra.ini** feststellen konnten, wenden Sie sich an den HP Software-Unterstützung.

Eine Anmeldung bei BSM ist nicht möglich, und JBoss Application Server wird nicht initialisiert

Führen Sie das Programm zur Überprüfung des Datenbankschemas aus, um zu überprüfen, ob der Datenbankserver, auf dem die Verwaltungsdatenbank ausgeführt wird, betriebsbereit ist. Weitere Informationen finden Sie unter "Database Schema Verification" im Handbuch BSM Database Guide.

Der Browser erreicht BSM nicht und ein Fehler zu unzureichendem Heap-Speicher tritt auf

Ein Meldungsfeld wird geöffnet, in dem angegeben wird, dass BSM nicht verfügbar ist und dass Sie die Anmeldung später wiederholen sollten.

Mögliche Ursache 1:

Überprüfen Sie die Protokolldateien im Verzeichnis < HPBSM Stammverzeichnis>\log auf Fehler.

Das Microsoft-Sicherheitsupdate 921883 für Windows 2003 Service Pack 1 und für Windows XP Professional x64 Edition kann zu Fehlem bei Applikationen führen, die mehr als 700 MB zusammenhängenden Speicher nutzen. BSM-JVM verwendet eine Heap-Größe von mehr als 768 MB Speicher. Weitere Informationen zum Sicherheitsupdate 921883 finden Sie unter http://www.microsoft.com/technet/security/Bulletin/MS06-040.mspx.

Wenn der BSM-Server ausfällt, suchen Sie nach dem folgenden Fehler in < **Stammverzeichnis** des HPBSM-Servers>\log\jboss_boot.log, wenn der Dienst oder Prozess neu gestartet wird:

```
Error occurred during initialization of VM. Could not reserve enough space for object heap.
```

Lösung:

Zwar bietet Microsoft speziell für Microsoft Support-Kunden ein Hotfix an, es empfiehlt sich aber, bis zur Veröffentlichung des nächsten Service Packs zu warten. Weitere Informationen zu diesem Hotfix finden Sie in http://support.microsoft.com/kb/924054.

Ist das Sicherheitsupdate 921883 bereits installiert, führen Sie folgenden Schritte aus:

- Falls das Sicherheitsupdate für Ihre Website nicht wichtig ist:
- Deinstallieren Sie das Sicherheitsupdate und warten Sie auf das n\u00e4chste Service Pack von Microsoft.
- Deaktivieren Sie die automatischen Windows-Updates, damit das Sicherheitsupdate 921883 nicht erneut installiert wird.
- Falls das Sicherheitsupdate für Ihre Website wichtig ist, installieren Sie das Hotfix.

Mögliche Ursache 2:

Die Auslagerungsdatei ist zu klein.

Lösung:

Konfigurieren Sie als Größe der Auslagerungsdatei mindestens 150 % der RAM-Größe. Starten Sie den Server neu.

Der Browser erreicht BSM nicht oder der JSP-Quellcode wird im Browserfenster angezeigt

Ein Meldungsfeld wird geöffnet, in dem angegeben wird, dass die BSM-Seite nicht vorhanden ist.

Lösung:

Stellen Sie sicher, dass der Jakarta-Filterpfad richtig ist. Der Pfad kann falsch sein, falls Sie z. B. BSM-Server deinstallieren und dann in einem anderen Verzeichnis neu installieren. In diesem Fall wird der Jakarta-Filterpfad nicht aktualisiert und führt so zu Umleitungsproblemen.

So aktualisieren Sie den Jakarta-Filterpfad:

- Öffnen Sie den Internetdienste-Manager von IIS.
- 2. Klicken Sie mit der rechten Maustaste in der Struktur auf den Computernamen und wählen Sie **Properties** aus.
- 3. Wenn WWW Service in der Liste Master Properties angezeigt wird, klicken Sie auf Edit.
- 4. Wählen Sie die Registerkarte ISAPI Filter aus.
- 5. Wählen Sie jakartaFilter aus und klicken Sie auf Edit.
- 6. Aktualisieren Sie im Feld **Filter Properties** den Pfad, sodass er auf das Laufwerk und das Verzeichnis der aktuellen BSM-Installation verweist.

- 7. Übernehmen Sie die Änderungen und beenden Sie den Internetdienste-Manager.
- 8. Starten Sie den IIS-Dienst neu.

BSM befindet sich hinter einem Proxy und der Servername wird vom Proxy nicht erkannt

Das Problem tritt bei Microsoft IIS und Apache Web Server auf.

Mögliche Ursache:

Der Webserver leitet die Browserseite an eine URL weiter, die den vom Benutzer eingegebenen Servernamen ersetzt.

Lösung:

Fügen Sie den BSM-Servernamen der Datei < Windows-

Systemstammverzeichnis>\system32\drivers\etc\hosts auf dem Proxy-Server hinzu.

Hostnamen des Gateway-Servers oder des Servers für die Datenverarbeitung wurden geändert

Sie können auf BSM nicht mehr über die Namen der Server zugreifen, auf denen das Programm installiert wurde, und müssen die Namen der Server ändern. Informationen finden Sie in der HP-Wissensdatenbank zum Lösen von Softwareproblemen im Artikel KM522738, auf den Sie unter http://h20230.www2.hp.com/selfsolve/document/KM522738 zugreifen können.

Prozesse werden nach einem automatischen Failover nicht automatisch neu gestartet

Wenn der automatische Failover-Modus des Hochverfügbarkeitscontrollers aktiviert ist und die Verwaltungsdatenbank seit einer gewissen Zeit ausgefallen ist, werden einige Prozesse möglicherweise beendet und nicht automatisch fortgesetzt, sobald die Verwaltungsdatenbank wieder normal funktioniert. Bei diesen Prozessen wird der Status **Wird gestartet** auf der BSM-Statusseite (**<HPBSM-**

Stammverzeichnis>\AppServer\webapps\myStatus.war\myStatus.html, aufzurufen im Windows-Betriebssystem über Start > Programme > HP Business Service Management > Verwaltung > HP Business Service Management Status) angezeigt.

Lösung:

Starten Sie diese Prozesse neu, wenn die Verwaltungsdatenbank wieder verfügbar ist.