

IBM Intelligent Operations Center



# IBM Intelligent Operations Center Documentazione del prodotto

*Versione 1 Release 5*



IBM Intelligent Operations Center



# IBM Intelligent Operations Center Documentazione del prodotto

*Versione 1 Release 5*

**Nota**

Prima di utilizzare queste informazioni e il prodotto supportato, leggere le informazioni contenute in “Informazioni particolari” a pagina 359.

Questa edizione si applica a IBM Intelligent Operations Center versione 1, release 5, modifica 0 e a tutte le release e modifiche successive fino a quando non viene diversamente indicato nelle nuove edizioni.

© Copyright IBM Corporation 2011, 2012.

# Indice

<b>Figure</b> . . . . .	<b>vii</b>
-------------------------	------------

## **Capitolo 1. Panoramica della soluzione** **1**

Destinatari previsti . . . . .	1
Funzioni . . . . .	2
Utenti e vantaggi . . . . .	3
Componenti . . . . .	5
Gestione eventi . . . . .	7
Novità nella versione 1.5 . . . . .	8
Novità per l'utente . . . . .	8
Novità per l'amministratore . . . . .	9

## **Capitolo 2. Installazione e configurazione** . . . . . **11**

Preparazione per l'installazione . . . . .	11
I servizi di sistema IBM Intelligent Operations Center . . . . .	11
Requisiti hardware di IBM Intelligent Operations Center . . . . .	12
Requisiti software . . . . .	13
Browser supportati . . . . .	13
Packaging del supporto . . . . .	14
Elenchi di controllo installazione . . . . .	14
Elenco di controllo - installazione utilizzando IBM Installation Manager . . . . .	14
Elenco di controllo - installazione dettagliata . . . . .	16
Preparazione dei server . . . . .	17
Connessione di rete TCP/IP . . . . .	21
Copia del package di installazione in server di installazione . . . . .	25
Installazione di JRE (Java runtime environment) . . . . .	26
Installazione di IBM Intelligent Operations Center utilizzando Installation Manager . . . . .	26
Componenti dell'installazione . . . . .	30
Opzioni di configurazione . . . . .	31
Riavvio dell'installazione utilizzando Installation Manager . . . . .	34
Installazione dettagliata di IBM Intelligent Operations Center . . . . .	34
Preparazione del package di installazione . . . . .	34
Verifica degli script di installazione . . . . .	35
Personalizzazione delle proprietà di installazione . . . . .	35
Installazione dei file della topologia . . . . .	36
Esecuzione dello strumento di pre-verifica . . . . .	43
Impostazioni di sicurezza Linux . . . . .	44
Comando installTopology . . . . .	45
Opzioni per l'installazione dei componenti di IBM Intelligent Operations Center . . . . .	46
Riavvio dell'installazione dell'architettura IBM Intelligent Operations Center durante un'installazione dettagliata . . . . .	49
Installazione di Strumento di controllo della piattaforma . . . . .	49
Installazione dello strumento Controllo di verifica del sistema . . . . .	50

Installazione dell'applicazione IBM Intelligent Operations Center . . . . .	51
Verifica dell'installazione . . . . .	52
Configurazione post-installazione di IBM Intelligent Operations Center . . . . .	53
Configurazione dei servizi di collaborazione per IPv6 . . . . .	53
Configurazione di SSO (Single Sign-On) per i servizi di collaborazione . . . . .	54
Impostazione del timeout della sessione . . . . .	55
Installazione e configurazione di servizi di modelli semantici . . . . .	56
Configurazione di Strumento di controllo della piattaforma . . . . .	60
Codifica della password di gestione di Tivoli Service Request Manager . . . . .	60
Impostazione del numero minimo di processi per EventProcessor . . . . .	61
Modifica della dimensione del pool di thread predefinito e WebContainer . . . . .	61
Installazione ed esecuzione guidata di cyber hygiene . . . . .	62
Modifiche al sistema operativo Linux . . . . .	64
Controllare il log cyber hygiene . . . . .	64
Nuova abilitazione accesso root remoto . . . . .	65
Configurazione di utenti che richiedono accesso ssh . . . . .	66
Strumenti di installazione forniti con la soluzione . . . . .	66
Eliminazione di utenti di esempio . . . . .	67
Rimozione dei servizi di installazione dal sistema di produzione . . . . .	68

## **Capitolo 3. Protezione della soluzione** **69**

Ruoli utente e accesso . . . . .	70
Utenti di esempio . . . . .	71
Gruppi di ruoli utente e autorizzazioni . . . . .	72
Gruppi di categoria utente e autorizzazioni ai dati . . . . .	74
Aggiunta di un gruppo o di un utente . . . . .	75
Visualizzazione o modifica dell'appartenenza al gruppo . . . . .	77
Visualizzazione o modifica di un profilo utente . . . . .	78
Eliminazione di un utente o di un gruppo . . . . .	78
Importazione di utenti e gruppi . . . . .	79
Riepilogo autorizzazioni utente . . . . .	80
Panoramica su cyber hygiene . . . . .	81
Sicurezza Cyber . . . . .	82
Elenco di controllo Cyber hygiene . . . . .	83
Configurazione predefinita di Cyber hygiene . . . . .	85
Strumenti di soluzione . . . . .	89
Documentazione Cyber hygiene . . . . .	89

## **Capitolo 4. Integrazione della soluzione** **91**

Esempi dei sistemi che possono essere integrati . . . . .	91
Integrazione punti e protocolli . . . . .	91
Eventi e KPI . . . . .	91
Integrazione con CAP (Common Alerting Protocol) . . . . .	93

Creazione di eventi utilizzando il servizio Publisher . . . . .	100
Creazione e pubblicazione degli eventi di test Publisher di esempio . . . . .	103
Programmazione script di eventi . . . . .	107
Creazione ed integrazione dei KPI . . . . .	109
Monitoraggio dei modelli e KPI . . . . .	110
Monitoraggio istanze di contesto . . . . .	111
Modellazione dei PKI. . . . .	111
Definizione delle gerarchie KPI . . . . .	114
Definizione di gerarchie KPI con OWL . . . . .	115
Comunicazione evento KPI tra IBM WebSphere Business Monitor e IBM Intelligent Operations Center. . . . .	116
Distribuzione dei modelli di monitoraggio. . . . .	119
Valori di visualizzazione KPI . . . . .	120
Memorizzazione nella cache dei KPI. . . . .	121
KPI di esempio. . . . .	121
Configurazione di Tivoli Service Request Manager Utilizzo dell'interfaccia utente Tivoli Service Request Manager. . . . .	124
Configurazione di nuovi utenti in Tivoli Service Request Manager . . . . .	126
SOP (Standard Operating Procedure) . . . . .	127
Gestione risorse . . . . .	132
Esempi e risorse procedure operative standard, flussi di lavoro . . . . .	138

## Capitolo 5. Personalizzazione della soluzione . . . . . 141

Personalizzazione dell'interfaccia utente Localizzazione dell'interfaccia utente . . . . .	141
Elenco di portlet . . . . .	141
Creazione e personalizzazione di una pagina Personalizzazione dei portlet . . . . .	145
Personalizzazione della guida del portlet . . . . .	165
Ubicazioni dei file della guida del portlet . . . . .	166
Personalizzazione dei KPI . . . . .	167
KPI (Key Performance Indicators) . . . . .	168
Backup prima della personalizzazione KPI . . . . .	172
Personalizzazione degli eventi correlati. . . . .	173
Correlazione di eventi e applicazione delle regole . . . . .	173
Personalizzazione delle impostazioni di correlazione eventi . . . . .	173
Gestore mappa ubicazioni . . . . .	176
Aggiunta di una classificazione al menu mappa . . . . .	177
Aggiunta di una mappa al portlet . . . . .	177
Aggiunta o modifica delle aree in un mappa ubicazioni . . . . .	177
Personalizzazione del portlet Gestore mappa ubicazioni . . . . .	178
Specificazione dei dati di configurazione del sistema . . . . .	178
Aggiornamento della tabella delle proprietà del sistema . . . . .	183
Configurazione di IBM Cognos Business Intelligence per la creazione di report . . . . .	184
Creazione di un portlet Report . . . . .	184
Modifica del layout del portlet Report . . . . .	185
Personalizzazione di un portlet per la visualizzazione di report . . . . .	185

Individuazione degli URL del report . . . . .	186
Come lavorare con il modello di dati . . . . .	186

## Capitolo 6. Gestione della soluzione 195

Informazioni . . . . .	195
Controllo dei servizi . . . . .	195
Avvio dei servizi . . . . .	196
Avvio e arresto del probe Tivoli Netcool/OMNIbus . . . . .	199
Arresto dei servizi. . . . .	199
Query dello stato dei servizi . . . . .	202
Come ottenere supporto per Strumento di controllo della piattaforma . . . . .	203
Console di gestione . . . . .	203
Gestione dei servizi . . . . .	206
Verifica dei componenti . . . . .	210
Come utilizzare lo strumento Controllo di verifica del sistema . . . . .	210
Test di Controllo di verifica del sistema. . . . .	211

## Capitolo 7. Manutenzione della soluzione . . . . . 259

Esecuzione backup dei dati. . . . .	259
Ottimizzazione delle prestazioni . . . . .	260
Ottimizzazione di server delle applicazioni . . . . .	260
Ottimizzazione di WebSphere Application Server . . . . .	261
Gestione file di log . . . . .	261
Aggiornamento del token LTPA per SSO (single sign-on) . . . . .	261
Suggerimenti per la manutenzione . . . . .	263

## Capitolo 8. Utilizzo dell'interfaccia di soluzioni . . . . . 265

Collegamento . . . . .	265
Scollegamento . . . . .	266
Visualizzazione o modifica del profilo utente. . . . .	266
Utilizzo di pagine . . . . .	267
Vista Supervisore: Stato . . . . .	267
Vista Supervisore: Operazioni . . . . .	268
Vista Operatore: Operazioni . . . . .	269
Supervisore: Report . . . . .	270
Operatore: Report . . . . .	270
Vista Mappa ubicazioni . . . . .	270
Utilizzo di portlet . . . . .	271
Contatti . . . . .	271
Dettagli . . . . .	272
Gestione di eventi e incidenti . . . . .	274
Gestione delle risorse. . . . .	275
Personalizzazione del portlet Dettagli . . . . .	275
Drill Down KPI (Key Performance Indicator) . . . . .	275
Mappa ubicazioni . . . . .	276
Controlli della mappa . . . . .	278
Selezione di categorie di eventi per la mappa . . . . .	278
Personalizzazione del portlet Mappa ubicazioni Mappa . . . . .	279
Utilizzo dei controlli della mappa . . . . .	281
Selezione di categorie di eventi per la mappa . . . . .	282
Selezione di funzionalità di risorse per la mappa . . . . .	282
Reimpostazione della mappa . . . . .	282

Aggiunta di un evento . . . . .	283
Personalizzazione del portlet Mappa . . . . .	284
Attività personali . . . . .	284
Notifiche . . . . .	287
Report. . . . .	288
Stato . . . . .	291

**Capitolo 9. Risoluzione dei problemi e supporto . . . . . 293**

Tecniche per la risoluzione dei problemi . . . . .	293
Abilitazione delle tracce e visualizzazione dei file di log . . . . .	295
File di log del Server delle applicazioni. . . . .	295
File di log del Server eventi . . . . .	296
Esecuzione dello strumento "must gather" dell'installazione . . . . .	299
Risoluzione dei problemi dei componenti . . . . .	300
Installazione ed utilizzo di IBM Support Assistant Lite. . . . .	303
Messaggi di IBM Intelligent Operations Center . . . . .	304
Utilizzo di Knowledge base e del supporto IBM	322
Ricerca nei knowledge base . . . . .	322
Ottenimento di fix da Fix Central. . . . .	323
Contattare il supporto IBM . . . . .	324
Sottoscrizione agli aggiornamenti del supporto	325
Scambio di informazioni con IBM . . . . .	326
Problemi noti e soluzioni . . . . .	328
Gli errori di connessione quando si installa IBM Intelligent Operations Center . . . . .	330
La rete IPv6 non viene avviata . . . . .	330
Tivoli Service Request Manager non parte. . . . .	330
Impossibile creare una nuova pagina per l'interfaccia utente . . . . .	331
Soluzioni temporanee per l'accesso facilitato per i portlet . . . . .	331
Soluzione temporanea di accessibilità per la selezione di date nel portlet Report . . . . .	332
I nuovi eventi non vengono visualizzati nel portlet Dettagli . . . . .	332
Meccanismo di autenticazione non disponibile	334
Un server di terze parti non risponde . . . . .	335
Nel portlet Attività personali non viene visualizzata alcuna attività . . . . .	335
Risoluzione dei problemi relativi ai dati di esempio . . . . .	335
Verifica dello stato di Tivoli Service Request Manager . . . . .	336
Verifica delle autorizzazioni utente . . . . .	337
Verifica dell'associazione di un flusso di lavoro ad una procedura operativa standard . . . . .	338
Verifica dei file di log. . . . .	338

I dati KPI non vengono visualizzati nei portlet Stato o Drill Down KPI (Key Performance Indicator). . . . .	339
Gli eventi non vengono aggiornati nei portlet Stato o Drill Down KPI (Key Performance Indicator). . . . .	339

**Capitolo 10. Riferimento. . . . . 341**

Prodotti e componenti inclusi con IBM Intelligent Operations Center . . . . .	341
Processi in esecuzione con l'account root . . . . .	342
Eccezioni Cyber hygiene. . . . .	343
Le autorizzazioni file che richiedono la convalida dell'amministratore di sistema. . . . .	344
Certificazione della sicurezza del prodotto e dei componenti . . . . .	345
Libreria di PDF. . . . .	346
Glossario . . . . .	346
A . . . . .	346
B . . . . .	347
C . . . . .	347
D . . . . .	348
E . . . . .	348
F . . . . .	349
G . . . . .	349
H . . . . .	349
I . . . . .	350
J . . . . .	350
K . . . . .	350
L . . . . .	351
M . . . . .	352
N . . . . .	352
O . . . . .	352
P . . . . .	352
R . . . . .	352
S . . . . .	353
T . . . . .	354
U . . . . .	354
V . . . . .	355
W . . . . .	355
X . . . . .	356
Ulteriori informazioni sul prodotto . . . . .	356
Avviso sul copyright e marchi. . . . .	357
Avviso sul copyright . . . . .	357
Marchi . . . . .	358

**Informazioni particolari . . . . . 359**

Marchi . . . . .	360
------------------	-----

**Indice analitico. . . . . 363**





---

## Figure



---

## Capitolo 1. Panoramica della soluzione

Molte organizzazioni e imprese richiedono una supervisione operativa e un coordinamento efficienti. Hanno tutte in comune la necessità di riunire insieme le giuste informazioni in modo che le persone appropriate possano prendere decisioni rapide ed accurate, e possano tenere traccia dell'effetto di tali decisioni. IBM® Intelligent Operations Center è una soluzione software progettata per facilitare una supervisione e un coordinamento efficaci delle operazioni.

Le autorità affrontano sfide comuni nei loro sistemi base e nell'apportare miglioramenti ai sistemi interconnessi. Le autorità all'avanguardia desiderano utilizzare i miglioramenti con l'efficienza e l'efficacia dei sistemi base smarter. Adottano nuovi modi di pensare nei confronti di questi sistemi e di utilizzarli. L'applicazione di IT (information technology) avanzata può aiutare le autorità a comprendere meglio, prevedere e rispondere in modo intelligente ai modelli di comportamento e agli eventi.

Ad esempio, IBM definisce una città intelligente in termini di miglioramenti nella qualità della vita e nel benessere economico raggiunti mediante l'applicazione di IT (information technology) per pianificare, progettare, creare ed operare l'infrastruttura della città. Una città intelligente non è principalmente una questione di "tecnologia più recente." Si tratta di trovare i modi per utilizzare la tecnologia e fare un utilizzo di massima efficacia delle risorse esistenti, per migliorare la vita dei cittadini della città.

IBM Intelligent Operations Center utilizza la potenza dei dati del mondo reale generati da sistemi di computer:

- Raccogliendo e gestendo i dati corretti
- Integrando e analizzando quei dati
- Facilitando un accesso facile e tempestivo alle informazioni
- Presentando informazioni correlate in un modo coerente

I vantaggi di questa soluzione sono di:

- Regolare i sistemi per raggiungere risultati basati sulla consapevolezza guadagnata
- Ottimizzare operazioni pianificate e non pianificate utilizzando un approccio olistico di report e monitoraggio
- Creare una convergenza di domini in un'organizzazione facilitando la comunicazione e la collaborazione
- Migliorare la qualità del servizio e ridurre la spesa coordinando gli eventi

Un'operazione può essere suddivisa in singoli domini, che in genere corrispondono alla struttura dell'organizzazione e alla competenza delle persone coinvolte. In una città, la competenza viene mantenuta in dipartimenti, ad esempio trasporto, acqua e sicurezza pubblica.

Poiché la complessità delle operazioni in un dominio è in aumento, è necessaria una soluzione più personalizzata. IBM Intelligent Operations Center ha una serie di punti di integrazione differenti in cui può avvenire la personalizzazione. Questi punti di integrazione e l'infrastruttura inclusi forniscono ai partner commerciali IBM, ai provider di servizi e ai clienti la flessibilità per creare una soluzione vasta e potente.

---

### Destinatari previsti

Questo centro informazioni è rivolto alle persone che utilizzano, installano, gestiscono e amministrano IBM Intelligent Operations Center. Contiene inoltre la documentazione di implementazione per personalizzare la soluzione e integrare i sistemi esterni sottostanti richiesti da IBM Intelligent Operations Center.

Questo centro informazioni si basa sul presupposto che gli utenti abbiano una precedente conoscenza o competenza nell'utilizzo dei prodotti componente inclusi in questa soluzione. Il centro informazioni si basa inoltre sul presupposto che gli utenti abbiano una conoscenza di base del sistema operativo Red Hat Enterprise Linux. La formazione per i prodotti componente o per il sistema operativo esula dall'ambito di questo centro informazioni. Se si richiede una formazione per questi prodotti, domandare all'integratore di sistemi o al rappresentante IBM dove è possibile ottenere informazioni relative alle opportunità di formazione sui componenti di base.

I link alla documentazione del prodotto del componente sono disponibili nella sezione Riferimento; consultare il link alla fine dell'argomento.

#### **Concetti correlati:**

“Ulteriori informazioni sul prodotto” a pagina 356

Le seguenti ulteriori risorse sono disponibili online.

---

## **Funzioni**

IBM Intelligent Operations Center fornisce funzioni di misurazione, monitoraggio e modellazione che integrano i sistemi sottostanti in un'unica soluzione per migliorare l'efficienza operativa, la pianificazione e il coordinamento.

IBM Intelligent Operations Center è una soluzione all'interno della famiglia di prodotti IBM Smarter Cities Software Solutions. IBM Intelligent Operations Center può essere installato su hardware esistente (sul posto) o può essere distribuito nel cloud. IBM Intelligent Operations Center può essere installato da solo o con altre soluzioni della famiglia di prodotti IBM Smarter Cities Software Solutions.

IBM Intelligent Operations Center è una soluzione basata su GUI con accesso agli eventi in base al ruolo per un'organizzazione e i domini sottostanti. Dispone delle funzionalità di gestione eventi, associazione integrata e monitoraggio delle risorse. La soluzione può fornire e seguire le procedure appropriate e il flusso di lavoro per le attività in preparazione e in risposta agli eventi. Dispone inoltre delle funzionalità di KPI (key performance indicator), di creazione di report e di collaborazione per una migliorata efficacia. Queste funzioni forniscono alle autorità la possibilità di integrare domini per una migliorata cooperazione e scelta decisionale.

### **Gestione di eventi e incidenti**

IBM Intelligent Operations Center fornisce un meccanismo di notifica eventi e di traccia per consentire l'identificazione e la comprensione tra i domini sottostanti. È possibile gestire eventi previsti, eventi pianificati ed eventi correnti mentre si evolvono. Ad esempio, la sostituzione di tubature che passano sotto una strada è un evento pianificato o un ordine di lavoro che implica operazioni idriche e stradali. Condizioni atmosferiche inclementi in arrivo entro le successive 24 ore è un evento previsto. Un intasamento del traffico è un evento corrente interessato sia dai lavori stradali che dalle condizioni atmosferiche.

Un GIS (geographic information system) integrato o un piano di ubicazione associa visivamente gli eventi, in modo da poter misurare l'impatto degli eventi mediante l'associazione interattiva e l'analisi dello scenario.

### **Gestione di risorse, risposte e attività**

IBM Intelligent Operations Center fornisce un sistema per memorizzare le procedure e i flussi di lavoro appropriati in base alle attività associate agli eventi. È possibile tracciare l'avanzamento dei flussi di lavoro e monitorare o aggiornare lo stato delle attività assegnate all'utente.

Le informazioni relative ad una gamma delle risorse disponibili possono essere evidenziate su una mappa. Le informazioni sono facili da accedere quando e dove necessario.

## Monitoraggio dello stato

IBM Intelligent Operations Center fornisce uno strumento per la creazione e la visualizzazione dei KPI. I KPI possono essere aggiornati come modifiche dei dati sottostanti. È possibile utilizzare questo strumento per:

- Riepilogare lo stato a livello esecutivo per un singolo dominio o tra i domini
- Evidenziare le problematiche ed identificare i problemi
- Indagare ulteriormente approfondendo i dettagli dei KPI

## Notifica istantanea e messaggistica

IBM Intelligent Operations Center fornisce uno spazio di lavoro dove è possibile gestire gli avvisi per le questioni che richiedono attenzione. È possibile utilizzare questo spazio di lavoro per monitorare le notizie e gli eventi, specialmente quando altri portlet che annunciano novità non sono nella vista.

IBM Lotus Sametime fornisce uno strumento integrato di collaborazione e comunicazione che può essere utilizzato per i messaggi istantanei dove e quando necessario.

## Produzione di report

IBM Intelligent Operations Center dispone di una funzione integrata di creazione report che consente all'utente di impostare ed eseguire report con gli eventi e i KPI forniti dalla soluzione. È possibile utilizzare questa funzione per raccogliere e presentare le informazioni più utili per l'utente su base regolare e aggiornata. Questa funzione fornisce all'utente tutti i vantaggi dei riepiloghi personalizzati e della presentazione grafica.

---

## Utenti e vantaggi

IBM Intelligent Operations Center è progettato per il personale coinvolto nel controllo operativo nelle organizzazioni, nei dipartimenti governativi, nelle autorità locali o cittadine: dirigenti, supervisor e operatori.

La seguente tabella descrive gli utenti e i vantaggi associati all'utilizzo di IBM Intelligent Operations Center.

*Tabella 1. Utenti e vantaggi di IBM Intelligent Operations Center*

Se si è un...	Questo software può aiutare a...
Esecutivo	<ul style="list-style-type: none"><li>• Ottenere un riepilogo a livello esecutivo degli eventi e degli incidenti attraverso mappe, dashboard, avvisi</li><li>• Determinare le misurazioni dell'esito organizzativo con i KPI (key performance indicator)</li><li>• Identificare e tracciare i problemi tramite i report</li><li>• Indirizzare le priorità e l'implementazione della politica sulla base dei dati forniti</li></ul>

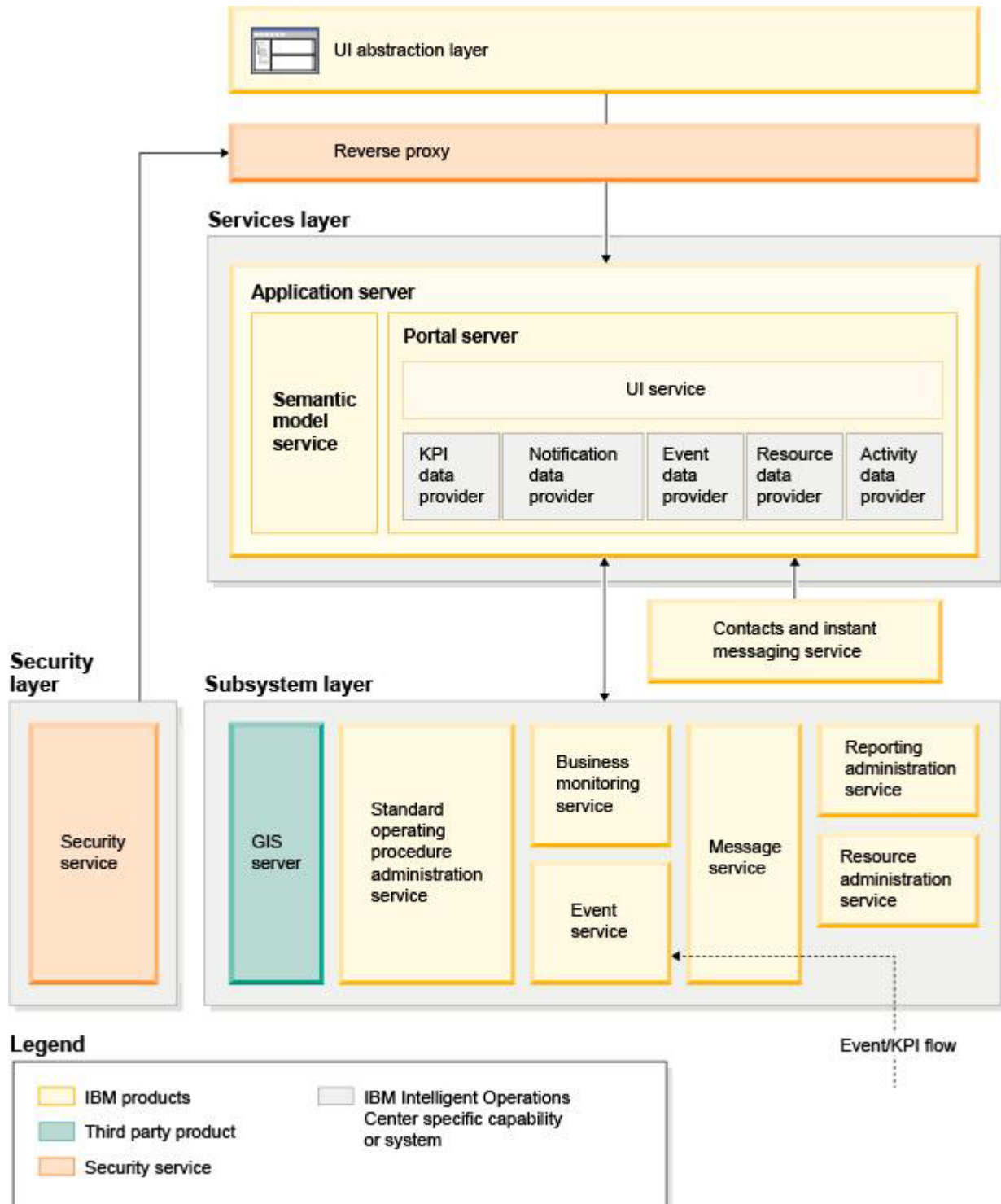
Tabella 1. Utenti e vantaggi di IBM Intelligent Operations Center (Continua)

Se si è un...	Questo software può aiutare a...
Supervisore	<ul style="list-style-type: none"> <li>• Identificare ed agire sui conflitti e sui problemi mostrati nelle mappe, nei dashboard e negli avvisi</li> <li>• Gestire gli eventi aggiungendo nuovi eventi, modificando eventi esistenti, annullando eventi ed eseguendo un'escalation degli eventi in incidenti</li> <li>• Fornire informazioni sulle risorse e gestire le risorse</li> <li>• Memorizzare e gestire l'esecuzione di procedure e flussi di lavoro associati agli eventi</li> <li>• Monitorare i KPI</li> <li>• Comunicare rapidamente e facilmente su questioni importanti</li> <li>• Progettare utili report</li> </ul>
Operatore	<ul style="list-style-type: none"> <li>• Creare, modificare e monitorare eventi di stato e incidenti da visualizzare negli elenchi</li> <li>• Ricevere e aggiornare lo stato delle attività assegnate</li> <li>• Controllare le risorse disponibili</li> <li>• Eseguire report regolari e aggiornati</li> <li>• Notificare, aggiornare e inviare avvisi a colleghi, responsabili o dirigenti appropriati</li> <li>• Comunicare rapidamente e facilmente durante le emergenze ed altre situazioni che richiedono una risposta</li> </ul>
Amministratore utenti	<ul style="list-style-type: none"> <li>• Aggiungere nuovi utenti ed assegnarli a gruppi con l'autenticazione appropriata</li> <li>• Garantire la sicurezza dei dati tramite gruppi di autorizzazione di categoria e basati sul ruolo con le autorizzazioni appropriate</li> <li>• Impostare le autorizzazioni appropriate alle aree di competenza e ai dati richiesti</li> </ul>
Amministratore del sistema	<ul style="list-style-type: none"> <li>• Personalizzare le pagine e i portlet per adattarli all'organizzazione</li> <li>• Personalizzare, in base ai requisiti di gestione, gli eventi e i KPI visualizzati</li> <li>• Creare e pubblicare eventi di test</li> <li>• Configurare i report e la distribuzione</li> </ul>

# Componenti

Ad un livello elevato, la struttura di IBM Intelligent Operations Center può essere suddivisa in componenti principali, sottosistemi e servizi.

Il seguente diagramma mostra una vista di livello elevato di IBM Intelligent Operations Center.



## **Livello di astrazione della UI**

IBM Intelligent Operations Center fornisce portali centralizzati basati su web per informazioni sugli eventi, stato complessivo e dettagli. L'interfaccia utente (UI) presenta informazioni personalizzate in varie viste preconfigurate in formati comuni. Tutte le informazioni vengono visualizzate tramite dashboard di facile utilizzo.

## **Livello di sicurezza**

Tutto l'accesso alle informazioni è controllato dal livello di sicurezza mediante ruoli organizzativi e categorie di dati. Questo controllo impedisce l'accesso non autorizzato ma al contempo consentendo una facile gestione dei diritti.

## **Livello dei servizi**

Il livello dei servizi utilizza widget comuni e un framework di servizi di UI comuni per ricevere i dati degli eventi e trasmetterli al sistema di messaggi tramite la gestione eventi. I provider di dati di IBM Intelligent Operations Center estendono i servizi della UI. A causa della varietà di dati che possono essere forniti dai sistemi operativi sottostanti, i dati vengono normalizzati secondo un modello di riferimento semantico standard, che fornisce un dizionario comune per associare le relazioni. Questo modello facilita l'analisi dell'effetto e la risposta a eventi senza la necessità di più traduzioni di informazioni. Il modello semantico fornisce l'accesso a KPI e alle informazioni gerarchiche dei domini sottostanti. È possibile eseguire l'analisi avanzata sui dati, identificando le ottimizzazioni e le previsioni utili per la scelta decisionale e la governance.

## **Livello del sottosistema**

La soluzione fornisce un livello di mediazione per facilitare lo scambio di informazioni tra la soluzione i sistemi operativi dei domini sottostanti. I dati di varie origini configurabili possono essere forniti tramite gateway in un livello di sottosistema, che può generare avvisi, KPI ed eventi. Questo livello di integrazione consente la comunicazione bidirezionale dei messaggi in vari formati, open standard quando possibile. Utilizzando gli strumenti standard del settore per la trasformazione dalle origini al modello semantico di riferimento, non è necessario cambiare i sistemi operativi sottostanti. I sistemi di emergenza e di altro tipo di risposta possono essere connessi a IBM Intelligent Operations Center per i flussi di lavoro appropriati.

La struttura di IBM Intelligent Operations Center supporta:

- Un punto centrale per la comprensione dello stato delle operazioni, la gestione degli eventi e degli incidenti e la connessione dei domini sotto un controllo centrale delle operazioni
- L'integrazione con un GIS (geographic information system), un diagramma di mappa di ubicazioni o un piano per l'associazione di eventi, incidenti e risorse visivamente e in relazione allo spazio
- La creazione e il monitoraggio di KPI (key performance indicator), che vengono aggiornati quando i dati cambiano attraverso le connessioni ai sistemi dei domini sottostanti
- La creazione e il monitoraggio di procedure operative standard (SOP) con flussi di lavoro e attività in associazione con gli eventi
- Gli avvisi in arrivo dal campo, inclusi quelli che richiedono risposte di emergenza o standard
- La funzionalità di collaborazione, tramite una funzione di messaggistica istantanea con IBM Lotus Sametime
- La creazione e la distribuzione di report aggiornati e regolari basati sui dati di un evento o un KPI
- Un modello di sicurezza basato sul ruolo

Per ulteriori informazioni sui servizi di sistema di IBM Intelligent Operations Center, vedere il link alla fine dell'argomento.



## Concetti correlati:

“I servizi di sistema IBM Intelligent Operations Center” a pagina 11  
I server IBM Intelligent Operations Center forniscono una serie di servizi.

---

## Gestione eventi

La soluzione IBM Intelligent Operations Center è incentrata sull'integrazione e ottimizzazione delle informazioni all'interno e attraverso più domini in un hub operazioni centrale, in tempo reale e su lunghi periodi. La gestione dei dati degli eventi consente a IBM Intelligent Operations Center di assimilare dati provenienti da più sistemi per prevedere e reagire costantemente ad eventi e tendenze significative.

I messaggi di evento sono elementi di dati contenenti informazioni di base ma complete cui i destinatari possono rispondere. I messaggi di eventi vengono inseriti nelle code da IBM Intelligent Operations Center ed elaborati dal servizio di gestione degli eventi.

Gli eventi inseriti in IBM Intelligent Operations Center in forme diverse in base alla natura delle operazioni e dei domini nell'hub operazioni centrale. Alcuni esempi delle forme di evento sono: trigger, soglie, eventi complessi e gli eventi generati manualmente.

I trigger sono eventi generati da qualcosa che si verifica e generalmente richiedono un'azione che deve essere eseguita dal destinatario. Esempi di trigger sono:

- Attivazione di allarmi incendio o fumo
- Disattivazione di sistemi IT (Information Technology)
- Rivelatori antintrusione scattati
- Eventi naturali rilevati dai sensori, ad esempio tremori della terra.

IBM Intelligent Operations Center può ricevere informazioni su tali eventi da sistemi esterni e convertirli in avvisi per i destinatari. In generale, è probabile che gli indicatori di livello inferiore vengano riepilogati e trasmessi a IBM Intelligent Operations Center solo nel caso in cui meritino maggiore attenzione. Ad esempio, tutti gli incendi potrebbero non essere riportati come eventi. Tuttavia, un incendio che a causa di sostanze pericolose, coinvolge più divisioni del servizio antincendio e la competenza di tutela ambientale, dovrebbero essere segnalati al centro operazioni.

Gli eventi di soglia consentono di determinare quando le misurazioni ottenute da un sensore o da altra fonte sono esterni all'intervallo normale. Gli eventi di soglia di base confrontano due o più misure e segnalano una tendenza. Gli eventi di soglia più sofisticati possono confrontare le misure rispetto alle soglie create da informazioni cronologiche. Esempi di eventi di soglia sono:

- Sopra e sotto gli allarmi per la temperatura
- Livelli di acqua alta e bassa
- Qualità dell'aria e dell'acqua che violano le norme di purezza ambientale standard
- Un eccessivo consumo di energia

IBM Intelligent Operations Center può gestire tali eventi sotto forma di KPI (key performance indicator).

Gli eventi complessi aggregano informazioni provenienti da più sistemi per determinare se un gruppo di eventi correlati devono essere segnalati. Ad esempio, l'autorità per il pedaggio riceve un evento trigger dal sistema di monitoraggio che indica che il link del computer per l'autorizzazione della carta di credito non è attivo, seguito a breve da un evento di soglia del sistema finanziario che avverte che si sta per raggiungere il limite del credito per pagamenti non autorizzati. La combinazione di questi due problemi è molto più grave che se presi singolarmente, pertanto viene generato un evento complesso per sensibilizzare e coordinare una soluzione.

Gli eventi immessi manualmente sono particolarmente importanti nelle città. Alcuni di questi sono incidenti osservati, come crimini e incidenti stradali. Altri esempi di eventi immessi manualmente sono

quelli generati dalle chiamate di emergenza dei cittadini, dai report redatti dai funzionari di polizia o dai sistemi di gestione sullo stato della città. I tipi più comuni di evento immessi manualmente sono:

- Avvertenze meteo gravi
- Report sulla criminalità
- Incendi
- Incidenti stradali, incidenti, congestione, carichi insoliti
- Eventi imminenti - concerti rock, corse, parate

L'elaborazione di eventi complessi consente a una città di identificare facilmente le eccezioni nei sistemi urbani, di identificare le tendenze da dati non collegati e di prevedere problemi futuri.

---

## Novità nella versione 1.5

IBM Intelligent Operations Center 1.5 introduce nuove utili funzioni per l'amministratore e l'utente.

### Novità per l'utente

Con IBM Intelligent Operations Center 1.5 è possibile gestire le risorse e le attività associate ad un evento.

#### Gestione delle risorse e interazione con le mappe di ubicazioni

Nella nuova Mappa ubicazioni e nei portlet migliorati Mappa, è possibile:

- Valutare le risorse disponibili nelle vicinanze di un evento in base ad una mappa geografica.
- Lavorare con un nuovo tipo di mappa, una mappa di ubicazioni, con definite delle aree interattive. Ad esempio, una mappa di ubicazioni può essere basata su un piano di instradamenti per un sistema di trasporto.
- Visualizzare più di un evento raggruppato nella stessa ubicazione su una mappa.

 Per ulteriori informazioni relative al nuovo portlet Mappa ubicazioni ed ai portlet Mappa e Dettagli migliorati, consultare i link alla fine dell'argomento.

#### Traccia dello stato delle attività associate a eventi

Nel nuovo portlet Attività personali è possibile:

- Visualizzare per il proprio gruppo le attività aperte associate ad una procedura e un evento.
- Visualizzare lo stato delle attività assegnate a sé stessi.
- Modificare lo stato delle attività assegnate a sé stessi.

 Per ulteriori informazioni relative al portlet Attività personali, consultare il link alla fine dell'argomento.

#### Produzione di report

Nel nuovo portlet Report, è possibile:

- Visualizzare fino a sei report di eventi come grafici.
- Creare report personalizzati in base a criteri e dati selezionati, inclusi i report per eventi in base alla data o a un intervallo di date.
- Copiare un URL di report e far sì che il report venga visualizzato in un frame sul lato destro del portlet.

 Per ulteriori informazioni relative al portlet Report, consultare il link alla fine dell'argomento.

### **Concetti correlati:**

“Mappa ubicazioni” a pagina 276

Utilizzare il portlet Mappa ubicazioni per visualizzare gli eventi contrassegnati sulla mappa ubicazioni. Una mappa ubicazioni in IBM Intelligent Operations Center è una mappa o piano con aree predefinite per l'interazione, ad esempio, i posti a sedere di un principale stadio sportivo.

“Mappa” a pagina 279

Utilizzare il portlet Mappa per visualizzare eventi e risorse presenti su una mappa.

“Dettagli” a pagina 272

Utilizzare il portlet Dettagli per visualizzare, monitorare e gestire gli eventi in IBM Intelligent Operations Center.

“Attività personali” a pagina 284

Il portlet Attività personali visualizza un elenco dinamico di attività di proprietà del gruppo di cui l'utente collegato all'interfaccia è membro.

“Report” a pagina 288

Utilizzare il portlet Report per visualizzare un report di eventi come grafico. Il portlet fornisce diverse opzioni in base alle quali raggruppare gli eventi, ed è possibile scegliere gli eventi in base a una data o intervallo di date particolare. I report in questione consentono di pianificare gli eventi correnti e futuri.

## **Novità per l'amministratore**

Con la versione 1.5, è possibile personalizzare i portlet e i layout delle pagine. È possibile inoltre configurare procedure operative standard e flussi di lavoro.

### **Personalizzazione dei portlet**

Con le nuove opzioni di configurazione dei portlet per ogni portlet è possibile impostare:

- Proprietà specifiche per i singoli portlet, ad esempio impostare il punto centrale e il livello di zoom di una mappa
- Proprietà generiche per i portlet, ad esempio impostare l'altezza del portlet



Per ulteriori informazioni relative alla personalizzazione dei portlet, consultare il link alla fine dell'argomento.

### **Gestione degli eventi con procedure operative standard e flussi di lavoro**

È possibile definire procedure ed attività associate agli eventi:

- Definire procedure operative standard in base ad un piano di lavoro.
- Creare flussi di lavoro.
- Definire parametri per la selezione di una procedura operativa standard basata sui parametri di un evento.



Per ulteriori informazioni relative all'associazione delle attività associate agli eventi, consultare il link procedura operativa standard alla fine dell'argomento.

### **Script e pubblicazione di eventi**

È possibile utilizzare il nuovo portlet Programmazione script di eventi per creare un elenco sequenziale di eventi da pubblicare ad intervalli di tempo predefiniti.



Per ulteriori informazioni relative alla creazione di script ed alla pubblicazione di eventi, consultare il link alla fine dell'argomento.

## Verifica dello stato del servizio


È possibile utilizzare il nuovo strumento Controllo di verifica del sistema per verificare lo stato operativo dei servizi di IBM Intelligent Operations Center.

 Per ulteriori informazioni relative allo strumento Controllo di verifica del sistema, consultare il link alla fine dell'argomento.

## Supporto protocolli

IBM Intelligent Operations Center ora supporta eventi con protocolli diversi da CAP (Common Alerting Protocol). È possibile:

- Estendere i tipi enumerati per eventi CAP (Common Alerting Protocol) e non CAP (Common Alerting Protocol).
- Personalizzare i menu a comparsa nel portlet Dettagli.
- Accettare eventi da più domini da visualizzare nei portlet.

 Per ulteriori informazioni relative ai protocolli ed ai punti di integrazione, consultare il link alla fine dell'argomento.

### Concetti correlati:

“SOP (Standard Operating Procedure)” a pagina 127

È possibile definire procedure operative standard e le attività per la gestione degli eventi inseriti in IBM Intelligent Operations Center. Utilizzare il portlet SOP (Standard Operating Procedure) per accedere alle applicazioni procedura operativa standard, matrice di selezione procedura operativa standard e designer flusso di lavoro in Tivoli Service Request Manager.

“Programmazione script di eventi” a pagina 107

Utilizzare il portlet Programmazione script di eventi per scrivere uno script e creare un elenco sequenziale di eventi da pubblicare a intervalli di tempo predefiniti.

“Verifica dei componenti” a pagina 210

Lo strumento Controllo di verifica del sistema esegue il test dei componenti presenti in IBM Intelligent Operations Center per verificare se sono accessibili e funzionanti.

“Integrazione punti e protocolli” a pagina 91

Altri sistemi possono essere integrati con la soluzione attraverso i servizi e le politiche IBM Intelligent Operations Center. I dati possono essere ricevuti nel formato CAP (Common Alerting Protocol); sono anche supportati altri protocolli.

### Attività correlate:

“Personalizzazione dei portlet” a pagina 145

In qualità di amministratore è possibile modificare le impostazioni del portlet per personalizzare un portlet.

---

## Capitolo 2. Installazione e configurazione

IBM Intelligent Operations Center fornisce una procedura guidata di distribuzione che installa l'ambiente richiesto da IBM Intelligent Operations Center. Una volta distribuito l'ambiente e il pacchetto IBM Intelligent Operations Center, sono richieste alcune configurazioni aggiuntive.

---

### Preparazione per l'installazione

Prima di distribuire IBM Intelligent Operations Center, conoscere la configurazione di sistema IBM Intelligent Operations Center ed accertarsi che i prerequisiti per l'ambiente siano soddisfatti.

### I servizi di sistema IBM Intelligent Operations Center

I server IBM Intelligent Operations Center forniscono una serie di servizi.

#### Servizi analitici

Fornisce servizi di analisi e presentazione dei dati.

#### Server delle applicazioni

Fornisce i servizi Java Enterprise Edition di supporto al prodotto.

#### Sicurezza

Fornisce servizi che determinano se un utente è autorizzato ad utilizzare il sistema e definirne i privilegi.

#### Servizi di autorizzazione

Fornisce servizi che determinano i servizi che l'utente è autorizzato ad utilizzare.

#### Monitoraggio del business

Fornisce aggregazione, analisi e presentazione dei processi di business e le informazioni sulle attività in tempo reale.

#### Server di messaggistica istantanea

Fornisce funzioni di collaborazione in tempo reale per gli utenti e le applicazioni.

#### Servizi di configurazione

Gestisce la configurazione del prodotto compresa la gestione delle modifiche e dell'inventario.

#### Database

Fornisce il gestore database per i dati dell'applicazione e del sistema.

#### Directory

Fornisce la mappatura tra i nomi e valori. I servizi dati sono utilizzati come repository per i nomi utente e le password.

#### Gestione eventi

Raccoglie, aggregata, presenta e gestisce gli eventi di sistema.

#### Servizi di messaggistica

Fornisce i servizi di messaggi e di flusso di lavoro al prodotto.

#### Servizi di monitoraggio e agent

Fornisce le attività di monitoraggio all'interno del prodotto.

#### Portale

Fornisce i servizi che supportano l'interazione dell'utente con il prodotto.

#### Modello semantico

Fornisce servizi che consentono alle applicazioni di modellare oggetti e relazioni del mondo reale.

### Concetti correlati:

“Componenti” a pagina 5

Ad un livello elevato, la struttura di IBM Intelligent Operations Center può essere suddivisa in componenti principali, sottosistemi e servizi.

## Requisiti hardware di IBM Intelligent Operations Center

Per installare IBM Intelligent Operations Center sono necessari cinque server che soddisfino i requisiti minimi.

I server devono essere server x86 a 64 bit.

I server con i requisiti minimi utilizzati da IBM Intelligent Operations Center sono riportati in Tabella 2. Lo spazio su disco minimo consigliato non include lo spazio per le partizioni di avvio e swap.

Tabella 2. Requisiti hardware minimi

Risorsa	Server delle applicazioni	Server eventi	Server di dati	Server di gestione	Server di installazione
CPU	4	4	4	4	2
Memoria	24 GB	16 GB	16 GB	24 GB	4 GB
Adattatori di rete	1	1	1	1	1
Spazio su disco	113 GB	108 GB	108 GB	108 GB	108 GB
Spazio su disco aggiuntivo richiesto durante l'installazione	90 GB	90 GB	90 GB	90 GB	90 GB

I requisiti minimi per le directory su ciascun server, escludendo lo spazio richiesto per le partizioni di avvio e swap viene mostrato nella Tabella 3.

Tabella 3. Spazio minimo richiesto per ciascuna directory

Directory	Spazio minimo	Note
/	8 GB	
/opt	35 GB o 40 GB	Sono richiesti 40 GB per server delle applicazioni, 35 GB per tutti gli altri server
/usr	8 GB	
/home	5 GB	
/tmp	10 GB	
/chroot	1 GB	
/datahome	25 GB	
/loghome	8 GB	
/installMedia	90 GB	Questa directory può essere eliminata dopo l'installazione.
/var	8 GB	

#### Attività correlate:

“Preparazione dei server” a pagina 17

Prima di installare IBM Intelligent Operations Center, verificare che i requisiti di configurazione del server siano soddisfatti. Lo strumento di pre-verifica verifica che molti di tali requisiti siano stati implementati.

#### Informazioni correlate:

 [Requisiti di sistema](#)

## Requisiti software

Prima di installare IBM Intelligent Operations Center, i server devono avere installato il software appropriato.

IBM Intelligent Operations Center richiede l'installazione su tutti i server di Red Hat Enterprise Linux (RHEL) 5 Server x86-64 Update 5 o versioni successive. Red Hat Enterprise Linux Versione 6 non è supportato.

#### Attività correlate:

“Preparazione dei server” a pagina 17

Prima di installare IBM Intelligent Operations Center, verificare che i requisiti di configurazione del server siano soddisfatti. Lo strumento di pre-verifica verifica che molti di tali requisiti siano stati implementati.

#### Informazioni correlate:

 [Requisiti di sistema](#)

## Browser supportati

L'interfaccia delle soluzioni IBM Intelligent Operations Center supporta un certo numero di browser. Alcuni browser possono essere utilizzati con alcune limitazioni.

IBM Intelligent Operations Center è stato testato ed è supportato solo sui browser di seguito riportati:

- Microsoft Internet Explorer 8.x (solo a 32 bit)
- Microsoft Internet Explorer 9.x (solo a 32 bit)
- Mozilla Firefox 10 ESR

## Internet Explorer Compatibility View

IBM Intelligent Operations Center non supporta Internet Explorer 8 o Internet Explorer 9 Compatibility View.

**Nota:** View Compatibility può essere attivato temporaneamente; se si verifica un problema durante la creazione di una nuova pagina per l'interfaccia utente, vedere il link alla fine dell'argomento per dettagli.

## Prestazioni di Internet Explorer 8.x

Gli utenti potrebbero riscontrare prestazioni lente utilizzando Internet Explorer 8.x.

Per evitare questo problema, utilizzare Internet Explorer 9.x o Firefox 10 ESR.

## Risoluzione minima dello schermo

IBM Intelligent Operations Center è progettato per essere eseguito a una risoluzione minima dello schermo di 1280 x 800.

### Attività correlate:

“Impossibile creare una nuova pagina per l'interfaccia utente” a pagina 331

Risolvere un problema che si verifica durante la creazione di una nuova pagina se si utilizza Microsoft Internet Explorer 9.

## Packaging del supporto

IBM Intelligent Operations Center può essere ordinato come pacchetto di DVD o mediante Passport Advantage.

Il numero prodotto è 5725-D69.

### Informazioni correlate:

 [Passport Advantage](#)

 [Download dei file immagine di IBM Intelligent Operations Center Versione 1.5](#)

---

## Elenchi di controllo installazione

Gli elenchi di controllo installazione sono disponibili per le due diverse opzioni di installazione per IBM Intelligent Operations Center. Tali elenchi di controllo forniscono una panoramica delle fasi di installazione e possono essere utilizzati per tenere traccia dell'avanzamento dell'installazione.

### Elenco di controllo - installazione utilizzando IBM Installation Manager

Utilizzare questo elenco di controllo per tenere traccia dei passi di installazione durante l'installazione di IBM Intelligent Operations Center utilizzando IBM Installation Manager.

### Informazioni su questa attività

Una versione stampabile di questo elenco di controllo è disponibile utilizzando il link correlato alla fine di questo argomento.

### Procedura

- \_\_\_ 1. Verificare di disporre dell'hardware necessario.
- \_\_\_ 2. Verificare che sull'hardware sia installato il software richiesto.
- \_\_\_ 3. Preparare i server.
- \_\_\_ 4. Copiare il package di installazione sul server di installazione.
- \_\_\_ 5. Installare JRE (Java runtime environment).
- \_\_\_ 6. Installare IBM Installation Manager.
- \_\_\_ 7. Riavviare IBM Installation Manager ed installare il package **Configura topologia**.
- \_\_\_ 8. Riavviare IBM Installation Manager ed installare il package **Prepara server di destinazione**. Se questo passo viene completato correttamente, ignorare il passo 9.
- \_\_\_ 9. Riavviare IBM Installation Manager ed installare il package **Ignora errori di verifica del sistema**. Durante l'esecuzione di IBM Installation Manager una volta risolti gli errori di verifica del sistema oppure una volta determinato che l'installazione può continuare, selezionare **Prepara server di destinazione** e **Ignora errori di verifica del sistema** nella seconda esecuzione.
- \_\_\_ 10. Riavviare IBM Installation Manager ed installare il package **Prepara l'ambiente**.
- \_\_\_ 11. Riavviare IBM Installation Manager ed installare il package **Installa e configura la piattaforma - Parte 1**.



**Suggerimento:** Non selezionare contemporaneamente le parti 1 e 2. Queste operazioni sono quelle che richiedono il maggior intervallo di tempo per l'esecuzione. Se vengono eseguite insieme e si verifica un errore, sarà necessario eseguirle entrambe nuovamente, anche se una delle due ha avuto esito positivo.

**Importante:** Non arrestare i server tra le fasi di installazione. L'arresto dei server tra le fasi non è stata sottoposta a test e può portare a risultati imprevedibili.

- \_\_ 12. Riavviare IBM Installation Manager ed installare il package **Installa e configura la piattaforma - Parte 2**.
- \_\_ 13. Riavviare IBM Installation Manager ed installare il package **Installa lo strumento di controllo della piattaforma**.
- \_\_ 14. Riavviare IBM Installation Manager ed installare il package **Installa lo strumento Controllo di verifica del sistema**.
- \_\_ 15. Riavviare tutti i server di IBM Intelligent Operations Center.
  - a. Arrestare tutti i server IBM Intelligent Operations Center utilizzando lo Strumento di controllo della piattaforma.
  - b. Arrestare e riavviare tutti i server dal sistema operativo.
  - c. Arrestare tutti i server IBM Intelligent Operations Center utilizzando lo Strumento di controllo della piattaforma.
- \_\_ 16. Riavviare IBM Installation Manager ed installare il package **Installa applicazione**. In questo modo verrà installata l'applicazione IBM Intelligent Operations Center.
- \_\_ 17. Configurare l'architettura IBM Intelligent Operations Center.
  - \_\_ a. Configurare i servizi di collaborazione se si utilizza IPv6.
  - \_\_ b. Configurare SSO (single sign-on) per i servizi di collaborazione.
  - \_\_ c. Installare e configurare servizi di modelli semantici.
  - \_\_ d. Configurare lo Strumento di controllo della piattaforma.
  - \_\_ e. Codificare la password di gestione di Tivoli Service Request Manager.
  - \_\_ f. Imposta il numero minimo di thread per EventProcessor.
  - \_\_ g. Modificare la dimensione del pool di thread WebContainer e predefinito.
- \_\_ 18. Installare eventuali altre applicazioni.
- \_\_ 19. Riavviare IBM Installation Manager ed installare ed eseguire il package **Cyber Hygiene**. Cyber hygiene fornisce ulteriore sicurezza al sistema IBM Intelligent Operations Center.

**Nota:** Cyber Hygiene viene installato ed eseguito nello stesso passo.
- \_\_ 20. Configurare gli utenti che richiedono l'accesso ssh e password.

## Risultati

L'architettura IBM Intelligent Operations Center e l'applicazione IBM Intelligent Operations Center sono installate e pronte per l'utilizzo.

## Operazioni successive

Viene fornito uno strumento "must gather" per raccogliere i log di installazione per consentire di diagnosticare i problemi relativi all'installazione.

## Concetti correlati:

“Panoramica su cyber hygiene” a pagina 81

La funzione cyber hygiene di IBM Intelligent Operations Center è progettata per fornire servizi che pongano rimedio a potenziali rischi nella sicurezza nel sistema installato.

## Informazioni correlate:



Versione stampabile di questo elenco di controllo

## Elenco di controllo - installazione dettagliata

Utilizzare questo elenco di controllo per tenere traccia dei passi di installazione durante l'installazione di IBM Intelligent Operations Center utilizzando script e comandi.

## Informazioni su questa attività

Una versione stampabile di questo elenco di controllo è disponibile utilizzando il relativo collegamento alla fine di questo argomento.

## Procedura

- \_\_\_ 1. Assicurarsi di disporre dell'hardware necessario.
- \_\_\_ 2. Assicurarsi che il software richiesto sia installato sull'hardware.
- \_\_\_ 3. Preparare i server.
- \_\_\_ 4. Installare l'ambiente runtime Java.
- \_\_\_ 5. Copiare il package di installazione sul server di installazione.
- \_\_\_ 6. Decomprimere e preparare il package di installazione.
- \_\_\_ 7. Definire le proprietà di installazione.
- \_\_\_ 8. Definire la topologia per l'installazione modificando il file delle proprietà della topologia.
- \_\_\_ 9. Generare la password della topologia che verrà utilizzata per codificare i file delle chiavi.
- \_\_\_ 10. Generare il file della topologia.
- \_\_\_ 11. Eseguire lo strumento di pre-verifica per controllare che l'ambiente sia pronto per installare IBM Intelligent Operations Center.
- \_\_\_ 12. Configurare le impostazioni di sicurezza Linux utilizzando lo strumento fornito o eseguendo una serie di comandi.
- \_\_\_ 13. Installare l'architettura IBM Intelligent Operations Center. Ciò può essere effettuato in una fase o in tre fasi. Se si opera in un ambiente virtualizzato, l'installazione in più fasi consente di creare un'istantanea tra le fasi di installazione.
  - Installare IBM Intelligent Operations Center in una fase. L'installazione impiegherà fino a 14 ore.
  - Installare IBM Intelligent Operations Center in tre fasi. Le tre fasi sono:
    - a. Copiare i file di installazione da server di installazione ai server di destinazione. Questa fase impiega circa 2 ore.
    - b. Installare la prima fase della topologia. Questa fase impiega circa 9 ore.
    - c. Installare la seconda fase della topologia. Questa fase impiega circa 3 ore.
- \_\_\_ 14. Installare Strumento di controllo della piattaforma.
- \_\_\_ 15. Installare lo strumento Controllo di verifica del sistema.
- \_\_\_ 16. Verificare che l'architettura IBM Intelligent Operations Center sia correttamente installata.
- \_\_\_ 17. Configurare l'architettura IBM Intelligent Operations Center.

**Importante:** Non arrestare i server tra le fasi di installazione. L'arresto dei server tra le fasi non è stata sottoposta a test e può portare a risultati imprevedibili.

- \_\_ a. Configurare i servizi di collaborazione se si sta utilizzando IPv6.
  - \_\_ b. Configurare SSO (single sign-on) per i servizi di collaborazione.
  - \_\_ c. Installare e configurare servizi di modelli semantici.
  - \_\_ d. Codificare la password di gestione Tivoli Service Request Manager.
  - \_\_ e. Impostare il numero minimo di thread per EventProcessor.
  - \_\_ f. Modificare la dimensione del pool di thread Default e WebContainer.
- \_\_ 18. Installare l'applicazione IBM Intelligent Operations Center.
- \_\_ 19. Installare eventuali altre applicazioni.
- \_\_ 20. Installare ed eseguire cyber hygiene. Cyber hygiene fornisce una sicurezza aggiuntiva al sistema IBM Intelligent Operations Center.
- Nota:** Cyber hygiene viene installato ed eseguito nello stesso passo.
- \_\_ 21. Configurare gli utenti che richiedono l'accesso ssh e password.

## Risultati

L'architettura IBM Intelligent Operations Center e l'applicazione IBM Intelligent Operations Center sono installate e pronte per l'utilizzo.

## Operazioni successive

Lo strumento must gather viene fornito per raccogliere i log di installazione per consentire di diagnosticare i problemi di installazione.

### Concetti correlati:

“Panoramica su cyber hygiene” a pagina 81

La funzione cyber hygiene di IBM Intelligent Operations Center è progettata per fornire servizi che pongano rimedio a potenziali rischi nella sicurezza nel sistema installato.

### Informazioni correlate:



Versione stampabile di questo elenco di controllo

---

## Preparazione dei server

Prima di installare IBM Intelligent Operations Center, verificare che i requisiti di configurazione del server siano soddisfatti. Lo strumento di pre-verifica verifica che molti di tali requisiti siano stati implementati.

## Informazioni su questa attività

Se in esecuzione in un sistema virtuale, l'utilizzo di un template per tali passi può consentire di ridurre il tempo necessario per l'impostazione.

## Procedura

1. Verificare che i server soddisfino i requisiti hardware e software.
2. Impostare la connessione di rete TCP/IP.
  - a. Definire un nome completo ed un nome host breve utilizzando un server DNS oppure mediante la definizione nel file `/etc/hosts`.
  - b. Verificare la configurazione TCP/IP. I server sono configurati correttamente se le verifiche riportate di seguito vengono completate con esito positivo.
    - 1) Il comando `hostname -s` restituisce il nome host breve definito per il server.
    - 2) Il comando `hostname -f` restituisce il nome host e il dominio completo per il server.

- 3) I risultati di un comando **ping** o di un comando **ping6** per ambienti IPV6, con il nome host breve per ciascun server, indica che il server è accessibile.
  - 4) I risultati di un comando **ping** o di un comando **ping6** per ambienti IPV6, con il nome completo per ciascun server, indica che il server è accessibile.
- c. Abilitare l'indirizzamento di loopback locale per ciascun server nel file `/etc/hosts`.
- d. Verificare l'indirizzamento loopback locale. I server sono configurati correttamente se le verifiche riportate di seguito vengono completate con esito positivo.
- 1) Il comando **ping -n localhost** restituisce l'indirizzo `127.0.0.1`.
  - 2) Il comando **ping -n localhost.localdomain** restituisce l'indirizzo `127.0.0.1`.
  - 3) Il comando **ping6 -n localhost6** in un ambiente IPV6 restituisce l'indirizzo `::1`.
  - 4) Il comando **ping6 -n localhost6.localdomain6** in un ambiente IPV6 restituisce l'indirizzo `::1`.
- e. Verificare che le porte richieste da IBM Intelligent Operations Center siano disponibili. Le porte richieste per ciascun server sono illustrate nella Tabella 4.

Tabella 4. Porte richieste per l'utilizzo del prodotto

Server	Porte richieste per l'utilizzo del prodotto
Applicazione	80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Eventi	80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Dati	389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008
Management	80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001

- f. Verificare che il numero massimo di descrittori file definito dal parametro **nofile** nel file `/etc/security/limits.conf` sia impostato su 20480 per i seguenti server:

- Server delle applicazioni
- Server eventi
- Server di dati
- Server di gestione

Ciò viene effettuato aggiungendo le seguenti righe al file `/etc/security/limits.conf`:

```
* soft nofile 20480
* hard nofile 20480
```

Ciò imposterà il limite soft (predefinito) del numero di file aperti per tutti gli utenti a 20480, ed imposterà anche il limite hard (massimo) per tutti gli utenti a 20480. È possibile che si desideri aumentare il limite hard se altre applicazioni richiedono più di 20480 file.

- g. Aggiungere o aggiornare il parametro **net.ipv4.tcp\_fin\_timeout** nel file `/etc/sysctl.conf` su 30 per i seguenti server:
  - Server delle applicazioni
  - Server eventi
  - Server di dati
  - Server di gestione
3. Disabilitare tutti i firewall Linux.
4. Disabilitare SELinux (Security Enforcing Linux) modificando il file `/etc/selinux/config` ed impostando SELINUX su `disabled`. Una volta modificata la configurazione, riavviare il server.
5. Verificare che su tutti i server sia impostata la stessa data ed ora indicate dal sistema operativo Linux. È possibile utilizzare un servizio di sincronizzazione dell'ora.
6. Abilitare il servizio `sshd` su ciascun server eseguendo il comando `/etc/init.d/sshd start`. Il servizio deve essere abilitato per l'accesso root con autenticazione della password. È necessario configurare la porta TCP/IP 22 nel sistema operativo come porta di accesso ssh disponibile da utilizzare durante l'installazione. Il numero di porta TCP/IP per l'accesso ssh del Strumento di controllo della piattaforma è specificato nel file delle proprietà della topologia. Solo il Strumento di controllo della piattaforma utilizza la porta configurata.
7. Installare i package Linux packages in Tabella 5 su ciascun server utilizzando il comando `yum install package_name`. Tali package sono disponibili da Red Hat.

Tabella 5. Package Linux richiesti e facoltativi per i server di destinazione IBM Intelligent Operations Center

Package	Server delle applicazioni	Server di dati	Server eventi	Server di gestione
compat-libstdc++-33-3*	richiesto	richiesto	richiesto	richiesto
libXp-1.0.0-8*	richiesto	facoltativo	richiesto	richiesto
libXmu-1*	richiesto	facoltativo	richiesto	richiesto
libXtst-1*	richiesto	facoltativo	richiesto	richiesto
pam-0*	richiesto	facoltativo	facoltativo	facoltativo
rpm-build-4*	richiesto	facoltativo	facoltativo	richiesto
libaio-0*	richiesto	richiesto	facoltativo	richiesto
libstdc++-4*	richiesto	richiesto	richiesto	richiesto
libXft-2*	richiesto	facoltativo	facoltativo	richiesto
compat-db-4*	richiesto	facoltativo	facoltativo	richiesto
elfutils-libs-0*	richiesto	facoltativo	facoltativo	richiesto
elfutils-0*	richiesto	facoltativo	facoltativo	richiesto
libgcc-4*	richiesto	facoltativo	richiesto	facoltativo
compat-glibc-2*	richiesto	facoltativo	richiesto	facoltativo
openmotif22-2*	richiesto	facoltativo	richiesto	facoltativo
audit-libs-1*	richiesto	facoltativo	facoltativo	facoltativo
glibc-2*	richiesto	facoltativo	facoltativo	facoltativo
glibc-common-2*	richiesto	facoltativo	facoltativo	facoltativo
glibc-headers-2*	facoltativo	richiesto	facoltativo	richiesto
glibc-devel-2*	facoltativo	richiesto	facoltativo	richiesto

Tabella 5. Package Linux richiesti e facoltativi per i server di destinazione IBM Intelligent Operations Center (Continua)

Package	Server delle applicazioni	Server di dati	Server eventi	Server di gestione
compat-gcc*	facoltativo	richiesto	facoltativo	richiesto
libXft-2*	facoltativo	facoltativo	richiesto	facoltativo
libXpm-3*	facoltativo	facoltativo	richiesto	facoltativo
xorg-x11-xauth*	facoltativo	facoltativo	richiesto	facoltativo
ksh-*	facoltativo	facoltativo	facoltativo	richiesto

È possibile utilizzare i seguenti comandi per installare i package richiesti su ciascun server. Se il package è già installato, non verrà installato nuovamente.

**Server delle applicazioni**

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0* rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2* glibc-common-2*
```

**Server di dati**

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2* glibc-devel-2* compat-gcc*
```

**Server eventi**

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4* libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

**Server di gestione**

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0* glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Assicurarsi che Java 1.6 non sia installato su nessun server:

- Server di installazione
- Server delle applicazioni
- Server eventi
- Server di dati
- Server di gestione

**Concetti correlati:**

“Requisiti software” a pagina 13

Prima di installare IBM Intelligent Operations Center, i server devono avere installato il software appropriato.

“Requisiti hardware di IBM Intelligent Operations Center” a pagina 12

Per installare IBM Intelligent Operations Center sono necessari cinque server che soddisfino i requisiti minimi.

**Attività correlate:**

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager” a pagina 26

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

**Informazioni correlate:**

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

## Connessione di rete TCP/IP

Prima di installare IBM Intelligent Operations Center, la connessione di rete TCP/IP tra i server deve essere configurata correttamente.

Tutti i server, incluso server di installazione, utilizzato da IBM Intelligent Operations Center devono essere configurati con un nome host breve e un nome host completo. I nomi host devono essere risolti nell'indirizzo IP corretto su ciascun server. La configurazione può essere effettuata utilizzando un server DNS o aggiungendo definizioni al file `/etc/hosts`.

Il nome host completo per ciascun server deve avere almeno tre componenti. Ad esempio: `myhost.mydomain.com`, dove il dominio è un dominio di primo livello standard di Internet.

**Importante:** I nomi host brevi e i nomi host completi devono essere specificati nel caso corretto. Ad esempio, `MyCompany.MyDomain.com` non può essere specificato come `mycompany.mydomain.com`.

La connessione di rete IPv6 è supportata da IBM Intelligent Operations Center, ma anche IPv4 deve essere installato e configurato. Gli indirizzi IPv4 non devono essere assegnati ai server, ma l'indirizzo di loopback IPv4 (`127.0.0.1`) deve essere abilitato e il nome host `localhost` deve essere risolto in `127.0.0.1`.

Le modifiche alla configurazione vengono mostrate in Tabella 6 a pagina 22. Queste sono le linee guida per l'impostazione della connessione di rete TCP/IP su IBM Intelligent Operations Center server di installazione e sui server di destinazione modificando i file di configurazione di rete Linux. Le note di configurazione in Tabella 6 a pagina 22 sono solo linee guida. Qualsiasi configurazione di rete conforme ai requisiti descritti in precedenza sono funzionanti.

Tabella 6. Linee guida di configurazione TCP/IP

File	Note
/etc/hosts	<p>Il file hosts risolve i nomi TCP/IP in indirizzi IP. Se la configurazione non ha un server DNS, tutti i server e relativi indirizzi IP, nomi host brevi e nomi completi devono essere definiti in questo file. Gli indirizzi loopback locali e i nomi host sono anche definiti in questo file.</p> <p>Se si sta utilizzando un server DNS, gli host che vengono risolti dal DNS non devono essere inclusi in questo file.</p> <p><b>Importante:</b> Quando si utilizza IPv4, l'indirizzo loopback locale 127.0.0.1 deve essere associato ai nomi host localhost e localhost.localdomain.</p> <p>Di seguito viene riportato un file di esempio /etc/hosts utilizzando indirizzi IPv4.</p> <pre># local loopback definitions -- do not remove # or alter these! 127.0.0.1 localhost.localdomain localhost # use the following if IPv6 is enabled in your # network definitions ::1 localhost6.localdomain localhost6  # installation server 192.168.0.205 IOC15Install.IOC15.com IOC15Install  # target runtime servers 192.168.0.211 IOC15App.IOC15.com IOC15App 192.168.0.212 IOC15Event.IOC15.com IOC15Event 192.168.0.213 IOC15DB.IOC15.com IOC15DB 192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt</pre> <p>Utilizzare la notazione indirizzi IPv6 per assegnare indirizzi statici IPv6.</p> <p>Sia gli indirizzi IPv6 che quelli IPv4 possono essere definiti sullo stesso server.</p>



Tabella 6. Linee guida di configurazione TCP/IP (Continua)

File	Note
<p>/etc/sysconfig/network-scripts/ifcfg-<i>nome_adattatore</i></p>	<p>Il file <i>ifcfg-<i>nome_adattatore</i></i> definisce le impostazioni di rete base per l'adattatore di rete specificato. Il nome assegnato Linux per l'adattatore di rete è specificato da <i>nome_adattatore</i>. Il valore tipico per <i>nome_adattatore</i> è <i>eth0</i> ma potrebbe essere differente per il proprio ambiente.</p> <p>Per la connessione di rete IPv4 è necessario definire i seguenti parametri.</p> <p><b>IPADDR</b> Specificare l'indirizzo IP IPv4 del server che si sta configurando.</p> <p><b>NETMASK</b> Specificare la maschera di rete IPv4 del server che si sta configurando.</p> <p><b>GATEWAY</b> Specificare l'indirizzo IP della rete predefinita IPv4 del server che si sta configurando.</p> <p><b>BOOTPROTO</b> Se si sta utilizzando un'assegnazione di indirizzi IP statici, specificare none.</p> <p><b>NM_CONTROLLED</b> Specificare no per disabilitare il servizio Network Management modificando il file <i>ifcfg-<i>nome_adattatore</i></i>.</p> <p><b>ONBOOT</b> Specificare yes per avviare automaticamente l'adattatore.</p> <p><b>IPV6INIT</b> Specificare yes se l'adattatore deve utilizzare la connessione di rete IPv6.</p> <p><b>IPV6ADDR</b> Specificare l'indirizzo IP IPv6 se IPV6INIT=yes è specificato.</p> <p><b>IPV6_DEFAULTGW</b> Specificare l'indirizzo IP del gateway di rete predefinita IPv6 del server se IPV6INIT=yes è specificato.</p>
<p>/etc/sysconfig/network</p>	<p>Il file <i>network</i> specifica i parametri di rete generali.</p> <p>Per la connessione di rete IPv4, è necessario definire i seguenti parametri:</p> <p><b>NETWORKING</b> Specificare yes per abilitare la connessione di rete IPv4.</p> <p><b>NETWORKING_IPV6</b> Specificare yes se si desidera anche la connessione di rete IPv6.</p> <p><b>HOSTNAME</b> Specificare il nome host breve del server.</p>

Tabella 6. Linee guida di configurazione TCP/IP (Continua)

File	Note
/etc/resolv.conf	<p>Il file <code>resolv.conf</code> viene utilizzato per definire i server DNS per la rete e un dominio di ricerca predefinito. Se i server DNS non vengono utilizzati, questo file deve essere vuoto.</p> <p>Se si utilizza un server DNS, il file <code>resolv.conf</code> deve contenere le seguenti righe:</p> <pre>search nome_dominio nameserver primo_server_DNS nameserver secondo_server_DNS</pre> <p>Ad esempio:</p> <pre>search yourcompany.com nameserver 10.75.20.10 nameserver 10.75.20.11</pre> <p>Il valore <code>search</code> specifica il dominio di ricerca predefinito. Il primo valore <code>nameserver</code> è l'indirizzo IP del server DNS. Un secondo valore <code>nameserver</code> può essere utilizzato per specificare un server DNS secondario. La seconda specifica <code>nameserver</code> è facoltativa.</p>
/etc/modprobe.conf	<p>Il file <code>modprobe.conf</code> definisce le opzioni di configurazione per i moduli caricati nel sistema.</p> <p>La connessione di rete IPv6 potrebbe richiedere la disabilitazione mediante commento delle seguenti righe e il riavvio del server:</p> <pre>alias ipv6 off options ipv6 disable=1</pre>

Se configurato correttamente, ogni server deve superare correttamente i seguenti test:

1. Il comando **hostname -s** restituisce il nome host breve definito per il server.
2. Il comando **hostname -f** restituisce il nome host e il dominio completo per il server.
3. I risultati di un comando **ping** o di un comando **ping6** per ambienti IPV6, con il nome host breve per ciascun server, indica che il server è accessibile.
4. I risultati di un comando **ping** o di un comando **ping6** per ambienti IPV6, con il nome completo per ciascun server, indica che il server è accessibile.

### Attività correlate:

“Preparazione dei server” a pagina 17

Prima di installare IBM Intelligent Operations Center, verificare che i requisiti di configurazione del server siano soddisfatti. Lo strumento di pre-verifica verifica che molti di tali requisiti siano stati implementati.

“La rete IPv6 non viene avviata” a pagina 330

Se su un server non viene avviata la rete IPv6, è possibile che sia necessario apportare delle modifiche al file `/etc/modprobe.conf`.

“Esecuzione dello strumento di pre-verifica” a pagina 43

Prima di caricare i package di installazione sui server di destinazione, verificare che i server di destinazione siano pronti per l'installazione eseguendo lo strumento di pre-verifica.

---

## Copia del package di installazione in server di installazione

Copiare il package di installazione di IBM Intelligent Operations Center in server di installazione prima di installare il prodotto.

### Prima di iniziare

Prima di copiare il package di installazione in server di installazione, assicurarsi che tutti i server siano stati adeguatamente preparati.

### Procedura

1. Creare una directory in server di installazione per i file di installazione, ad esempio `/installHome`.
2. Prendere nota del percorso completo della directory creata. Ad esempio, se la directory creata è `installHome` per l'utente `ibmadmin`, il percorso completo sarebbe `/home/ibmadmin/installHome`. Questo percorso di directory viene indicato come `install_home` in altre istruzioni di installazione.
3. Per ogni DVD fisico o immagine ISO scaricata da Passport Advantage, eseguire quanto indicato di seguito.
  - a. Creare una directory per montare il DVD. Ad esempio, eseguire il comando `mkdir /mnt/ba15`.
  - b. Montare il DVD. Ad esempio, quando si utilizza un'immagine ISO, eseguire il comando `mount loop -o ISO_directory/ISO_filename /mnt/ba15` dove `ISO_directory` è l'ubicazione dell'immagine ISO e `ISO_filename` è il file ISO.
  - c. Copiare il contenuto del DVD nella directory creata nel passo 1. Ad esempio, quando si utilizza un'immagine ISO, eseguire il comando `cp /mnt/ba15/* install_home`.
  - d. Smontare il DVD. Ad esempio, quando si utilizza un'immagine ISO, eseguire il comando `umount /mnt/ba15`.
4. Passare alla directory `install_home`.
5. Eseguire il comando `ba15_media_prep.sh combine`. Questo comando deve essere eseguito prima di eseguire qualsiasi altra procedura di installazione.

**Nota:** Se la directory `install_home` è diversa da `/installMedia`, modificare il file `ba15_media_prep.sh` e modificare il valore `MEDIA_BASE` con la directory `install_home` definita prima di eseguire lo script. Questo comando unisce i file che sono suddivisi nei DVD o nelle immagini ISO.

### Concetti correlati:

“Ubicazione del supporto di installazione” a pagina 31

IBM Installation Manager consente al programma di installazione di specificare dove sono situati i package di installazione durante l'installazione di IBM Intelligent Operations Center.

### Attività correlate:

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager”

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

“Installazione di JRE (Java runtime environment)”

L'ambiente runtime Java 6 deve essere installato sul server di installazione prima di installare IBM Intelligent Operations Center.

---

## Installazione di JRE (Java runtime environment)

L'ambiente runtime Java 6 deve essere installato sul server di installazione prima di installare IBM Intelligent Operations Center.

### Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Collegarsi come root oppure passare all'account root eseguendo il comando **su -**.
2. Passare alla directory in cui sono stati copiati i file di installazione di IBM Intelligent Operations Center.
3. Eseguire il comando **yum --nogpgcheck install install\_media/ibm-java-x86\_64-jre-6.0-10.1.x86\_64.rpm**.
4. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
5. Verificare l'ambiente Java eseguendo il comando **echo \$JAVA\_HOME** e confermando che venga restituito `/opt/ibm/java-x86_64-60/jre`.

### Attività correlate:

“Copia del package di installazione in server di installazione” a pagina 25

Copiare il package di installazione di IBM Intelligent Operations Center in server di installazione prima di installare il prodotto.

“Configurazione di Strumento di controllo della piattaforma” a pagina 60

Dopo l'installazione di IBM Intelligent Operations Center, se è stato installato un Java™ JRE diverso da quello fornito con IBM Intelligent Operations Center, è necessario definire l'ubicazione JRE utilizzata da Strumento di controllo della piattaforma.

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager”

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

---

## Installazione di IBM Intelligent Operations Center utilizzando Installation Manager

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

## Prima di iniziare

Il package del prodotto deve essere copiato in server di installazione, nella directory *install-home* prima di eseguire le seguenti operazioni.

## Informazioni su questa attività

Un indicatore di avanzamento viene visualizzato durante l'installazione. Tuttavia, poiché le attività di installazione vengono eseguite in remoto sui server di destinazione, l'indicatore di avanzamento non indica il tempo vero rimanente per l'installazione. "Componenti dell'installazione" a pagina 30 fornisce il tempo stimato di installazione per ciascun componente.

Se si desidera annullare l'installazione in qualsiasi momento, fare clic su **Annulla** nell'interfaccia utente di IBM Installation Manager.

**Importante:** Non eseguire il comando **launchpad.sh** dopo il primo componente viene installato correttamente. Non verrà fornita l'opzione per modificare l'installazione. Utilizzare il comando **/opt/IBM/InstallationManager/eclipse/IBMIM** per riavviare il programma di installazione anziché eseguire quanto indicato nell'operazione 24 a pagina 28.

## Procedura

1. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
2. Estrarre il **BA\_1.5\_GUI\_Installer\_Lite\_Launchpad.zip** in *install\_home*.
3. Avviare il launchpad di installazione eseguendo il comando *install\_home/launchpad.sh*.
4. Installare IBM Installation Manager.
  - a. Fare clic su **Installa IBM Installation Manager**.
  - b. Fare clic su **Avanti**.
  - c. Leggere le informazioni sulla licenza.
  - d. Se si accettano i termini di licenza, selezionare **Accetto i termini dell'accordo di licenza** e fare clic su **Avanti**. L'installazione continuerà.
  - e. Se non si accettano i termini di licenza, selezionare **Non accetto i termini dell'accordo di licenza** e fare clic su **Avanti**. L'installazione terminerà.
  - f. Selezionare dove IBM Installation Manager verrà installato.
  - g. Fare clic su **Avanti**.
  - h. Fare clic su **Installa**.
  - i. Riavviare IBM Installation Manager.

IBM Installation Manager viene installato.

5. Una volta che IBM Installation Manager è installato, IBM Installation Manager deve essere chiuso e riavviato. L'avvio di IBM Installation Manager dal launchpad, preleverà il file della topologia di IBM Intelligent Operations Center.
6. Fare clic su **Install IBM Intelligent Operations Center**.
7. Selezionare il package **IBM Intelligent Operations Center - Versione 1.5**.
8. Fare clic su **Avanti**.
9. Leggere le informazioni sulla licenza.
  - a. Se si accettano i termini di licenza, selezionare **Accetto i termini dell'accordo di licenza** e fare clic su **Avanti**. L'installazione continuerà.
  - b. Se non si accettano i termini di licenza, selezionare **Non accetto i termini dell'accordo di licenza** e fare clic su **Avanti**. L'installazione terminerà.

10. Specificare la Directory risorse condivise per l'installazione. Questa directory verrà utilizzata ogni volta che si utilizza IBM Installation Manager per installare i prodotti utilizzando server di installazione. Assicurarsi di specificare un'unità con il maggior spazio disponibile sul server.
11. Fare clic su **Avanti**.
12. Creare un nuovo gruppo di package selezionando crea un nuovo gruppo di package. Selezionare IBM Intelligent Operations Center.
13. Specificare il nome della Directory di installazione. La Directory di installazione verrà creata. Il programma di installazione creerà le sottodirectory in questa directory, in base alle esigenze.
14. Per selezione architettura, selezionare 64 bit.
15. Fare clic su **Avanti**.
16. Deselezionare tutte le opzioni.
17. Selezionare **Configura topologia**.
18. Fare clic su **Avanti**.
19. Immettere le opzioni di configurazione. Prendere nota di qualsiasi password definita.
20. Fare clic su **Avanti**.
21. Rivedere le opzioni di installazione e fare clic su **Avanti** per avviare l'installazione.
22. Una volta completata l'installazione, chiudere IBM Installation Manager e il launchpad. Non chiudere la finestra di terminale in cui è stato avviato il launchpad nell'operazione 3 a pagina 27 poiché ha un ambiente JAVA\_HOME impostato. Se la finestra di terminale è chiusa, JAVA\_HOME deve essere esportato di nuovo prima di continuare.
23. Se il valore immesso per la password della topologia supera la lunghezza di 15 caratteri, eseguire le seguenti operazioni per definire una password per ITM.ADMIN.USER.PWD che ha una lunghezza pari o inferiore a 15 caratteri.
  - a. In server di installazione modificare il file *install\_home/ioc/topology/iop\_lite\_topo.properties* dove *install\_home* è la directory in cui il package di installazione di IBM Intelligent Operations Center.
  - b. Modificare il valore definito per ITM.ADMIN.USER.PWD con un valore di 15 caratteri o inferiore. Questa password verrà utilizzata durante la registrazione nell'utente sysadmin utente, anziché la password della topologia.
  - c. Salvare le modifiche.
24. Avviare IBM Installation Manager eseguendo il comando **/opt/IBM/InstallationManager/eclipse/IBMIM**.
25. Fare clic su **Modifica > Avanti**.
26. Selezionare **Prepara server di destinazione**.
27. Fare clic su **Avanti > Modifica**.
28. Se ci sono errori, esaminare i file di log nella directory */var/ibm/InstallationManager/logs/native*. I nomi dei file di log iniziano con data/ora che può essere utilizzato per correlare il log al momento in cui lo strumento di installazione è stato eseguito.
29. Correggere gli errori o avvertenze rilevati nei log riguardanti il sistema e completare l'installazione prima di installare il componente successivo. Alcune avvertenze ed errori possono essere ignorati. Ad esempio, le avvertenze relative a IPv6 se non si ha IPv6 abilitato o se la configurazione non è connessa a un DNS (Domain Name Service).
30. Dopo aver corretto eventuali errori, tornare all'operazione 25. Sarà disponibile l'opzione per ignorare gli errori di verifica del sistema. Selezionare il componente successivo nell'elenco dell'operazione 26. Continuare il processo finché cyber hygiene non verrà installato.

**Importante:** Non arrestare i server tra le fasi di installazione. L'arresto dei server tra le fasi non è stata sottoposta a test e può portare a risultati imprevedibili.

Cyber Hygiene applica le configurazioni delle migliori prassi per fornire ulteriore sicurezza al sistema IBM Intelligent Operations Center. Prima di installare cyber hygiene, completare la

configurazione di post-installazione. Una volta completata la configurazione di post-installazione, ritornare al passo 24 a pagina 28 e installare ed eseguire cyber hygiene. I componenti installati correttamente quando IBM Installation Manager è stato precedentemente eseguito, vengono controllati. Non deselezionare queste componenti o i componenti verranno disinstallati quando IBM Installation Manager viene eseguito di nuovo.

Se in esecuzione in un ambiente virtualizzato, eseguire un'istantanea con memoria di tutti i server dopo un'operazione di installazione completata correttamente e prima di installare il componente successivo. Questa istantanea può essere utilizzata per riavviare l'installazione in uno stato corretto, in caso di errore.

Per ridurre il tempo in cui cyber hygiene esegue le scansioni e riparazioni, smontare qualsiasi file system che non deve essere valutato per la sicurezza. Ad esempio, le directory *install\_media* in ciascun server possono essere eliminate dopo che tutte le operazioni di installazione sono state completate. Queste directory possono essere eliminate o smontate prima di eseguire cyber hygiene.

**Nota:** Cyber hygiene viene installato ed eseguito nella stessa fase.

Cyber hygiene deve essere l'ultimo passo prima di spostare il sistema allo stato di produzione o quando il sistema deve affrontare le buone pratiche di sicurezza. Tutte le applicazioni e le soluzioni devono essere installate e configurate prima di eseguire cyber hygiene, in modo che il sistema finale possa essere sottoposto a scansione e le soluzioni possano essere applicate.

Le modifiche applicate al sistema da cyber hygiene possono causare problemi con altre applicazioni e soluzioni. Ad esempio, le altre applicazioni e soluzioni potrebbero avere requisiti sull'ambiente Linux che non sono in sintonia con le buone pratiche sulla sicurezza. Un'applicazione o soluzione potrebbe richiedere l'accesso al sistema come utente root per essere installato o eseguito. In questo caso alcune delle modifiche cyber hygiene potrebbe essere temporaneamente o permanentemente cambiate o un'altra soluzione trovata dal fornitore dell'applicazione o soluzione.

Una volta che le modifiche a cyber hygiene vengono apportate, non vi è alcun metodo automatizzato per modificarle. Tutte le modifiche devono essere apportate tramite aggiornamenti manuali al sistema operativo Linux o modificando le autorizzazioni del file o della directory.



### Concetti correlati:

“Rimozione dei servizi di installazione dal sistema di produzione” a pagina 68

Dopo l'installazione di IBM Intelligent Operations Center i servizi di installazione possono essere rimossi dai server del sistema di produzione. E' preferibile non cancellare il server di installazione poiché alcuni suoi servizi potrebbero essere richiesti per le attività di manutenzione.

“Configurazione post-installazione di IBM Intelligent Operations Center” a pagina 53

Dopo l'installazione dell'architettura IBM Intelligent Operations Center utilizzando Installation Manager o la procedura guidata, è necessario eseguire diverse operazioni di configurazione post-installazione per completare l'installazione.

“Panoramica su cyber hygiene” a pagina 81

La funzione cyber hygiene di IBM Intelligent Operations Center è progettata per fornire servizi che pongano rimedio a potenziali rischi nella sicurezza nel sistema installato.

### Attività correlate:

“Preparazione dei server” a pagina 17

Prima di installare IBM Intelligent Operations Center, verificare che i requisiti di configurazione del server siano soddisfatti. Lo strumento di pre-verifica verifica che molti di tali requisiti siano stati implementati.

“Verifica dell'installazione” a pagina 52

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

“Copia del package di installazione in server di installazione” a pagina 25

Copiare il package di installazione di IBM Intelligent Operations Center in server di installazione prima di installare il prodotto.

“Installazione di JRE (Java runtime environment)” a pagina 26

L'ambiente runtime Java 6 deve essere installato sul server di installazione prima di installare IBM Intelligent Operations Center.

## Componenti dell'installazione

IBM Intelligent Operations Center viene installato con sette componenti.

Tabella 7. Componenti dell'installazione di IBM Intelligent Operations Center

Componente	Tempo di installazione stimato	Cosa viene installato
Prepara l'installazione	Pre-verifica: 10 minuti Caricamento: 2 ore	Viene verificato se l'ambiente del server soddisfa i requisiti minimi e vengono copiati sui server di destinazione i file richiesti per l'installazione.
Prepara l'ambiente	10 minuti	Aggiorna i file /etc/sudoers e ~/.ssh/known_hosts in base alle necessità di IBM Intelligent Operations Center
Installa e configura la piattaforma	Fase 1: 12 ore Fase 2: 3 ore	La piattaforma richiesta viene installata sui server di destinazione. L'installazione viene effettuata in fasi.
Strumento di controllo della piattaforma	10 minuti	Vengono installati sul server di gestione gli strumenti richiesti per avviare e arrestare i server IBM Intelligent Operations Center ed eseguire query di stato.
Controllo di verifica del sistema della piattaforma	15 minuti	Strumenti utilizzati per determinare se le funzionalità fondamentali della piattaforma sono installate sul server delle applicazioni.
Applicazione	3 ore	L'applicazione IBM Intelligent Operations Center viene installata sui server di destinazione.



Tabella 7. Componenti dell'installazione di IBM Intelligent Operations Center (Continua)

Componente	Tempo di installazione stimato	Cosa viene installato
Cyber Hygiene	Fino a 1.5 ore	Sui server di destinazione vengono installate funzionalità per la riduzione e la soluzione di vulnerabilità note della sicurezza Cyber. Il tempo di elaborazione è determinato dalla velocità dell'hardware e dalla presenza sui server di destinazione di file supplementari non necessari.

## Opzioni di configurazione

IBM Installation Manager consente al programma di installazione di specificare le opzioni di configurazione durante l'installazione di IBM Intelligent Operations Center.

### Password della topologia

IBM Installation Manager consente al programma di installazione di specificare le password da utilizzare con IBM Intelligent Operations Center.

Il programma di installazione può specificare le password mostrate nella Tabella 8.

Tabella 8. Password di IBM Intelligent Operations Center

Password	Descrizione
Password della topologia	<p>La password della topologia è la password utilizzata per tutti gli account creati dal programma di installazione di IBM Intelligent Operations Center fatta eccezione per le password richieste specificatamente durante il processo di installazione e la password di <code>iicsystemuser</code> che è definita come <code>passwd</code> e non può essere modificata. La password della topologia protegge inoltre la chiave segreta creata dal comando <code>createSecretKey</code>.</p> <p>La password di un account non può superare i 15 caratteri. Se la password della topologia supera la lunghezza di 15 caratteri, è necessario effettuare alcune operazioni speciali di configurazione per ridefinire la password per l'account.</p>
Password dell'utente admin	La password di amministratore impostata per l'utente Linux <code>ibmadmin</code> . Questo viene utilizzato da Strumento di controllo della piattaforma durante la gestione dei componenti dei server di destinazione.
Valore seed di codifica	<p>Il valore seed di codifica viene utilizzato per codificare le password utente ed altri dati sensibili all'interno del database. Il seed di codifica deve essere un valore di carattere ASCII stampabile compreso tra 12 e 1016.</p> <p>Deve essere utilizzata una stringa sicura. Ad esempio, una stringa lunga che comprende lettere minuscole e maiuscole, numeri e caratteri speciali senza parole o frasi comuni.</p>
Salt della codifica	Il valore salt di codifica viene utilizzato per codificare le password utente ed altri dati sensibili all'interno del database. Il salt di codifica deve essere un valore di carattere ASCII 12 stampabile compreso tra i punti di codice 33 e 126.

### Ubicazione del supporto di installazione

IBM Installation Manager consente al programma di installazione di specificare dove sono situati i package di installazione durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le directory di installazione mostrate in Tabella 9 a pagina 32.

Tabella 9. Directory di installazione di IBM Intelligent Operations Center

Directory	Descrizione	Valore consigliato
Directory di base dell'immagine locale	Il nome della directory su server di installazione contenente i file di installazione IBM Intelligent Operations Center. Si tratta della directory in cui sono stati copiati i file del supporto di installazione prima di eseguire lo strumento di installazione. Questa directory viene indicata come <i>install_media</i> in altre istruzioni di installazione.	/installMedia
Directory temp dell'immagine locale	La directory su server di installazione utilizzata per memorizzare i file temporanei durante l'installazione.	/installMedia
Directory locale di backup	Questa directory è per solo uso interno.	/tmp/loc/backup
Directory immagine remota	La directory sui server di destinazione in cui verranno copiati i package da installare su quel server.	/installMedia/loc/image
Directory script remota	La directory sui server di destinazione in cui verranno copiati gli script di installazione da eseguire su quel server.	/installMedia/loc/script

#### Attività correlate:

“Copia del package di installazione in server di installazione” a pagina 25

Copiare il package di installazione di IBM Intelligent Operations Center in server di installazione prima di installare il prodotto.

#### Ubicazione del Server di dati

IBM Installation Manager consente al programma di installazione di definire la connessione al server di dati durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le opzioni di connessione al server di dati mostrate nella Tabella 10.

Tabella 10. Informazioni sulla connessione al Server di dati di IBM Intelligent Operations Center

Opzione	Descrizione	Valore consigliato
Nome host Server di dati	Il nome host completo del server.	Nessuno. Il valore dipende dall'installazione.
Utente Server di dati	L'account utente Linux da utilizzare durante il processo di installazione.	root
Password Server di dati	La password per l'account specificato in <b>Utente server di dati</b> .	Nessuno. Il valore dipende dall'installazione.

Per eseguire il test della connessione al server, fare clic su **Verifica connessione**.

#### Ubicazione del Server delle applicazioni

IBM Installation Manager consente al programma di installazione di definire la connessione al server delle applicazioni durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le opzioni di connessione al server delle applicazioni mostrate nella Tabella 11 a pagina 33.

Tabella 11. Informazioni sulla connessione al server delle applicazioni di IBM Intelligent Operations Center

Opzione	Descrizione	Valore consigliato
Nome host Server delle applicazioni	Il nome host completo del server.	Nessuno. Il valore dipende dall'installazione.
Utente Server delle applicazioni	L'account utente Linux da utilizzare durante il processo di installazione.	root
Password Server delle applicazioni	La password per l'account specificato in <b>Utente server delle applicazioni</b> .	Nessuno. Il valore dipende dall'installazione.

Per eseguire il test della connessione al server, fare clic su **Verifica connessione**.

### Ubicazione del Server eventi

IBM Installation Manager consente al programma di installazione di definire la connessione al server eventi durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le opzioni di connessione al server eventi mostrate nella Tabella 12.

Tabella 12. Informazioni sulla connessione al server eventi di IBM Intelligent Operations Center

Opzione	Descrizione	Valore consigliato
Nome host Server eventi	Il nome host completo del server.	Nessuno. Il valore dipende dall'installazione.
Utente Server eventi	L'account utente Linux da utilizzare durante il processo di installazione.	root
Password Server eventi	La password per l'account specificato in <b>Utente server di eventi</b> .	Nessuno. Il valore dipende dall'installazione.

Per eseguire il test della connessione al server, fare clic su **Verifica connessione**.

### Ubicazione del Server di gestione

IBM Installation Manager consente al programma di installazione di definire la connessione al server di gestione durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le opzioni di connessione al server di gestione mostrate nella Tabella 13.

Tabella 13. Informazioni sulla connessione al server di gestione di IBM Intelligent Operations Center

Opzione	Descrizione	Valore consigliato
Nome host Server di gestione	Il nome host completo del server.	Nessuno. Il valore dipende dall'installazione.
Utente Server di gestione	L'account utente Linux da utilizzare durante il processo di installazione.	root
Password Server di gestione	La password per l'account specificato in <b>Utente server di gestione</b> .	Nessuno. Il valore dipende dall'installazione.

Per eseguire il test della connessione al server, fare clic su **Verifica connessione**.

### Configurazione di Cyber Hygiene

IBM Installation Manager consente al programma di installazione di specificare le opzioni richieste per Cyber Hygiene durante l'installazione di IBM Intelligent Operations Center.

Il programma di installazione può specificare le opzioni di Cyber Hygiene nella Tabella 14.

Tabella 14. Opzioni di Cyber Hygiene IBM Intelligent Operations Center

Opzione	Descrizione	Valore consigliato
Password GRUB	La password bootloader per il sistema. Questa password verrà utilizzata per tutti i server di destinazione.	Una password specificata dal cliente e coerente con la politica di password dell'organizzazione del cliente.
Disabilita l'accesso root in remoto	Definisce se l'accesso remoto è disabilitato per l'utente root su tutti i server di destinazione.	Viene visualizzata una casella di spunta con l'opzione selezionata. L'opzione non può essere deselezionata. Il login remoto di root deve essere disabilitato. L'opzione viene visualizzata in modo che il programma di installazione capisca che il login remoto di root è disabilitato.  Questa configurazione non disabilita il login come root dalla console o passa all'utente root utilizzando il comando <b>su</b> quando è collegato al server.

## Riavvio dell'installazione utilizzando Installation Manager

Se l'installazione ha esito negativo, è possibile riavviarla.

### Informazioni su questa attività

Se l'installazione ha esito negativo, lo strumento di installazione eseguirà il rollback (ripristino dello stato precedente) delle modifiche apportate durante la sessione. Se sono stati selezionati più componenti di installazione, verrà eseguito il rollback di tutte le fasi selezionate anche se alcune fasi sono state completate correttamente.

Per riavviare un'installazione non riuscita, procedere come segue.

### Procedura

1. Fare clic su **Applicazioni > IBM Installation Manager > IBM Installation Manager**.
2. Se nessun componente è stato installato correttamente, selezionare **nuovo** per riavviare l'installazione dall'inizio.
3. Se uno o più componenti sono stati installati correttamente, selezionare **modifica** per conservare le modifiche all'installazione esistente. Selezionare i componenti o quelli da installare.

**Nota:** Si consiglia di utilizzare il programma di installazione per installare i componenti di un componente alla volta. In questo modo si limiterà l'esecuzione del rollback di componenti installati correttamente se le installazioni di successivi componenti hanno esito negativo.

---

## Installazione dettagliata di IBM Intelligent Operations Center

IBM Intelligent Operations Center può essere installato utilizzando script e passi di installazione dettagliati.

### Preparazione del package di installazione

Prima di eseguire gli script di installazione, è necessario decomprimere e preparare il package di installazione.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Copiare il package di installazione in *install\_home*.
2. Estrarre il package di installazione.
3. Estrarre BA\_1.5\_GUI\_Installer\_Lite\_Launchpad.zip nella directory *install\_home*.
4. Passare alla directory *install\_home/repository/native*.
5. Estrarre com.ibm.iop.ba.lite\_1.5.0.9.zip nella directory *install\_home*.
6. Estrarre com.ibm.iop.cat.lite\_1.5.0.9.zip nella directory *install\_home*.
7. Estrarre com.ibm.iop.isp.lite\_1.5.0.zip nella directory *install\_home/isp/*.
8. Estrarre com.ibm.iop.cyber.hygiene.install.lite\_1.5.0.zip nella directory *install\_home/ch*.
9. Eseguire il comando **cp ../files/com.ibm.iop.cyber.hygiene.scripts.lite\_1.5.0.zip [install-home]/ch/install**.
10. Estrarre com.ibm.iop.ioc.solution.lite\_1.5.0.20120807.1518.zip nella directory *install\_home/ioc/spec*.
11. Estrarre com.ibm.iop.ioc.topology.lite\_1.5.0.20120807.1518.zip nella directory *install\_home/ioc/topology*.
12. Eseguire il comando **find install\_home -name \\*.sh -exec chmod +x {} \;**
13. Eseguire il comando **find install\_home -name \\*.sh -exec dos2unix {} \;**

## Verifica degli script di installazione

È possibile eseguire un comando per visualizzare la documentazione nel programma di installazione. In questo modo, è anche possibile verificare che il package di installazione sia operativo.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Collegarsi come root oppure passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Eseguire il comando *install\_home/ioc/bin/ba.sh*. La documentazione relativa all'installazione viene visualizzata.

## Personalizzazione delle proprietà di installazione

Il file delle proprietà di installazione ed i file delle proprietà della topologia forniscono le definizioni richieste dagli script di installazione.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

## Procedura

Opzionale: Modificare il file *install\_home/ioc/resource/custom.properties* e sostituire i seguenti valori delle proprietà, se desiderato. Tutti i valori delle proprietà nel file non elencati in Tabella 15 non devono essere modificati.

Tabella 15. Proprietà di installazione di IBM Intelligent Operations Center

Proprietà	Descrizione	Valore predefinito
<code>image.basedir.local</code>	Il nome della directory su server di installazione contenente i file di installazione IBM Intelligent Operations Center. Si tratta della directory in cui sono stati copiati i file del supporto di installazione prima di eseguire lo strumento di installazione. Questa directory viene indicata come <i>install_media</i> in altre istruzioni di installazione.	<code>/installMedia</code>
<code>image.tempdir.local</code>	La directory su server di installazione utilizzata per memorizzare i file temporanei durante l'installazione.	<code>/installMedia</code>
<code>backup.local</code>	Questa directory è per solo uso interno.	<code>/tmp/loc/backup</code>
<code>Unix.image.basedir.remote</code>	La directory sui server di destinazione in cui verranno copiati i package da installare su quel server.	<code>/installMedia/loc/image</code>
<code>Unix.script.basedir.remote</code>	La directory sui server di destinazione in cui verranno copiati gli script di installazione da eseguire su quel server.	<code>/installMedia/loc/script</code>
<code>connection.timeout</code>	Intervallo di tempo (in millisecondi) di attesa di una connessione ai server di destinazione prima che venga restituito un errore	120000
<code>waiting.time</code>	Intervallo di tempo (in millisecondi) di attesa prima di provare ad eseguire nuovamente una connessione non riuscita	120000
<code>retry.count</code>	Numero di volte in cui ripetere una connessione non riuscita prima che l'installazione restituisca un errore	6

Se non modificati, vengono utilizzati i valori predefiniti.

### Concetti correlati:

“Informazioni sulla password” a pagina 39

Le password per i diversi ID utente nella soluzione IBM Intelligent Operations Center sono definite nel file delle proprietà della topologia. Per motivi di sicurezza le password predefinite fornite con IBM Intelligent Operations Center devono essere modificate.

## Installazione dei file della topologia

IBM Intelligent Operations Center è installato utilizzando un file della topologia. Il file della topologia è un file XML che definisce i parametri e i valori utilizzati quando IBM Intelligent Operations Center viene distribuito sui server e definisce la sequenza utilizzata per distribuire i componenti.

La modifica del file della topologia con un editor di test può introdurre errori. Per questo motivo tutte le proprietà personalizzabili dal cliente vengono definite in un file delle proprietà della topologia. Un file di modello della topologia fornisce la struttura della topologia.

Il comando **parameterizeTopology** acquisisce la coppia nome/valore definita nel file delle proprietà della topologia e la struttura fornita dal file di modello della topologia e crea un file della topologia valido che è quindi utilizzato durante l'installazione.

IBM Intelligent Operations Center fornisce i seguenti file della topologia:

Nome file	Scopo
<i>home_installazione/ioc/resource/custom.properties</i>	Definisce l'ubicazione del supporto di installazione, le directory di lavoro e altre proprietà. Questo file può essere modificato per soddisfare le esigenze dell'ambiente del cliente.
<i>home_installazione/ioc/topology/iop_lite_topo.properties</i>	Definisce le proprietà personalizzabili dal cliente per la distribuzione tra cui nomi host e password. Questo file può essere modificato per soddisfare le esigenze dell'ambiente del cliente.
<i>home_installazione/ioc/topology/iop_lite_topo.template.xml</i>	Definisce la struttura della topologia da distribuire. Questo file utilizza i valori definiti nel file delle proprietà. Questo file non deve essere modificato.
<i>home_installazione/ioc/topology/iop_lite_topo.xml</i>	Definisce la topologia da distribuire. Tale file viene creato dal comando <b>parameterizeTopology</b> utilizzando le informazioni nelle proprietà e nel file modello. Questo file non deve essere modificato tranne quando è necessario il ripristino da un errore di installazione.
<i>home_installazione/ioc/topology/iop_lite_topo.chk</i>	Definisce i ruoli utilizzati dallo strumento di pre-verifica per determinare se i server sono correttamente configurati per l'installazione di IBM Intelligent Operations Center. Questo file non deve essere modificato.

#### Attività correlate:

“Installazione di Strumento di controllo della piattaforma” a pagina 49

Lo Strumento di controllo della piattaforma viene utilizzato per gestire l'ambiente del server IBM Intelligent Operations Center. Lo strumento è installato separatamente dal prodotto.

### File delle proprietà della topologia

Il file delle proprietà della topologia definisce le proprietà personalizzabili dal cliente per la distribuzione di IBM Intelligent Operations Center. Questo file deve essere modificato per soddisfare le esigenze dell'ambiente del cliente. Le proprietà presenti nel file delle proprietà della topologia fornito non documentate qui non devono essere modificate.

Dopo avere modificato il file delle proprietà della topologia, salvare una copia in un luogo sicuro. Il file contiene informazioni sensibili sulla sicurezza, come i nomi utente e le password del sistema, in testo leggibile. Se una persona non autorizzata ha accesso a questo file, disporrà dell'accesso completo al sistema.

Il file delle proprietà della topologia può essere utilizzato dopo l'installazione nei seguenti modi:

- Come repository di informazioni relative alla password se una password viene dimenticata.
- Come un repository per le password quando vengono modificate dal sistema. Il file delle proprietà della topologia modificato può essere utilizzato per aggiornare le password utilizzate da Strumento di controllo della piattaforma.
- Come backup delle informazioni sull'installazione se il sistema deve essere reinstallato. Il file delle proprietà della topologia può essere utilizzato senza dover ridefinire tutti i parametri di installazione.



**Attività correlate:**

“Generazione del file della topologia” a pagina 42

Prima di eseguire i passi di installazione per IBM Intelligent Operations Center, generare un file della topologia con i parametri richiesti per l'installazione.

**Informazioni sul server di destinazione:**

La sezione SERVERS del file delle proprietà della topologia per i server di destinazione.

Tabella 16 mostra i valori delle proprietà del server che è possibile specificare nel file delle proprietà della topologia.

Tabella 16. Proprietà del server di destinazione

Proprietà	Descrizione
DB.1.HOST	Il nome host di server di dati
DB.1.ACCOUNT.PWD	La password di root password per server di dati
DB.1.SSH_PORT	Il numero di porta per l'accesso ssh a server di dati
APP.1.HOST	Il nome host di server delle applicazioni
APP.1.ACCOUNT.PWD	La password di root password per server delle applicazioni
APP.1.SSH_PORT	Il numero di porta per l'accesso ssh a server delle applicazioni
EVENT.1.HOST	Il nome host di server eventi
EVENT.1.ACCOUNT.PWD	La password di root password per server eventi
EVENT.1.SSH_PORT	Il numero di porta per l'accesso ssh a server eventi
MGMT.1.HOST	Il nome host di server di gestione
MGMT.1.ACCOUNT.PWD	La password di root password per server di gestione
MGMT.1.SSH_PORT	Il numero di porta per l'accesso ssh a server di gestione

**Importante:** I valori dei nomi host devono essere nomi host completi nel caso definito. Ad esempio, IOC15App.IOC15.com non è uguale a ioc15app.ioc15.com.

Un numero di porta ssh può essere impostato per ciascun server. Tuttavia, i numeri delle porte configurate verranno utilizzati solo da Strumento di controllo della piattaforma. La porta 22 deve essere abilitata per l'accesso ssh su ciascun server. La porta 22 è richiesta per l'accesso ssh da IBM Intelligent Operations Center durante l'installazione.

**Informazioni sui servizi di directory:**

Il file delle proprietà della topologia definisce i valori utilizzati per codificare le password utente e altri dati sensibili all'interno della directory.

La codifica è basata su due valori: LDAP.SEED e LDAP.SALT.

I valori devono essere caratteri ASCII stampabili. I caratteri ASCII stampabili sono caratteri con valori punto codice che vanno da 33 a 126. Non è possibile utilizzare uno spazio vuoto.



Tabella 17. Proprietà dei servizi di directory

Proprietà	Descrizione
LDAP.SEED	Una stringa di caratteri da 12 a 1016, composta da caratteri ASCII stampabili, tra i punti codice 33 e 126.  È necessario utilizzare una stringa con codifica strong. Ad esempio, una stringa lunga composta da lettere maiuscole e minuscole, numeri e caratteri speciali senza parole o frasi comuni.
LDAP.SALT	Una stringa di 12 caratteri, composta da caratteri ASCII stampabili, tra i punti codice 33 e 126. <b>Importante:</b> LDAP.SALT deve essere esattamente di 12 caratteri in lunghezza. Un valore con un numero di caratteri inferiore o superiore non consentirà l'installazione.

Registrare i valori LDAP.SEED e LDAP.SALT al di fuori del sistema. I valori saranno richiesti se è necessario esportare o replicare le voci di directory.

#### Informazioni sulla password:

Le password per i diversi ID utente nella soluzione IBM Intelligent Operations Center sono definite nel file delle proprietà della topologia. Per motivi di sicurezza le password predefinite fornite con IBM Intelligent Operations Center devono essere modificate.

Le password possono contenere solo caratteri alfanumerici (a-z, A-Z, 0-9). Se non diversamente indicato, le password devono essere di 30 caratteri o meno.

Tabella 18. Proprietà delle password

Proprietà	Nome utente associato	Descrizione
LDAP.DB.PWD	dsrdbm01	Database di directory LDAP
LDAP.ADMIN.DN.PWD	cn=root	Bind amministratore LDAP
LDAP.BIND.DN.PWD	cn=bind	Bind LDAP
LDAP.PROXY.INSTANCE.PWD	tdsproxy	Istanza proxy LDAP
LDAP.PROXY.ADMIN.DN.PWD	cn=root	Bind amministratore proxy LDAP
LDAP.PROXY.BIND.DN.PWD	cn=bind	Bind proxy LDAP
TAM.SECMASTER.PWD	nessuno	Password principale del servizio di sicurezza  A questo utente vengono concessi i privilegi equivalenti all'utente root sui server di destinazione. A causa dell'accesso offerto a questo utente, assicurarsi che la password abbia un valore lungo, sia diversa da altre password e che sia conservata in un luogo sicuro.

Tabella 18. Proprietà delle password (Continua)

Proprietà	Nome utente associato	Descrizione
TAM.WEBSEAL.ADMIN.PWD	sec_master	Amministratore del servizio di sicurezza  A questo utente vengono concessi i privilegi equivalenti all'utente root sui server di destinazione. A causa dell'accesso offerto a questo utente, assicurarsi che la password abbia un valore lungo, sia diversa da altre password e che sia conservata in un luogo sicuro.
WBM.DB.USER.PWD	db2ibm	Database del servizio di monitoraggio delle attività di business
WODM.DB.USER.PWD	db2wodm	Database del servizio di gestione decisioni
WODM.ADMIN.UID.PWD	resAdmin1	Amministratore del servizio di gestione decisioni
WODM.DEPLOYER.UID.PWD	resDeployer1	Distributore regole del servizio di gestione decisioni
WODM.MONITOR.UID.PWD	resMonitor1	Monitor del servizio di gestione decisioni
WODM.DB.DC.USER.PWD	wodmdc	Database della console decisioni
WODM.rtsAdmin.UID.PWD	rtsAdmin	Amministratore della console decisioni
WODM.rtsConfig.UID.PWD	rtsConfig	Configurazione della console decisioni
WODM.rtsUser.UID.PWD	rtsUser	Utente della console decisioni
UDDI.DB.USER.PWD	db2uddi	Database di servizio UDDI
IHS.KEYSTORE.PWD	nessuno	Keystore del server HTTP
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Amministratore di servizi delle applicazioni
WAS.LTPA.PWD	nessuno	Token LTPA
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Amministratore della console WebSphere Application Server per il server WebSphere Portal
PORTAL.ADMIN.UID.PWD	wpsadmin	Amministratore per il server WebSphere Portal
PORTAL.DB.USER.PWD	db2port1	Database WebSphere Portal
OMNIBUS.ADMIN.ACCOUNT.PWD	netcool	Amministratore dei servizi eventi
IMPACT.WAS.ACCOUNT.PWD	wasadmin	Amministratore dei servizi eventi di sistema
TSRM.WAS.ADMIN.PWD	waswebadmin	Amministratore del gestore richieste di servizi
TSRM.DB.USER.PWD	maximo	Database del gestore richieste di servizi
TSRM.ADMIN.USER.PWD	maxadmin	Amministratore del gestore richieste di servizi

Tabella 18. Proprietà delle password (Continua)

Proprietà	Nome utente associato	Descrizione
TSRM.REG.USER.PWD	maxreg	Utente del gestore richieste di servizi
TSRM.INITADM.USER.PWD	maxintadm	Utente di integrazione del gestore richieste di servizi
MGMT.WAS.ADMIN.PWD	waswebadmin	Amministratore di servizi delle applicazioni
TEPS.DB.USER.PWD	itmuser	Database del portale Enterprise
TIM.STORE.PWD	none	Archivio di gestione identità
TIM.ADMIN.USER.PWD	waswebadmin	Amministratore del gestore identità
DOMINO.USER.PWD	notes	Utente della collaborazione
DOMINO.ORG.PWD	IBM	Organizzazione della collaborazione
DOMINO.ADMIN.PWD	notes admin	Amministratore della collaborazione
DOMINO.ST.ADMIN.PWD	wpsadmin	Amministratore del portale di collaborazione
DOMINO.ST.BIND.PWD	wpsbind	Bind LDAP di collaborazione
DEFAULT.PWD.DAS	dausr1, dausr2, dausr3, dausr4, dausr5, dausr6, dausr7, dausr8	Server di gestione dei servizi di database
DEFAULT.PWD.DB2	db2inst1, db2inst2, db2inst3, db2inst4, db2inst5, db2inst6, db2inst7, db2inst8	Server di dati dei servizi di database
DEFAULT.PWD.IHS	ihsadmin	Server HTTP
DEFAULT.PWD.MQM	mqm	Utenti dei servizi di messaggistica
MQM.CONN.USER.PWD	mqmconn	Connessione dei servizi di messaggistica
DEFAULT.PWD.TAI	taiuser	Sicurezza dei servizi delle applicazioni
ITM.ADMIN.PWD	sysadmin	Amministratore di gestione del sistema <b>Limitazione:</b> La password deve essere di 15 caratteri o meno.
IOP.ADMIN.USER.PWD	ibmadmin	Strumenti di gestione del sistema  A questo utente vengono concessi i privilegi equivalenti all'utente root sui server di destinazione. Strumento di controllo della piattaforma viene eseguito con questo nome utente. A causa dell'accesso offerto a questo utente, assicurarsi che la password abbia un valore lungo, sia diversa da altre password e che sia conservata in un luogo sicuro.
IOP.USER.USER.PWD	ibmuser	Utente generale di sistema

### Concetti correlati:

Capitolo 3, “Protezione della soluzione”, a pagina 69

La sicurezza è importante all'interno di IBM Intelligent Operations Center poiché la soluzione è fondamentale per operazioni essenziali. Per garantire la sicurezza, è importante conoscere le impostazioni predefinite e gestire gli utenti della soluzione per fornire a tutti gli utenti il corretto livello di accesso.

### Attività correlate:

“Personalizzazione delle proprietà di installazione” a pagina 35

Il file delle proprietà di installazione ed i file delle proprietà della topologia forniscono le definizioni richieste dagli script di installazione.

### Riferimenti correlati:

“Utenti di esempio” a pagina 71

Durante la distribuzione di IBM Intelligent Operations Center, vengono creati utenti di esempio.

## Creazione della password della topologia

La password della topologia viene utilizzata durante il processo di installazione per codificare ed accedere al file che definisce la topologia della soluzione.

### Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Collegarsi come root oppure passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Passare alla directory *install\_home/ioc*.
4. Eseguire il comando **bin/ba.sh createSecretKey -p password** dove *password* è la password da creare per la topologia. Questo comando crea il file *install\_home/ioc/resource/ioc.keystore*. Questo file contiene le chiavi utilizzate per codificare il file delle proprietà della topologia. Il file *ioc.keystore* viene inoltre codificato con la password specificata nel comando **createSecretKey**. Per modificare la password e la chiave per l'installazione, eliminare il file *install\_home/ioc/resource/ioc.keystore* ed eseguire nuovamente il comando **createSecretKey**. Prendere nota della password per utilizzarla in altri passi dell'installazione.

### Attività correlate:

“Generazione del file della topologia”

Prima di eseguire i passi di installazione per IBM Intelligent Operations Center, generare un file della topologia con i parametri richiesti per l'installazione.

## Generazione del file della topologia

Prima di eseguire i passi di installazione per IBM Intelligent Operations Center, generare un file della topologia con i parametri richiesti per l'installazione.

### Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Collegarsi come root oppure passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Passare alla directory *install\_home/ioc/topology*.

4. Modificare il file `iop_lite_topo.properties` ed apportare le modifiche richieste per il proprio ambiente.
5. Copiare il file template della topologia nel file della topologia eseguendo il comando `cp iop_lite_topo.template.xml iop_lite_topo.xml`.
6. Passare alla directory `install_home/ioc`.
7. Eseguire il comando `bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password` dove `password` è la password della topologia. I parametri definiti nel file delle proprietà della topologia vengono applicati al file della topologia.
8. Opzionale: Per codificare le password nel file della topologia, eseguire il comando `bin/ba.sh encryptTopology -t iop_lite_topo -p password` dove `password` è la password della topologia.

**Importante:** Verranno codificate solo le password nel file della topologia. Le password in altri file, ad esempio nel file delle proprietà della topologia, non verranno codificate.

#### Concetti correlati:

“File delle proprietà della topologia” a pagina 37

Il file delle proprietà della topologia definisce le proprietà personalizzabili dal cliente per la distribuzione di IBM Intelligent Operations Center. Questo file deve essere modificato per soddisfare le esigenze dell'ambiente del cliente. Le proprietà presenti nel file delle proprietà della topologia fornito non documentate qui non devono essere modificate.

#### Attività correlate:

“Creazione della password della topologia” a pagina 42

La password della topologia viene utilizzata durante il processo di installazione per codificare ed accedere al file che definisce la topologia della soluzione.

## Esecuzione dello strumento di pre-verifica

Prima di caricare i package di installazione sui server di destinazione, verificare che i server di destinazione siano pronti per l'installazione eseguendo lo strumento di pre-verifica.

### Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come `install_home`.

#### Procedura

1. Collegarsi come root oppure passare all'account root eseguendo il comando `su -`.
2. Eseguire il comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`.
3. Passare alla directory `install_home/ioc`.
4. Eseguire il comando `bin/ba.sh precheckTopology -t iop_lite_topo -p password` dove `password` è la password della topologia. Per ciascun test di pre-verifica su ciascun server, verranno visualizzati dei messaggi. Lo stato di ciascun test sarà [Pass] oppure [Fail]. Una volta eseguiti tutti i test, viene visualizzato un riepilogo di tutti i test non superati.
5. In caso di errori, eseguire le azioni appropriate per risolvere il problema ed eseguire nuovamente lo strumento di pre-verifica fino a quando non sono più presenti errori.

#### Risultati

Se viene visualizzato il messaggio CHK0101W, per l'ambiente non è configurato alcun server DNS oppure nel server DNS non sono definiti i propri server. È possibile ignorare questo messaggio di avvertenza se i server sono definiti utilizzando l'indirizzamento IP statico nel file `/etc/hosts`.

### Concetti correlati:

“Connessione di rete TCP/IP” a pagina 21

Prima di installare IBM Intelligent Operations Center, la connessione di rete TCP/IP tra i server deve essere configurata correttamente.

## Impostazioni di sicurezza Linux

Per abilitare lo Strumento di controllo della piattaforma, è necessario modificare le impostazioni di sicurezza Linux.

È possibile modificare tali impostazioni eseguendo una serie di comandi o utilizzando uno script.

Lo script apporta le modifiche indicate dai comandi. Se i comandi non soddisfano le esigenze della propria installazione o se i processi aziendali non consentono di apportare modifiche alla sicurezza utilizzando uno script, modificare le impostazioni utilizzando comandi singoli.

### Personalizzazione manuale delle impostazioni di sicurezza Linux

È possibile configurare le impostazioni di sicurezza Linux richieste eseguendo una serie di comandi.

#### Procedura

1. Sul sistema server di installazione collegarsi come root oppure eseguire il comando **su** - per passare all'account root.
2. Effettuare quanto segue per abilitare Strumento di controllo della piattaforma. Queste operazioni devono essere eseguite per ciascun server di destinazione seguente:
  - Server delle applicazioni
  - Server di dati
  - Server eventi
  - Server di gestione
  - a. Eseguire il comando **visudo**. Il file `/etc/sudoers` verrà aperto per la modifica.
  - b. Immettere la lettera `i` per cambiare la modalità di inserimento consentendo di apportare le modifiche al file.
  - c. Trovare la seguente riga:

```
#%wheel ALL=(ALL) NOPASSWD: ALL
```

e modificarla in:

```
%wheel ALL=(ALL) NOPASSWD: ALL
```
  - d. Aggiungere la seguente riga alla fine del file:

```
Defaults:%wheel !requiretty
```
  - e. Premere Esc. Si esce dalla modalità di inserimento.
  - f. Immettere `:wq`. Il file è salvato.
  - g. Eseguire il comando **exit**. Il sistema ritorna al login di server di installazione.

Dopo aver completato le operazioni per tutti e quattro i server, la sicurezza di Linux consente agli utenti nel gruppo `wheel` di utilizzare il comando **sudo** per eseguire i comandi di sistema localmente o da una sessione remota.

#### Attività correlate:

“Personalizzazione delle impostazioni di sicurezza Linux con uno script”

Le impostazioni di sicurezza Linux richieste possono essere effettuata eseguendo uno script.

### Personalizzazione delle impostazioni di sicurezza Linux con uno script

Le impostazioni di sicurezza Linux richieste possono essere effettuata eseguendo uno script.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. Passare alla directory *install\_home/ioc*.
2. Eseguire il comando `bin/install-prepare-env.sh -d install_home/ioc -f topology/iop_lite_topo.properties -p password` dove *password* è la password della topologia.

#### Attività correlate:

“Personalizzazione manuale delle impostazioni di sicurezza Linux” a pagina 44

È possibile configurare le impostazioni di sicurezza Linux richieste eseguendo una serie di comandi.

## Comando installTopology

Il comando **installTopology** utilizza le informazioni nel file della topologia per installare IBM Intelligent Operations Center.

Prima di utilizzare il file della topologia per installare IBM Intelligent Operations Center, il comando **installTopology** controlla che i file di installazione siano stati copiati sui server di destinazione. Se i file non sono stati copiati, il comando **installTopology** copia i file necessari prima di continuare.

Utilizzando il file della topologia come guida, il comando **installTopology** installa ciascun componente di IBM Intelligent Operations Center ed esegue la configurazione richiesta. Durante l'installazione vengono visualizzati dei messaggi che indicano l'avanzamento dell'installazione.

Se si verificano errori durante l'elaborazione del comando **installTopology**, è possibile riavviare l'installazione una volta risolti i problemi che hanno causato gli errori di installazione di uno o più componenti. Le installazioni non riuscite sono indicate dallo stato dell'installazione nel file della topologia.

**Nota:** In un ambiente virtuale, si consiglia di eseguire un'istanza dell'ambiente prima di eseguire il comando **installTopology** e dopo ciascuna installazione eseguita correttamente.

## Stato dell'installazione

L'attributo **Status** del file della topologia indica lo stato dell'installazione di ciascun componente. Quando viene eseguito il comando **installTopology**, viene eseguita l'azione indicata in Tabella 19, in base allo stato del componente.

Tabella 19. Stato dell'installazione ed azioni

Valore	Stato	Azione installTopology
New	Il componente non è stato installato.	Lo stato viene modificato in Uncertain ed il componente verrà installato. Quando il componente viene installato correttamente, lo stato viene modificato in Ready.
Ready	Il componente è stato installato correttamente.	Quando il comando <b>installTopology</b> viene eseguito nuovamente, l'installazione del componente viene ignorata.
Uncertain	Il componente non è stato installato correttamente oppure l'installazione è in corso.	Il componente verrà installato. Quando il componente viene installato correttamente, lo stato viene modificato in Ready.



# Opzioni per l'installazione dei componenti di IBM Intelligent Operations Center

L'installazione di IBM Intelligent Operations Center può impiegare diverse ore. A causa del tempo necessario, è possibile installare IBM Intelligent Operations Center in una o più fasi.

In un'installazione a fase singola, il processo di installazione viene eseguito fino a quando non vengono installati tutti i componenti oppure si verifica un errore nell'installazione. In caso di errore, è necessario riavviare l'installazione dall'inizio.

In un'installazione a più fasi, il processo di installazione è suddiviso in tre fasi separate:

## **uploadTopology**

Copia i file di installazione dal server di installazione ai server di destinazione.

**Fase 1** Installa alcuni dei componenti di IBM Intelligent Operations Center creando una base per l'installazione dei componenti rimanenti.

**Fase 2** Installa i componenti di IBM Intelligent Operations Center rimanenti.

Durante l'esecuzione in un ambiente virtualizzato, è necessario eseguire un'istantanea dopo ciascuna fase, nel caso in cui sia richiesto un riavvio.

La fase **uploadTopology** viene eseguita come un comando separato. Se i file di installazione sono già stati copiati sui server di destinazione, non verranno copiati nuovamente.

La fase o le fasi da eseguire sono definite nel file delle proprietà della topologia. Le proprietà **Status.Phase1** e **Status.Phase2** determinano se le fasi di installazione vengono eseguite quando viene eseguito il comando **installTopology**. Se le proprietà sono impostate su **New**, la fase viene eseguita. Se le proprietà sono impostate su **Ready**, la fase viene ignorata.

## **Installazione dell'architettura IBM Intelligent Operations Center in una singola fase**

L'architettura utilizzata con IBM Intelligent Operations Center può essere installata in una singola fase. Se si sta eseguendo l'installazione in un ambiente virtualizzato, l'esecuzione dell'installazione in una singola fase non consente di eseguire istantanee durante il processo di installazione.

## **Informazioni su questa attività**

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

## **Procedura**

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando **su -**.
2. Copiare i file richiesti per l'installazione nei server di destinazione ed installare IBM Intelligent Operations Center.
  - a. Passare alla directory *install\_home/ioc*.
  - b. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
  - c. Eseguire il comando **bin/ba.sh installTopology -t iop\_lite\_topo -p password** dove *password* è la password della topologia.

I file di installazione richiesti verranno copiati sui server di destinazione e IBM Intelligent Operations Center verrà installato.

I messaggi vengono visualizzati indicando lo stato di avanzamento dell'installazione. I messaggi indicano lo stato del componente installato. Lo stato sarà uno dei seguenti:

[ OK ] Componente installato correttamente.



[ Fail ]

Installazione componente non riuscita.

## Risultati

Il processo di installazione può richiedere fino a 14 ore. L'architettura IBM Intelligent Operations Center è installata correttamente quando tutti i messaggi vengono completati con lo stato [ OK ].

## Installazione di IBM Intelligent Operations Center in più fasi

L'architettura utilizzata con IBM Intelligent Operations Center può essere installata in più fasi.

Un'installazione a più fasi consente di risolvere i problemi relativi all'installazione più rapidamente, invece di attendere il completamento dell'intero processo di installazione. Se si sta eseguendo l'installazione in un ambiente virtualizzato, l'esecuzione dell'installazione in più fasi consente anche di eseguire istantanee durante il processo di installazione.

## Informazioni su questa attività

**Importante:** Non arrestare i server tra le fasi di installazione. L'arresto dei server tra le fasi non è stata sottoposta a test e può portare a risultati imprevedibili.

## Procedura

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Copiare i file di installazione sui server di destinazione.
  - a. Passare alla directory *install\_home/ioc*.
  - b. Eseguire il comando **bin/ba.sh uploadImage -t iop\_lite\_topo -threadCount 4 -p password** dove *password* è la password della topologia. Il parametro **-threadCount** specifica il numero di thread utilizzati durante la copia dei file di installazione. Se necessario, è possibile modificare il valore.

I file richiesti per ciascun server di destinazione vengono copiati dal server di installazione ai server di destinazione. Questo passo può richiedere fino a 2 ore.

Vengono visualizzati dei messaggi che indicano l'avanzamento del processo di caricamento. I messaggi indicano lo stato del componente caricato. Lo stato sarà uno dei seguenti:

[ OK ] Componente caricato correttamente.

[ Fail ]

Caricamento del componente non riuscito.

4. Opzionale: Se si sta eseguendo l'installazione in un ambiente virtualizzato, eseguire un'istananea di tutti i server di destinazione. Prima di eseguire l'istananea, arrestare le macchine virtuali per risparmiare spazio su disco e ridurre il tempo di elaborazione. Una volta eseguita l'istananea, riavviare le macchine virtuali. È possibile utilizzare l'istananea per riavviare l'installazione da questo punto in caso di errori durante le operazioni di installazione successive.
5. Preparare l'esecuzione della fase 1 di installazione.
  - a. Utilizzando un editor di testo, modificare il file delle proprietà della topologia:  
*install\_home/ioc/topology/iop\_lite\_topo.properties*.
  - b. Modificare i valori dello stato nel modo riportato di seguito:  
Status.Phase1="New"  
Status.Phase2="Ready"

Questa istruzione indica al programma di installazione di installare la prima fase ed ignorare la seconda fase.

- c. Passare alla directory *install\_home/ioc*.

- d. Eseguire il comando **cp topology/iop\_lite\_topo.template.xml topology/iop\_lite\_topo.xml**. Il file template della topologia verrà copiato nel file della topologia.
  - e. Eseguire il comando **bin/ba.sh parameterizeTopology -t iop\_lite\_topo -r topology/iop\_lite\_topo.properties -p password** dove *password* è la password della topologia. I valori delle proprietà definiti nel file delle proprietà della topologia verranno applicati al file della topologia.
  - f. Opzionale: Eseguire il comando **bin/ba.sh encryptTopology -t iop\_lite\_topo -ppassword** dove *password* è la password della topologia. Le password nel file della topologia verranno codificate utilizzando la password della topologia fornita.
6. Eseguire la fase 1 dell'installazione.
    - a. Passare alla directory *install\_home/ioc*.
    - b. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
    - c. Eseguire il comando **bin/ba.sh installTopology -t iop\_lite\_topo -p password** dove *password* è la password della topologia.

L'installazione installa i componenti di base richiesti per IBM Intelligent Operations Center. Questo passo può richiedere fino a 9 ore.

I messaggi vengono visualizzati indicando lo stato di avanzamento dell'installazione. I messaggi indicano lo stato del componente installato. Lo stato sarà uno dei seguenti:

[ OK ] Componente installato correttamente.

[ Fail ]

Installazione componente non riuscita.

7. Opzionale: Se si sta eseguendo l'installazione in un ambiente virtualizzato, eseguire un'istantanea di tutti i server di destinazione. Non arrestare i server virtuali prima di eseguire l'istantanea. Durante l'esecuzione dell'istantanea, includere un'istantanea della memoria della macchina virtuale. È possibile utilizzare l'istantanea per riavviare l'installazione da questo punto in caso di errori durante le operazioni di installazione successive.
8. Preparare l'esecuzione della fase 2 di installazione.
  - a. Utilizzando un editor di testo, modificare il file delle proprietà della topologia: *install\_home/ioc/topology/iop\_lite\_topo.properties*.
  - b. Modificare i valori dello stato nel modo riportato di seguito:
 

```
Status.Phase1="Ready"
Status.Phase2="New"
```

Questa istruzione indica al programma di installazione di installare la seconda fase ed ignorare la prima fase.
  - c. Passare alla directory *install\_home/ioc*.
  - d. Eseguire il comando **cp topology/iop\_lite\_topo.template.xml topology/iop\_lite\_topo.xml**. Il file template della topologia verrà copiato nel file della topologia.
  - e. Eseguire il comando **bin/ba.sh parameterizeTopology -t iop\_lite\_topo -r topology/iop\_lite\_topo.properties -p password** dove *password* è la password della topologia. I valori delle proprietà definiti nel file delle proprietà della topologia verranno applicati al file della topologia.
  - f. Opzionale: Eseguire il comando **bin/ba.sh encryptTopology -t iop\_lite\_topo -ppassword** dove *password* è la password della topologia. Le password nel file della topologia verranno codificate utilizzando la password della topologia fornita.
9. Eseguire la fase 2 dell'installazione.
  - a. Passare alla directory *install\_home/ioc*.
  - b. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
  - c. Eseguire il comando **bin/ba.sh installTopology -t iop\_lite\_topo -p password** dove *password* è la password della topologia.

L'installazione installa i componenti rimanenti richiesti per IBM Intelligent Operations Center. Questo passo può richiedere fino a 4 ore.

I messaggi vengono visualizzati indicando lo stato di avanzamento dell'installazione. I messaggi indicano lo stato del componente installato. Lo stato sarà uno dei seguenti:

[ OK ] Componente installato correttamente.

[ Fail ]

Installazione componente non riuscita.

## Risultati

L'architettura IBM Intelligent Operations Center è installata correttamente quando tutti i messaggi vengono completati con lo stato [ OK ].

## Riavvio dell'installazione dell'architettura IBM Intelligent Operations Center durante un'installazione dettagliata

In caso di errore dell'installazione dell'architettura, è possibile riavviare l'installazione.

### Informazioni su questa attività

Per riavviare un'installazione non riuscita, effettuare le operazioni riportate di seguito.

### Procedura

1. Aprire il file della topologia per determinare il componente per cui si è verificato l'errore. Tale componente è indicato da `Status="Uncertain"`.
2. Determinare e risolvere la causa dell'errore. È possibile utilizzare lo strumento "must gather" dell'installazione per raccogliere i log di installazione per l'analisi.
3. Eseguire nuovamente il comando `installTopology`. Verrà eseguito un nuovo tentativo di installazione. Verranno installati tutti i componenti con `Status="New"` e `Status="Uncertain"`. I componenti con `Status="Ready"` sono stati installati correttamente e vengono ignorati.

### Operazioni successive

In alcuni casi, l'installazione di un componente non riuscita non viene eseguita correttamente. In questo caso, è necessario creare ripristinare l'ambiente nello stato in cui si trovava prima dell'esecuzione del comando `installTopology` e riavviare l'installazione. Per gli ambienti con virtualizzazione, è possibile utilizzare le istantanee dell'ambiente per riportare il sistema allo stato in cui si trovava prima dell'esecuzione del comando `installTopology`.

#### Attività correlate:

“Esecuzione dello strumento "must gather" dell'installazione” a pagina 299

Durante l'installazione di IBM Intelligent Operations Center vengono generati dei file di log. Uno strumento è disponibile per raccogliere questi file di log per l'analisi.

## Installazione di Strumento di controllo della piattaforma

Lo Strumento di controllo della piattaforma viene utilizzato per gestire l'ambiente del server IBM Intelligent Operations Center. Lo strumento è installato separatamente dal prodotto.

### Prima di iniziare

Il prodotto IBM Intelligent Operations Center deve essere installato prima di installare lo Strumento di controllo della piattaforma.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Procedura

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando **su -**.
2. Passare alla directory *install\_home/isp/mgmt/setup*.
3. Eseguire il comando **./iopmgmt-install.sh -finstall\_home/ioc/topology/iop\_lite\_topo.properties -p password** dove *password* è la password che si desidera utilizzare durante l'accesso allo strumento. Ricordare tale password, perché sarà necessaria durante l'esecuzione dello strumento. Lo Strumento di controllo della piattaforma è correttamente installato sul server di gestione quando tutti i componenti sono visualizzati come installati con lo stato [ OK ].
4. Opzionale: Se non si utilizza Java fornito da IBM Intelligent Operations Center, sul server di gestione modificare i file */opt/IBM/ISP/mgmt/scripts/CommandEngine.sh* e */opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh*. Modificare il valore `export JAVA_HOME=` in ciascun file impostando l'ubicazione di JRE Java sul server.

### Operazioni successive

Verificare che lo Strumento di controllo della piattaforma sia stato installato correttamente avviando, arrestando ed eseguendo le query dei servizi utilizzando lo Strumento di controllo della piattaforma.

#### Concetti correlati:

“Installazione dei file della topologia” a pagina 36

IBM Intelligent Operations Center è installato utilizzando un file della topologia. Il file della topologia è un file XML che definisce i parametri e i valori utilizzati quando IBM Intelligent Operations Center viene distribuito sui server e definisce la sequenza utilizzata per distribuire i componenti.

#### Attività correlate:

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Query dello stato dei servizi” a pagina 202

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

## Installazione dello strumento Controllo di verifica del sistema

Lo strumento Controllo di verifica del sistema viene utilizzato per verificare lo stato operativo dei componenti in IBM Intelligent Operations Center. Lo strumento viene installato separatamente dal prodotto.

### Prima di iniziare

Il prodotto IBM Intelligent Operations Center deve essere installato prima di installare lo strumento Controllo di verifica del sistema.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

## Procedura

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Passare alla directory *install\_home/cat/bin*.
4. Eseguire il comando **./install-cat-lite.sh -d install\_home/cat -f install\_home/ioc/topology/iop\_lite\_topo.properties -p password** dove *password* è la password della topologia.

**Nota:** Il comando deve essere eseguito dalla directory *install\_home/cat/bin*.

Lo strumento Controllo di verifica del sistema è installato correttamente quando vengono visualizzati tutti i componenti installati vengono visualizzati con lo stato [ OK ].

5. Riavviare tutti i server di IBM Intelligent Operations Center.
  - a. Arrestare tutti i server IBM Intelligent Operations Center utilizzando lo Strumento di controllo della piattaforma.
  - b. Arrestare e riavviare tutti i server dal sistema operativo.
  - c. Arrestare tutti i server IBM Intelligent Operations Center utilizzando lo Strumento di controllo della piattaforma.

## Operazioni successive

Verificare che lo strumento Controllo di verifica del sistema sia stato installato correttamente eseguendo lo strumento Controllo di verifica del sistema.

### Attività correlate:

“Come utilizzare lo strumento Controllo di verifica del sistema” a pagina 210

Lo strumento Controllo di verifica del sistema viene utilizzato per determinare lo stato operativo di servizi compreso il sistema IBM Intelligent Operations Center.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

## Installazione dell'applicazione IBM Intelligent Operations Center

Installare l'applicazione IBM Intelligent Operations Center dopo aver installato l'architettura IBM Intelligent Operations Center, incluso Controllo di verifica del sistema e Strumento di controllo della piattaforma.

## Prima di iniziare

L'architettura IBM Intelligent Operations Center deve essere installata e tutti i servizi avviati.

## Procedura

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando **su -**.
2. Eseguire il comando **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre**.
3. Passare alla directory *install\_home/ioc*.
4. Eseguire il comando **cp topology/iop\_lite\_topo.xml topology/iop\_lite\_topo\_phase2.xml**.
5. Eseguire il comando **bin/ba.sh installTopology -t ioc\_lite\_topo -p password** dove *password* è la password della topologia. L'installazione installa l'applicazione IBM Intelligent Operations Center. L'esecuzione di questo passo può richiedere fino a un'ora.

I messaggi vengono visualizzati indicando lo stato di avanzamento dell'installazione. I messaggi indicano lo stato del componente installato. Lo stato sarà uno dei seguenti:

[ OK ] Componente installato correttamente.

[ Fail ]

Installazione componente non riuscita.

## Risultati

L'applicazione IBM Intelligent Operations Center è installata correttamente quando tutti i messaggi terminano con stato [ OK ].

---

## Verifica dell'installazione

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

## Procedura

Avviare tutti i servizi.

1. Avviare tutti i servizi IBM Intelligent Operations Center eseguendo Strumento di controllo della piattaforma con il parametro **start all**.
2. Accertarsi che tutti i servizi siano stati avviati correttamente controllando i messaggi visualizzati.
3. Eseguire tutti i test nello strumento Controllo di verifica del sistema.
4. Accertarsi che tutti i test siano stati eseguiti correttamente.

Facoltativamente, arrestare e riavviare tutti i servizi.

5. Arrestare tutti i servizi IBM Intelligent Operations Center eseguendo Strumento di controllo della piattaforma con il parametro **stop all**.
6. Accertarsi che tutti i servizi siano stati arrestati correttamente controllando i messaggi visualizzati.
7. Arrestare il sistema operativo Linux su tutti i server.
8. Spegnerne e riaccendere tutti i server runtime oppure riavviare tutti i server.
9. Avviare tutti i servizi IBM Intelligent Operations Center eseguendo Strumento di controllo della piattaforma con il parametro **start all**.
10. Accertarsi che tutti i servizi siano stati avviati correttamente controllando i messaggi visualizzati.
11. Eseguire tutti i test nello strumento Controllo di verifica del sistema.
12. Accertarsi che tutti i test siano stati eseguiti correttamente.

## Operazioni successive

Se vengono rilevati degli errori, risolverli e rieseguire questa procedura.

**Concetti correlati:**

“Informazioni” a pagina 195

Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.

**Attività correlate:**

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager” a pagina 26

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Come utilizzare lo strumento Controllo di verifica del sistema” a pagina 210

Lo strumento Controllo di verifica del sistema viene utilizzato per determinare lo stato operativo di servizi compreso il sistema IBM Intelligent Operations Center.

---

## Configurazione post-installazione di IBM Intelligent Operations Center

Dopo l'installazione dell'architettura IBM Intelligent Operations Center utilizzando Installation Manager o la procedura guidata, è necessario eseguire diverse operazioni di configurazione post-installazione per completare l'installazione.

**Importante:** Tutte le attività di configurazione post-installazione devono essere eseguite prima che venga installato cyber hygiene.

**Attività correlate:**

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager” a pagina 26

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

## Configurazione dei servizi di collaborazione per IPv6

Se l'installazione utilizza reti IPv6, le operazioni di configurazione vengono richieste per i servizi di collaborazione.

### Informazioni su questa attività




L'architettura IBM Intelligent Operations Center deve essere installata prima di configurare la rete IPv6 per i servizi di collaborazione.

### Procedura

1. Seguire i passi nella documentazione Lotus Domino per configurare Lotus Domino per l'indirizzamento IPv6.
2. Seguire i passi nella documentazione Lotus Sametime Standard per configurare Lotus Sametime Standard per l'indirizzamento IPv6.
3. Seguire i passi nella documentazione WebSphere Portal per configurare l'attendibilità per il portlet Sametime Contact List se non si utilizza una rete IPv4 con un indirizzo IPv4 assegnato a server eventi.



## Informazioni correlate:

-  Configurazione di Lotus Domino per l'indirizzamento IPv6
-  Configurazione di Sametime Community Server per il supporto IPv6
-  Configurazione dell'attendibilità per il portlet Sametime Contact List

## Configurazione di SSO (Single Sign-On) per i servizi di collaborazione

Importare il token LTPA SSO di WebSphere Portal in server eventi per consentire agli utenti di accedere ai servizi di collaborazione senza dover immettere nuovamente le credenziali.

### Informazioni su questa attività

L'architettura IBM Intelligent Operations Center deve essere installata prima di importare il token LTPA (Lightweight Third-Party Authentication).

Questo token è stato creato durante l'installazione dell'architettura IBM Intelligent Operations Center.

### Procedura

1. Installare un client Lotus Notes 8.5.x su una workstation. È possibile utilizzare un'installazione esistente. La workstation deve essere in grado di collegarsi a server eventi su TCP/IP utilizzando il nome host completo.
2. Copiare il file `/opt/pdweb/etc/stproxy.ltpa` da server delle applicazioni nella workstation in cui viene eseguito Lotus Notes. Questo è il token LTPA che verrà importato nella directory del servizio di collaborazione.
3. Copiare il file `/local/notesdata/admin.id` da server eventi nella workstation in cui viene eseguito Lotus Notes. Questo è il file ID per l'amministratore del servizio di collaborazione. Si utilizzerà questo ID per accedere alla directory dei servizi di collaborazione.
4. Sulla workstation, avviare il client Lotus Notes e accedere al file `admin.id`.
  - a. Nel log Lotus Notes sul pannello, fare clic su **Nome utente**.
  - b. Spostarsi sulla directory in cui sono stati copiati il file `admin.id` e selezionarlo.
  - c. Immettere la password definita nel file delle proprietà della topologia per la proprietà `DOMINO.ADMIN.PWD`.
  - d. Fare clic su **Sì** se viene visualizzato un avviso di sicurezza.
5. Aprire il file `names.nsf`.
  - a. Fare clic su **File > Apri > Lotus Notes Application**.
  - b. Immettere il nome host completo di server eventi in **Cerca in**.
  - c. Immettere `names.nsf` in **Nome file**.
  - d. Fare clic su **Apri**.
6. Spostarsi su **Web > Configurazioni Web**.
7. Selezionare **Web SSO Configuration for LTPA token** e fare clic su **Modifica documento**.
8. Fare clic su **Keys > Import WebSphere LTPA Keys**. Fare clic su **OK** se si riceve un'avvertenza riguardante la sovrascrittura di chiavi esistenti.
9. Immettere il percorso in cui è stato copiato il file `stproxy.ltpa`. Fare clic su **OK**.
10. Immettere la password per il token LTPA. La password viene definita nella proprietà del file delle proprietà della topologia `WAS.LTPA.PWD`.
11. Fare clic su **OK > Salva e chiudi**.
12. Riavviare il servizio di collaborazione utilizzando Strumento di controllo della piattaforma.
  - a. Collegarsi a server di gestione e aprire una finestra di terminale.



- b. Eseguire `su -ibmadmin`.
- c. Eseguire `stop /opt/IBM/ISP/mgmt/scripts/IOControl.sh stop st password`, dove *password* è la password per Strumento di controllo della piattaforma definita quando Strumento di controllo della piattaforma è stato installato.
- d. Eseguire `/opt/IBM/ISP/mgmt/scripts/IOControl.sh start st password` dove *password* è la password per Strumento di controllo della piattaforma definita quando Strumento di controllo della piattaforma è stato installato.

## Impostazione del timeout della sessione

Il timeout della sessione determina il tempo in cui l'utente può restare inattivo prima che la sessione venga terminata, rendendo necessario un nuovo accesso dell'utente. Il timeout della sessione è valido anche per gli amministratori collegati tramite il servizio del portale.

### Informazioni su questa attività

Quando IBM Intelligent Operations Center è installato, non viene definito alcun timeout della sessione. Gli utenti rimarranno collegati fino alla loro disconnessione anche se la sessione è inattiva.

Se la propria organizzazione dispone di politiche di sicurezza che richiedono la disconnessione delle sessioni dopo un periodo di inattività, utilizzare la seguente procedura per definire un timeout della sessione per il proprio sistema IBM Intelligent Operations Center.

### Procedura

1. Mediante l'utilizzo di un browser Web accedere a `http://server_applicazioni:9060/ibm/console`, dove *server\_applicazioni* è il nome host di server delle applicazioni.
2. Accedere come utente `waswebadmin` con la password definita per `PORTAL.ADMIN.ACCOUNT.PWD` nel file delle proprietà della topologia.
3. Fare clic su **Server > Tipo di server > WebSphere Application Server > WebSphere Portal**.
4. Fare clic su **Impostazioni contenitore > Gestione sessioni > Imposta timeout**.
5. Immettere il valore di timeout desiderato in minuti.
6. Fare clic su **OK**.
7. Fare clic su **Salva**.
8. Fare clic su **Server > Tipo di server > WebSphere Application Server > STProxyServer1**.
9. Fare clic su **Impostazioni contenitore > Gestione sessioni > Imposta timeout**.
10. Immettere il valore di timeout desiderato in minuti.
11. Fare clic su **OK**.
12. Fare clic su **Salva**.
13. Fare clic su **Server > Tipo di server > WebSphere Application Server > CongnosX\_GW1**.
14. Fare clic su **Impostazioni contenitore > Gestione sessioni > Imposta timeout**.
15. Immettere il valore di timeout desiderato in minuti.
16. Fare clic su **OK**.
17. Fare clic su **Salva**.
18. Fare clic su **Server > Tipo di server > WebSphere Application Server > CongnosX\_Displ1**.
19. Fare clic su **Impostazioni contenitore > Gestione sessioni > Imposta timeout**.
20. Immettere il valore di timeout desiderato in minuti.
21. Fare clic su **OK**.
22. Fare clic su **Salva**.
23. Arrestare e riavviare server delle applicazioni

24. Su server delle applicazioni, collegarsi come utente `ibmadmin` con la password definita per `IOP.ADMIN.USER.PWD` nel file delle proprietà della topologia.
25. Eseguire il comando `sudo su -` per passare all'utente `root`.
26. Modificare il file `/opt/pdweb/etc/webseald-default.conf` con un editor di testo.
27. Nella sezione `SESSION CACHE SETTINGS` modificare il valore `timeout = 0` sul timeout di sessione desiderato in secondi. Il timeout deve essere uguale al tempo impostato per il servizio del portale. Tuttavia, il valore del portale è impostato in minuti e l'impostazione della cache di sessione è specificata in secondi. Il valore di timeout delle impostazioni della cache di sessione deve essere esattamente 60 volte il valore impostato per il servizio del portale. Ad esempio, se il valore del portale era 30 (minuti), il valore delle impostazioni delle cache di sessione deve essere 1800 (secondi).
28. Eseguire il comando `/usr/bin/pdweb restart` per riavviare il servizio di sicurezza.

## Installazione e configurazione di servizi di modelli semantici

IBM Intelligent Operations Center fornisce un'applicazione servizi di modelli semantici e un modello di esempio. Questo servizio deve essere installato e configurato prima dell'utilizzo.

### Configurazione di Jazz Team Server

Il IBM Intelligent Operations Center servizi di modelli semantici è installato su Jazz Team Server. È necessario configurare Jazz Team Server prima che siano installati i servizi di modelli semantici del IBM Intelligent Operations Center.

### Informazioni su questa attività

L'architettura IBM Intelligent Operations Center deve essere installata prima di configurare Jazz Team Server.

### Procedura

1. In un browser Web, passare a `http://management_host:82/jts/setup` dove `management_host` è il nome host completo del server di gestione.
2. Accedere con l'ID utente `iicsystemuser` e la password `passw0rd`.
3. Fare clic su **Avanti**.
4. Nella pagina Configura URI Pubblico, immettere un valore **Root URI pubblico** nel formato `https://management_host:9448/jts` e selezionare **Comprendo che una volta impostato l'URI pubblico non può essere modificato**. Fare clic su **Avanti**.
5. Fare clic su **Verifica connessione**. Viene visualizzato un messaggio che indica che la verifica della configurazione ha avuto esito positivo.
6. Fare clic su **Avanti** per salvare le impostazioni e continuare.
7. Configurare il database nella pagina Configura database.
  - a. Selezionare **DB2 per Fornitore database**.
  - b. Selezionare **JDBC per Tipo di connessione**.
  - c. Immettere la password del database DB2 definita come proprietà `DEFAULT.PWD.DB2` nel file delle proprietà della topologia per **Password JDBC**. Ignorare il messaggio relativo alla password visualizzato.
  - d. Per **Ubicazione JDBC** immettere `//db_host:50005/JTS:user=db2inst5;password={password}`; dove `db_host` è il nome host del server di dati. La stringa `{password}` deve essere immessa nel modo indicato. Non sostituire con il valore della password.
  - e. Fare clic su **Verifica connessione**. Se si verifica un errore, controllare e correggere le voci. Se le voci sono corrette, verificare che i servizi database siano avviati sul server di dati utilizzando lo Strumento di controllo della piattaforma.

- f. Dopo la visualizzazione di un messaggio che informa che non sono presenti tabelle Jazz nel database, fare clic su **Crea tabelle**. Il completamento dell'elaborazione richiederà alcuni minuti.
- g. Fare clic su **Avanti**.
8. Nella pagina Abilita notifica email, impostare il valore su **Disabilitato** e fare clic su **Avanti**.
9. Nella pagina Registra applicazioni dovrebbe essere visualizzato il messaggio "Nessuna nuova applicazione rilevata". Fare clic su **Avanti**.
10. Selezionare **LDAP** per **Tipo di registro utente** nel passo 1 della pagina Configura registro utente.
11. Al Passo 2 configurare LDAP per il registro di Jazz Team Server.
  - a. Immettere `ldap://mgmt_host:389` per **Ubicazione registro LDAP** dove *mgmt\_host* è il nome host completo del server di gestione.
  - b. Immettere `OU=USERS,OU=SWG,O=IBM,C=US` per **DN utente base**.
  - c. Immettere `userId=uid,name=cn,emailAddress=mail` per **Associazione nomi proprietà utente**.
  - d. Immettere `OU=GROUPS,OU=SWG,O=IBM,C=US` per **DN gruppo base**.
  - e. Per **Associazione gruppo Jazz-LDAP**, verificare che il valore sia impostato su `JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDWAdmins=JazzDWAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests`.
  - f. Immettere `cn` per **Proprietà nome gruppo**.
  - g. Immettere `cn` per **Proprietà membro gruppo**.
12. Fare clic su **Verifica connessione**. Se viene visualizzato un messaggio di avvertenza, fare clic su **Mostra dettagli**. Se il messaggio di avvertenza fa riferimento alla proprietà `mail`, è possibile ignorarlo.
13. Per **Tipo di licenza accesso client**, selezionare **IBM Integrated Information Core - IIC Model Server**.
14. Fare clic su **Avanti**.
15. Per **Configura Data Warehouse**, selezionare la casella di spunta **Non desidero configurare il data warehouse in questo momento**.
16. Fare clic su **Fine** nella pagina Riepilogo.

## Risultati

Jazz Team Server è operativo.

## Installazione di servizi di modelli semantici

servizi di modelli semantici e un'applicazione di esempio vengono forniti con IBM Intelligent Operations Center.

## Informazioni su questa attività

La configurazione di Jazz Team Server in server di gestione è obbligatoria prima di utilizzare servizi di modelli semantici.

## Procedura

1. In un browser Web, andare all'indirizzo `http://management_host:82/jts/admin` dove *management\_host* è il nome host completo di server di gestione.
2. Nella pagina Server di gestione, fare clic su **Server > Configurazione > Registrazione applicazioni**.
3. Fare clic su **Aggiungi** nella pagina Applicazioni registrate.
4. Aggiungere l'applicazione del server modello nella pagina Aggiungi applicazione.
  - a. Immettere Server modello per **Nome applicazione**.
  - b. Immettere `http://management_host:82/modelserver/scr`, dove *management\_host* è il nome host completo di server di gestione, per **Rilevamento URL**.

- c. Immettere un valore di propria scelta per **segreto consumer**. Questo valore verrà utilizzato per fornire l'accesso all'applicazione. Il valore deve essere trattato con la stessa sicurezza della password.
- d. Immettere `iicsystemuser` per **ID funzionale**

Il **Tipo di applicazione** verrà modificato in Server modello.

- 5. Se non vi sono errori, fare clic su **Fine**.

## Verifica della configurazione servizi di modelli semantici

Un esempio dell'applicazione servizi di modelli semantici viene fornito con IBM Intelligent Operations Center e può essere utilizzato per verificare la corretta installazione e configurazione di servizi di modelli semantici.

### Procedura

1. Preparare i file del modello di esempio.
  - a. In server di installazione trovare il file `iic15_2_stagebuiltdoserver.xx.jar` nella directory `install_media`.
  - b. Espandere il file `iic15_2_stagebuiltdoserver.xx.jar` in una directory di propria scelta. Nella parte rimanente di questa procedura, questa directory viene indicata come `model_home`.
2. Installare il modello di esempio.
  - a. In un browser Web sul server in cui si trova `model_home`, andare all'indirizzo `http://mgmt_host:82/iic/console` dove `mgmt_host` è il nome host completo di server di gestione.
  - b. Collegarsi come utente `iicsystemuser` con `passwd` come password.
  - c. Fare clic su **Gestore modello > ontologie > Sfoglia**.
  - d. Spostarsi nella directory `install_media/ioc/image/IIC/install/modelServices/post_install/`.
  - e. Aprire il file `rsm.owl`.
  - f. Fare clic su **Carica**. Il file viene caricato.
  - g. Fare clic su **Gestore modello > ontologie > Sfoglia**.
  - h. Spostarsi nella directory `install_media/ioc/image/IIC/install/modelServices/post_install/`.
  - i. Aprire il file `modelServer.owl`.
  - j. Fare clic su **Carica**. Il file viene caricato.
  - k. Fare clic su **Gestore modello > ontologie > Sfoglia**.
  - l. Spostarsi nella directory `install_media/ioc/image/IIC/install/ktpRuntimeServices/post_install/`.
  - m. Aprire il file `kpi.owl`.
  - n. Fare clic su **Carica**. Il file viene caricato.
  - o. Fare clic su **Gestore modello > Carica > Sfoglia**
  - p. Spostarsi nella directory `install_media/ioc/image/IIC/samples/rdf/rsm/`.
  - q. Aprire il file `IBMOilDownstreamSampleRDF.xml`.
  - r. Fare clic su **Carica**. Il file viene caricato.
  - s. Fare clic su **Gestore modello > Carica > Sfoglia**
  - t. Spostarsi nella directory `install_media/ioc/image/IIC/samples/rdf/rsm/`.
  - u. Aprire il file `IBMOilUpstreamSampleRDF.xml`.
  - v. Fare clic su **Carica**. Il file viene caricato.
  - w. Fare clic su **Gestore modello > Carica > Sfoglia**
  - x. Spostarsi nella directory `install_media/ioc/image/IIC/samples/rdf/rsm/`.
  - y. Aprire il file `IBMOilDownstreamSampleReferenceRDF.xml`.
  - z. Fare clic su **Carica**. Il file viene caricato.

- aa. Fare clic su **Gestore modello > Carica > Sfoglia**
  - ab. Spostarsi nella directory `install_media/ioc/image/IIC/samples/rdf/rsm/`.
  - ac. Aprire il file `IBMOilUpstreamSampleReferenceRDF.xml`.
  - ad. Fare clic su **Carica**. Il file viene caricato.
3. Verificare ce il modello di esempio sia installato correttamente.
    - a. Fare clic su **Gestore modello > Query > Query**. Una query predefinita verrà eseguita. Una struttura XML verrà visualizzato con i risultati della query. La tag di livello superiore deve essere `spargl` e avere le tag secondarie `head` e `results`.
    - b. Fare clic su **Esplora modelli** ed assicurarsi che sia possibile sfogliare il modello.
  4. Utilizzare il modello per verificare l'installazione di gestore modello.
    - a. In un browser Web in server di gestione, andare all'indirizzo `http://mgmt_host:82/iic/ibmoil` dove `mgmt_host` è il nome host completo di server di gestione.
    - b. Fare clic su **IBM Oil Company > Variabili**. Vengono visualizzati gli URL del servizio Web.

## Risultati

servizi di modelli semantici e il modello di esempio IBMOil vengono installati.

## Miglioramento delle prestazioni di servizi di modelli semantici

Configurare servizi di modelli semantici fornito da IBM Intelligent Operations Center per migliorare le prestazioni quando si eseguono query sui modelli.

## Procedura

1. In un browser Web passare a `http://host_gestione:82/iic/console` dove `host_gestione` è il nome host completo di server di gestione.
2. Aggiungere i valori delle proprietà in Tabella 20 alla categoria **OPCWEBSERVICE**.

Tabella 20. Proprietà OPCWEBSERVICE

Proprietà	Valore
<code>cache.browse.timetolive.second</code>	3600
<code>cache.timetolive.second</code>	2592000
<code>cache.wait.second.after.create.action</code>	1

3. Aggiornare o aggiungere le seguenti proprietà e valori in Tabella 21 alla categoria RSM.

Tabella 21. Proprietà RSM

Proprietà	Valore
<code>mvmViewPath.0</code>	<code>http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue</code>

Tabella 21. Proprietà RSM (Continua)

Proprietà	Valore
mvmViewPath.1	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue
mvmDownLevelPreRequest	3
mvmCacheProperty.0	cim:RSM_IdentifiedObject.name
mvmMaxQueryURI	500
mvmMaxSparqlEntry	4000

4. Fare clic su **Pubblica**. Le proprietà nuove e modificate verranno salvate.
5. Riavviare servizi di modelli semantici using the Strumento di controllo della piattaforma.
6. In un browser Web passare a `http://host_gestione:82/iic/console` dove `host_gestione` è il nome host completo di server di gestione.
7. Apportare le modifiche specifiche dell'applicazione o alla soluzione in base alle necessità. Se sono richieste modifiche, esse verranno identificate nel prodotto o nella documentazione della soluzione.

## Configurazione di Strumento di controllo della piattaforma

Dopo l'installazione di IBM Intelligent Operations Center, se è stato installato un Java JRE diverso da quello fornito con IBM Intelligent Operations Center, è necessario definire l'ubicazione JRE utilizzata da Strumento di controllo della piattaforma.

### Procedura

1. server di gestione, modificare il file `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh`.
2. Modificare `export JAVA_HOME=` con l'ubicazione di Java JRE.
3. Salvare le modifiche.
4. In server di gestione, modificare il file `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh`.
5. Modificare `export JAVA_HOME=` con l'ubicazione di Java JRE.
6. Salvare le modifiche.

### Attività correlate:

“Installazione di JRE (Java runtime environment)” a pagina 26

L'ambiente runtime Java 6 deve essere installato sul server di installazione prima di installare IBM Intelligent Operations Center.

## Codifica della password di gestione di Tivoli Service Request Manager

Utilizzare la seguente procedura per codificare la password di gestione di Tivoli Service Request Manager in Tivoli Netcool/Impact.

### Procedura

1. Collegarsi alla console di gestione di Tivoli Netcool/Impact all'indirizzo `http://event_host:9080/nci/main` dove `event_host` è il nome host di server eventi. Accedere come utente `admin` con la password `netcool`.



2. Fare clic su **Progetto IOC**.
3. Nella sezione Politiche, fare doppio clic sulla politica **IOC\_Sample\_Password\_Encoder**. La politica viene aperta nella finestra Editor politiche.
4. Nel campo **Immettere la password**, immettere la password per Maxadmin. La password Maxadmin è la password utente di gestione immessa durante l'installazione.
5. Per salvare la politica, fare clic su **Salva**.
6. Fare clic sull'icona **Attiva politica**.
7. Fare clic su **Esegui**.
8. Nella sezione Stato servizio, scorrere su **PolicyLogger**, fare clic su **Visualizza log per PolicyLogger** (icona con la freccia in basso).
9. Nella finestra Policy Logger, individuare l'istruzione simile a quella riportata di seguito:  

```
11 May 2012 14:19:12,260: [IOC_Sample_Password_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
```
10. Copiare la password codificata **Maxadmin** dall'istruzione, ad esempio:  

```
{aes}FF877B74ADF4DF1C2002F94ACB38FAFF
```
11. Nella console di gestione Tivoli Netcool/Impact, nella sezione Politiche, fare doppio clic sulla politica **UTILS\_LIBRARY\_IOC\_TSRM**. La politica viene aperta nella finestra Editor politiche.
12. Sostituire il valore di `MAXAdminPassword` con il valore codificato che viene copiato nel passo 10:  

```
MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";
```
13. Per salvare la politica, fare clic su **Salva**.
14. Fare clic su **Progetto IOC**.
15. Nella sezione Politiche, fare doppio clic sulla politica **IOC\_Sample\_Password\_Encoder**. La politica viene aperta nella finestra Editor politiche.
16. Nel campo **Immettere la password**, cancellare la password per **Maxadmin**.
17. Per salvare la politica, fare clic su **Salva**.

## Impostazione del numero minimo di processi per EventProcessor

Il numero minimo di processi per EventProcessor deve essere impostato su 25 per motivi legati alle prestazioni.

### Procedura

1. Collegarsi alla console di gestione di Tivoli Netcool/Impact all'indirizzo `http://event_host:9080/nci/main` dove `event_host` è il nome host di server eventi.
2. Fare clic su **Stato servizio > EventProcessor**.
3. Specificare 25 per **Numero minimo di processi**.

**Nota:** Il valore di **Numero minimo di processi** non può essere superiore al valore di **Numero massimo di processi**.

4. Fare clic su **OK**.
5. Fare clic sull'icona **Arresta processo** per arrestare EventProcessor.
6. Fare clic sull'icona **Avvia processo** per avviare EventProcessor.

## Modifica della dimensione del pool di thread predefinito e WebContainer

È necessario modificare le impostazioni della dimensione del pool di thread Predefinito e WebContainer per migliorare le prestazioni delle procedure operative standard.

### Procedura

1. Sul server eventi in nell'interfaccia di gestione WebSphere Portal fare clic su **Intelligent Operations > Strumenti di amministrazione > Console di gestione**.

2. In Server eventi, fare clic su **Server delle applicazioni SOP (Standard Operating Procedure)**.
3. Accedere a WebSphere Application Server come amministratore. L'ID utente è stato definito nella proprietà WAS.ADMIN.ACCOUNT e la password è stata definita nella proprietà WAS.ADMIN.ACCOUNT.PWD nel file delle proprietà topologia quando è stato installato IBM Intelligent Operations Center.
4. Fare clic su **Server > Server delle applicazioni > MXServer1 > Pool thread > WebContainer**.
5. Immettere 50 per la **Dimensione minima**.
6. Immettere 50 per la **Dimensione massima**.
7. Fare clic su **OK**.
8. Fare clic su **Server > Server delle applicazioni > MXServer1 > Pool di thread > Predefinito**.
9. immettere 20 per la **Dimensione minima**.
10. Immettere 50 per la **Dimensione massima**.
11. Fare clic su **OK**.
12. Riavviare TSRCcluster.
  - a. Fare clic su **Server > Cluster**.
  - b. Selezionare TSRCcluster.
  - c. Fare clic su **Arresta**.
  - d. Attendere che lo stato diventi rosso.
  - e. Fare clic su **Avvia**.

---

## Installazione ed esecuzione guidata di cyber hygiene

Cyber hygiene viene installato ed eseguito separatamente da IBM Intelligent Operations Center e deve essere installato ed eseguito dopo che tutti gli altri componenti di IBM Intelligent Operations Center sono stati installati, configurati e operativi. Cyber hygiene modifica la configurazione del sistema operativo predefinito con un insieme più sicuro di opzioni che consentono di assicurare una base più sicura al sistema IBM Intelligent Operations Center.

### Prima di iniziare

**Nota:** Cyber hygiene viene installato ed eseguito nella stessa fase. Se si installa IBM Intelligent Operations Center utilizzando IBM Installation Manager, non utilizzare questa procedura. L'installazione di IBM Installation Manager fornisce un'opzione per installare ed eseguire cyber hygiene.

Per ridurre il tempo in cui cyber hygiene esegue le scansioni e riparazioni, smontare qualsiasi file system che non deve essere valutato per la sicurezza. Ad esempio, le directory *install\_media* in ciascun server possono essere eliminate dopo che tutte le operazioni di installazione sono state completate. Queste directory possono essere eliminate o smontate prima di eseguire cyber hygiene.

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

### Informazioni su questa attività

Cyber hygiene deve essere l'ultima operazione dopo l'installazione del IBM Intelligent Operations Center. La scansione e le soluzioni sulle vulnerabilità della sicurezza della configurazione dell'indirizzo che esistono dopo che il sistema operativo predefinito e il prodotto IBM Intelligent Operations Center vengono installati. Le soluzioni applicate sono state verificate per confermare che i servizi IBM Intelligent Operations Center funzioneranno correttamente.

Le modifiche applicate al sistema da cyber hygiene possono causare problemi con altre applicazioni e soluzioni. Ad esempio, le altre applicazioni e soluzioni potrebbero avere requisiti sull'ambiente Linux che non sono in sintonia con le buone pratiche sulla sicurezza. Un'applicazione o soluzione potrebbe



richiedere l'accesso al sistema come utente root per essere installato o eseguito. In questo caso alcune delle modifiche cyber hygiene potrebbe essere temporaneamente o permanentemente cambiate o un'altra soluzione trovata dal fornitore dell'applicazione o soluzione.

Una volta che le modifiche a cyber hygiene vengono apportate, non vi è alcun metodo automatizzato per modificarle. Tutte le modifiche devono essere apportate tramite aggiornamenti manuali al sistema operativo Linux o modificando le autorizzazioni del file o della directory.

## Procedura

1. In server di installazione aprire una finestra di terminale e collegarsi come root. Se non si è collegati come root, passare all'account root eseguendo il comando `su -`.
2. Eseguire il comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`. La variabile `JAVA_HOME` è impostata su JRE (Java runtime environment).
3. Passare alla directory `install_home/ch/install`.
4. Modificare il file `iop-ch-install.xml` utilizzando un editor di testo.
5. Sostituire i parametri nel file `iop-ch-install.xml` con i valori appropriati per l'installazione.

Tabella 22. Parametri di installazione di Cyber hygiene

Parametro	Valore
<code>\${APP.1.HOST}</code>	Il nome host completo di server delle applicazioni
<code>\${APP.1.ACCT}</code>	Il nome utente Linux per l'accesso SSH a server delle applicazioni
<code>\${APP.1.ACCT.PWD}</code>	La password per <code>\${APP.1.ACCT}</code>
<code>\${APP.1.SSH_PORT}</code>	La porta SSH server delle applicazioni
<code>\${DB.1.HOST}</code>	Il nome host completo di server di dati
<code>\${DB.1.ACCT}</code>	Il nome utente Linux per l'accesso SSH a server di dati
<code>\${DB.1.ACCT.PWD}</code>	La password per <code>\${DB.1.ACCT}</code>
<code>\${DB.1.SSH_PORT}</code>	La porta SSH server di dati
<code>\${EVENT.1.HOST}</code>	Il nome host completo di server eventi
<code>\${EVENT.1.ACCT}</code>	Il nome utente Linux per l'accesso SSH a server eventi
<code>\${EVENT.1.ACCT.PWD}</code>	La password per <code>\${EVENT.1.ACCT}</code>
<code>\${EVENT.1.SSH_PORT}</code>	La porta SSH server eventi
<code>\${MGMT.1.HOST}</code>	Il nome host completo di server di gestione
<code>\${MGMT.1.ACCT}</code>	Il nome utente Linux per l'accesso SSH a server di gestione
<code>\${MGMT.1.ACCT.PWD}</code>	La password per <code>\${MGMT.1.ACCT}</code>
<code>\${MGMT.1.SSH_PORT}</code>	La porta SSH server di gestione

6. Salvare il file.
7. Passare alla directory `install_home/ch`.
8. Eseguire il comando `install_home/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d install_media/ioc/image -p GRUB_password`, dove `GRUB_password` è la password per il bootloader GRUB sui server. `GRUB_password` verrà applicata a tutti i server di destinazione. Normalmente, quando i server vengono riavviati, non viene richiesta alcuna password. Tuttavia, una volta cyber hygiene è installato, se si avvia un server con qualunque opzione Linux, come ad esempio l'avvio in modalità utente singolo, `GRUB_password` dovrà essere immessa sulla console del server.

## Risultati

Il tempo di elaborazione è determinato dalla velocità dell'hardware e se ci sono file supplementari, non necessari sui server di destinazione. L'elaborazione può durare fino a 1,5 ore. Durante tale periodo i server di destinazione verranno sottoposti a scansione e la soluzione appropriata verrà applicata.

## Operazioni successive

Controllare il file di log cyber hygiene per eventuali errori. I log mostreranno anche le soluzioni applicate e i passi manuali facoltativi.

### Concetti correlati:

“Panoramica su cyber hygiene” a pagina 81

La funzione cyber hygiene di IBM Intelligent Operations Center è progettata per fornire servizi che pongano rimedio a potenziali rischi nella sicurezza nel sistema installato.

## Modifiche al sistema operativo Linux

Cyber hygiene esegue la scansione del sistema operativo Linux per i rischi noti sulla sicurezza e rende le modifiche appropriate. I log descrivono le vulnerabilità sottoposte a scansione e le modifiche apportate alle impostazioni e politiche del sistema operativo Linux.

I log elencano anche i rischi che sono stati rilevati e dove non sono state apportate modifiche. Questi rischi possono includere:

- Il sistema è già configurato nel modo in cui cyber hygiene lo avrebbe modificato.
- La modifica richiede che un amministratore di sistema intraprenda un'azione o decida se la modifica sia appropriata per l'ambiente.
- La modifica non può essere effettuata da uno script automatizzata. Ad esempio, il rischio relativo alle politiche di sicurezza generali dell'organizzazione.

Qualsiasi soluzione applicata da cyber hygiene può essere modificata successivamente se necessario. I log di cyber hygiene forniscono informazioni sulle modifiche applicate al sistema. Le modifiche potrebbero essere richieste per utilizzare il sistema con altre applicazioni o soluzioni se le modifiche apportate da cyber hygiene sono incompatibili con tali sistemi.

## Controllare il log cyber hygiene

Dopo aver installato ed eseguito cyber hygiene, esaminare il log per conoscere le modifiche apportate al sistema e qualsiasi altro rischio.

## Informazioni su questa attività

Su server di installazione, passare alla directory in cui è stato copiato il package di installazione di IBM Intelligent Operations Center. Durante questa procedura, tale directory viene indicata come *install\_home*.

## Procedura

1. Esaminare il log cyber hygiene nella directory `/var/ibm/InstallationManager/logs/native` in server di installazione per garantire che tutte le azioni sono state eseguite su tutti i server. È possibile trovare il log eseguendo il comando **fgrep yber \*.log**. Il file di log visualizzerà le informazioni per ciascun server. In generale la procedura con le informazioni di log include:
  - Preparazione dell'ambiente per eseguire le attività cyber hygiene.
  - Esecuzione del remediator autonomo. Questo consente di correggere le vulnerabilità che non richiedono scansione. Ad esempio, l'impostazione di una password bootloader GRUB e il passaggio alla verifica.
  - Disabilitazione dell'accesso root remoto.

- Scansione delle vulnerabilità. Vengono eseguite in background e le attività principali attendono che la scansione venga completata.
  - Esecuzione di remediator per affrontare le vulnerabilità rilevate durante la scansione.
  - Scansione dopo la soluzione. Ciò identifica le vulnerabilità non trovate durante la scansione iniziale.
  - Esecuzione di remediator per affrontare le vulnerabilità rilevate durante la seconda scansione. Le soluzioni non completate vengono registrate.
2. Esaminare i log di cyber hygiene dettagliati che si trovano nella directory `/var/BA15/CH/results` su ognuno dei server di destinazione. `standrem-date_time.log` mostra i risultati del remediator autonomo. `standrem-disableRemoteRoot-date_time.log` mostra il risultato della disabilitazione dell'accesso remoto su root. `scanrem-combined-log-date_time.log` mostra i risultati delle azioni sottoposte a scansione dal remediator. Esistono due log per le due operazioni di scansione/soluzione.
    - a. Rivedere i file di log per le righe che iniziano con il testo `Vulnerabilità`. Ogni riga indica l'azione intrapresa e include:
      - I risultati della scansione.
      - Le soluzioni selezionate.
      - I dettagli sulle soluzioni applicate.
    - b. Nel log per la seconda scansione e soluzione, le soluzioni annotate con il testo `NOT DONE` dovrebbero essere esaminate per ulteriori azioni manuali.

## Nuova abilitazione accesso root remoto

Cyber hygiene disabilita l'accesso remoto all'account root mediante il comando `ssh`. I comandi `telnet` e `rsh` sono completamente disabilitati nel sistema operativo Linux. Se necessario, è possibile riabilitare l'accesso remoto.

### Informazioni su questa attività

Una nuova abilitazione dell'accesso remoto per l'utente root potrebbe non essere richiesta. Un utente con i privilegi appropriati può utilizzare i comandi `su` e `sudo` per operare come utente root. Gli utenti con privilegi che operano come utente root sono collegati per finalità di controllo.

IBM Intelligent Operations Center definisce l'utente `ibmadmin` nel gruppo `wheel`. Gli utenti nel gruppo `wheel` possono utilizzare il comando `sudo su -` da eseguire come root.

### Procedura

Effettuare quanto segue per abilitare l'accesso root utilizzando il comando `ssh`.

1. Modificare il file `/etc/ssh/sshd_config` sul server in cui si richiede l'accesso remoto come root utilizzando `ssh` o un terminale remoto.
2. Modificare il parametro `PermitRootLogin` su `yes` e salvare il file. Modificare questo parametro su `no` se il login remoto che utilizza il comando `ssh` deve essere disabilitato.
3. Salvare il file.
4. Riavviare il servizio `ssh` eseguendo il comando `service sshd restart`.

L'accesso remoto all'account root utilizzando terminali remoti è disabilitato da cyber hygiene. Solo lo schermo e la tastiera fisicamente collegati al server possono collegarsi come utente root. Effettuare quanto segue per abilitare nuovamente l'accesso root remoto su un server da un terminale remoto.

5. Modificare il file `/etc/securetty` sul server in cui si richiede l'accesso remoto come root utilizzando `ssh` o un terminale remoto.
6. Aggiungere i nomi dispositivo Linux per i terminali autorizzati a collegarsi in remoto come utente root. Ad esempio, se si desidera aggiungere `tty1`, modificare l'elenco affinché venga visualizzato:
 

```
console
tty1
```

Per disabilitare un terminare, inserire il carattere # prima del terminale che occorre disabilitare. Ad esempio:

```
console  
#ttyl
```

7. Salvare il file.

---

## Configurazione di utenti che richiedono accesso ssh

IBM Intelligent Operations Center richiede che determinati utenti siano configurati con accesso ssh e password.

### Informazioni su questa attività

I seguenti utenti devono essere configurati in server di installazione ed in tutti i server di destinazione per avere accesso ssh e le password.

- ibmadmin
- ibmuser
- mqconn

---

## Strumenti di installazione forniti con la soluzione

Toolkit e strumenti di sviluppo sono inclusi con il IBM Intelligent Operations Center. Questi sono utilizzati quando si personalizza il IBM Intelligent Operations Center.

Ad eccezione di Rational Application Developer, sono forniti sul DVD o immagine di Toolkit Developer IBM Intelligent Operations Center Rational Application Developer è incluso con il IBM Intelligent Operations Center su separati DVD o immagini.

### Lotus Sametime Client

Per le informazioni sull'installazione ed utilizzo di Lotus Sametime Client , consultare Lotus Domino e il centro informazioni Lotus Notes.

### WebSphere Message Broker Toolkit

Per le informazioni sull'installazione ed utilizzo del Toolkit WebSphere Message Broker, consultare il centro informazioni WebSphere Message Broker.

### Development Toolkit IBM WebSphere Business Monitor

Per informazioni sull'installazione ed utilizzo del Development Toolkit IBM WebSphere Business Monitor, consultare il centro informazioni IBM WebSphere Business Monitor.

### Rational Application Developer





Per le informazioni sull'installazione ed utilizzo di Rational Application Developer, consultare il centro informazioni Rational Application Developer.

### Concetti correlati:

“Creazione ed integrazione dei KPI” a pagina 109

I modelli KPI (Key performance indicator) possono essere creati e modificati utilizzando un toolkit di sviluppo del monitoraggio di business e un portlet di gestione KPI.

### Informazioni correlate:

-  Centro informazione Lotus Domino e Lotus Notes
-  Centro informazione WebSphere Message Broker
-  Centro informazione IBM Business Monitor
-  Centro informazione Rational Application Developer

---

## Eliminazione di utenti di esempio

IBM Intelligent Operations Center viene fornito con utenti di esempio. Per motivi legati alla sicurezza, questi utenti devono essere cancellati dopo che IBM Intelligent Operations Center è stato installato nel proprio ambiente di produzione.

### Informazioni su questa attività

Per eliminare gli utenti predefiniti, completare la seguente procedura:

#### Procedura

1. Su server delle applicazioni, accedere a WebSphere Portal.
2. Nel portale di **amministrazione**, fare clic su **Accesso > Utenti e gruppi > Tutti gli utenti autenticati del portale**.
3. Fare clic sull'icona di eliminazione per i seguenti utenti:
  - tdelorne
  - scollins
  - akelly

**Importante:** Non cancellare i seguenti utenti obbligatori. Se vengono cancellati, IBM Intelligent Operations Center non funzionerà correttamente.

- admin
- iicsystemuser
- maxadmin
- maxintadm
- maxreg
- notesadmin
- resAdmin1
- resDeployer1
- resMonitor1
- rtsAdmin
- rtsConfig
- rtsUser
- taiuser
- SRMSELFSERVICEUSR
- wasadmin

- waswebadmin
- wpsadmin
- wpsbind
- Tutti gli ID utente che iniziano con "PM"

**Riferimenti correlati:**

“Utenti di esempio” a pagina 71

Durante la distribuzione di IBM Intelligent Operations Center, vengono creati utenti di esempio.

---

## Rimozione dei servizi di installazione dal sistema di produzione

Dopo l'installazione di IBM Intelligent Operations Center i servizi di installazione possono essere rimossi dai server del sistema di produzione. E' preferibile non cancellare il server di installazione poiché alcuni suoi servizi potrebbero essere richiesti per le attività di manutenzione.

Dopo aver completato l'installazione ed averla verificata, i componenti che vengono utilizzati solo nel processo di installazione possono essere rimossi dai server del sistema di produzione. (server delle applicazioni, server eventi, server di gestione, server di dati). Questi servizi includono:

- La directory definita dalla proprietà `Unix.image.basedir.remote` nel file delle proprietà della topologia.
- La directory definita dalla proprietà `Unix.script.basedir.remote` nel file delle proprietà della topologia.
- La directory `install_media`, definita dalla proprietà `image.basedir.local` nel file delle proprietà della topologia.

**Nota:** Si consiglia di non eliminare il server di installazione perché potrebbe essere utile in futuro. Poiché il file delle proprietà della topologia contiene le password in testo non codificato, questo server deve essere ubicato in una posizione sicura.

**Attività correlate:**

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager” a pagina 26

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

---

## Capitolo 3. Protezione della soluzione

La sicurezza è importante all'interno di IBM Intelligent Operations Center poiché la soluzione è fondamentale per operazioni essenziali. Per garantire la sicurezza, è importante conoscere le impostazioni predefinite e gestire gli utenti della soluzione per fornire a tutti gli utenti il corretto livello di accesso.

### Password predefinite

La prima attività per la protezione della soluzione è accertarsi che vengano cambiate tutte le password predefinite. Per ulteriori informazioni sulle password predefinite, vedere il link alla fine dell'argomento.

### Connessione sicura

IBM Intelligent Operations Center è abilitato a HTTPS per impostazione predefinita. È possibile modificare le impostazioni HTTPS per i seguenti singoli servizi all'interno di IBM Intelligent Operations Center:

- Il servizio di monitoraggio del business che elabora i KPI
- Il servizio di risorsa e di amministrazione della procedura operativa standard

Qualsiasi modifica all'impostazione HTTPS di un singolo servizio deve essere accompagnata da un aggiornamento alla corrispondente impostazione della porta. Per ulteriori dettagli sulla modifica di queste impostazioni nella tabella proprietà di sistema, vedere il link alla fine dell'argomento

### Autenticazione dell'utente

L'autenticazione dell'utente è associata ai diritti di autorizzazione che forniscono all'utente l'accesso alle funzioni e ai dati appropriati. IBM Intelligent Operations Center supporta l'integrazione all'infrastruttura di sicurezza esistente per il single sign-on.

Le autorizzazioni utente di IBM Intelligent Operations Center vengono gestite tramite gli utenti e i gruppi di WebSphere Portal. WebSphere Portal utilizza il database LDAP (Lightweight Directory Access Protocol) fornito da Tivoli Directory Server in esecuzione sul server di dati.

Il sistema di sicurezza fornito con IBM Intelligent Operations Center può contenere molti gruppi di utenti, ruoli e autorizzazioni. La sistemazione di molti gruppi di utenti, ruoli e autorizzazioni può portare ad un regime di sicurezza difficile da gestire. Si consiglia agli amministratori di limitare il numero di gruppi e autorizzazioni.

### Ruoli utente e autorizzazioni

L'appartenenza ad un gruppo di utenti basato sul ruolo fornisce a IBM Intelligent Operations Center un modo per controllare l'accesso. Gli utenti di un gruppo hanno accesso solo alle funzioni della soluzione corrispondenti al loro ruolo. Essere membri di un gruppo di utenti basato sul ruolo inoltre aiuta gli utenti a concentrare l'attenzione sulle attività appropriate. I ruoli standard sono: Esecutivo, Supervisore e Operatore.

Per aggiungere un utente a the IBM Intelligent Operations Center:

1. Scegliere un gruppo appropriato al ruolo dell'utente nell'organizzazione e rendere l'utente membro di quel gruppo.
2. Completare un profilo per l'utente e includere almeno l'ID utente, il nome e la password.

## Categorie di dati e autorizzazioni

La sicurezza dei dati memorizzati nei database in IBM Intelligent Operations Center viene gestita implementando l'accesso ai database basato sul ruolo. L'accesso ad una funzione di IBM Intelligent Operations Center non significa che tutti i dati siano disponibili per l'utente. La sicurezza dei dati viene applicata a livello di server per accertarsi che gli utenti vedano solo i dati appropriati. Le categorie standard sono: Geofisico, Trasporto, Meteorologico Ambientale, Infrastruttura, Chimico, Biologico, Incolumità, Sicurezza, Salvataggio, Incendio, Salute ed Altro.

## Portale

Il servizio del portale fornisce una piattaforma che può essere modificata in scala per sistemare la serie di utenti richiesta. Fornisce inoltre l'accesso basato sul ruolo che può essere regolato per riflettere la struttura organizzativa richiesta. È possibile visualizzare, creare ed eliminare utenti o gruppi di utenti con il portlet **Gestisci utenti e gruppi**. È possibile inoltre modificare le appartenenze ai gruppi. Per ulteriori informazioni su questo portlet, vedere il link alla fine di questo argomento.

### Concetti correlati:

“Informazioni sulla password” a pagina 39

Le password per i diversi ID utente nella soluzione IBM Intelligent Operations Center sono definite nel file delle proprietà della topologia. Per motivi di sicurezza le password predefinite fornite con IBM Intelligent Operations Center devono essere modificate.

### Informazioni correlate:

 Documentazione del prodotto IBM WebSphere Portal 7

---

## Ruoli utente e accesso

IBM Intelligent Operations Center implementa la sicurezza limitando l'accesso alle funzioni in base ai ruoli utente.

Per utilizzare una specifica funzione di IBM Intelligent Operations Center, un utente deve essere membro del gruppo di ruolo utente che fornisce l'accesso richiesto a quella funzione. Un utente viene reso membro di un gruppo di ruolo utente da un amministratore. La seguente tabella mostra in che modo i ruoli della vita reale possono essere associati ai gruppi di ruoli utente con livelli di accesso con login in IBM Intelligent Operations Center.

Tabella 23. Ruoli lavorativi e gruppi di ruoli utente di IBM Intelligent Operations Center

Ruolo lavorativo	Responsabilità	Gruppo di ruolo utente
Esecutivo	<ul style="list-style-type: none"><li>Definisce le soglie e i requisiti di input di eventi, incidenti e KPI (key performance indicator)</li><li>Visualizza riepiloghi visivi, dettagli e report di livello elevato di:<ul style="list-style-type: none"><li>KPI</li><li>Eventi</li></ul></li><li>Comunica la politica, la direzione a lungo termine o le decisioni a livello elevato</li></ul>	Esecutivo intera città
Supervisore o manager	<ul style="list-style-type: none"><li>Gestisce gli eventi e gli incidenti</li><li>Produce e monitora report KPI</li><li>Emette avvisi</li><li>Analizza eventi per una modifica di stato o requisiti di azione</li><li>Decide misure correttive a breve termine</li></ul>	Supervisore intera città



Tabella 23. Ruoli lavorativi e gruppi di ruoli utente di IBM Intelligent Operations Center (Continua)

Ruolo lavorativo	Responsabilità	Gruppo di ruolo utente
Operatore	<ul style="list-style-type: none"> <li>• Monitora le informazioni degli eventi</li> <li>• Monitora gli avvisi</li> <li>• Visualizza i dettagli</li> <li>• Emette comunicazioni</li> <li>• Aggiorna i dati degli eventi o degli incidenti con ulteriori informazioni, ad esempio:                             <ul style="list-style-type: none"> <li>– Report telefonici</li> <li>– Input da costruzione o manutenzione</li> </ul> </li> </ul>	Operatore intera città
Amministratore utenti	Amministra tutti gli aspetti degli utenti incluso la definizione di gruppi, l'assegnazione di autorizzazioni ai gruppi e l'assegnazione di utenti ai gruppi. Fornisce agli utenti il livello di accesso corretto. Il livello di accesso viene assegnato in base all'appartenenza ad un gruppo.	wpsadmins

Prima di personalizzare i ruoli e di definire gli utenti per l'organizzazione, familiarizzare con il sistema di sicurezza di IBM Intelligent Operations Center.

**Attività correlate:**

“Aggiunta di un gruppo o di un utente” a pagina 75

Selezionare un gruppo e creare un profilo utente per aggiungere un nuovo utente a IBM Intelligent Operations Center. Selezionare un nome di gruppo per aggiungere un nuovo gruppo.

**Riferimenti correlati:**

“Gruppi di ruoli utente e autorizzazioni” a pagina 72

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

“Gruppi di categoria utente e autorizzazioni ai dati” a pagina 74

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

## Utenti di esempio

Durante la distribuzione di IBM Intelligent Operations Center, vengono creati utenti di esempio.

Vengono definiti utenti di esempio generici con i gruppi di ruolo utente e le corrispondenti autorizzazioni di accesso. Questi utenti di esempio vengono definiti solo come esempi e sono elencati nella tabella riportata di seguito. Altri utenti sono richiesti per l'amministrazione della soluzione.

Tabella 24. Utenti definiti in IBM Intelligent Operations Center

ID utente	Gruppo di ruolo utente
<b>Utenti di esempio</b>	
tdelorne	Esecutivo intera città
scollins	Supervisore intera città
akelly	Operatore intera città
<b>Utente richiesto</b>	
wpsadmin	wpsadmins

Quando si è pronti per definire utenti per la propria organizzazione, eliminare solo gli utenti di esempio. Non eliminare l'utente wpsadmin. L'utente wpsadmin è essenziale per le attività di amministrazione associate a IBM Intelligent Operations Center. Per ulteriori informazioni sugli utenti richiesti, vedere il link alla fine di questo argomento.

**Importante:** Sostituire la password predefinita dell'utente wpsadmin con una nuova password. Per informazioni sull'aggiornamento di ID utente e password dell'amministratore del portale, consultare la documentazione WebSphere Portal.

**Concetti correlati:**

“Informazioni sulla password” a pagina 39

Le password per i diversi ID utente nella soluzione IBM Intelligent Operations Center sono definite nel file delle proprietà della topologia. Per motivi di sicurezza le password predefinite fornite con IBM Intelligent Operations Center devono essere modificate.

**Attività correlate:**

“Eliminazione di utenti di esempio” a pagina 67

IBM Intelligent Operations Center viene fornito con utenti di esempio. Per motivi legati alla sicurezza, questi utenti devono essere cancellati dopo che IBM Intelligent Operations Center è stato installato nel proprio ambiente di produzione.

**Informazioni correlate:**

 Documentazione del prodotto IBM WebSphere Portal 7

## Gruppi di ruoli utente e autorizzazioni

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

Un amministratore assegna un ruolo ad un utente rendendo l'utente membro del corrispondente gruppo di ruolo utente. Ad ogni utente viene assegnata l'appartenenza ad uno o più gruppi di ruolo utente.

La seguente tabella elenca le autorizzazioni per ciascun gruppo di ruolo utente fornite con IBM Intelligent Operations Center. Per ogni gruppo di ruolo utente, viene fornita un'autorizzazione a ciascuna funzione in IBM Intelligent Operations Center.

*Tabella 25. Funzioni di IBM Intelligent Operations Center e autorizzazioni di gruppo di ruolo utente associate*

Tipo di funzione	Nome funzione	Esecutivo intera città	Supervisore intera città	Operatore intera città	wpsadmins
Pagina	Supervisore: Stato	Autorizzazione utente	Autorizzazione utente	Nessuna	Autorizzazione amministratore
	Supervisore: Operazioni	Autorizzazione utente	Nessuna	Nessuna	Autorizzazione amministratore
	Supervisore: Report	Nessuna	Autorizzazione utente	Nessuna	Autorizzazione amministratore
	Operatore: Operazioni	Nessuna	Nessuna	Autorizzazione utente	Autorizzazione amministratore
	Operatore: Report	Nessuna	Nessuna	Autorizzazione utente	Autorizzazione amministratore
	Mappa ubicazioni	Nessuna	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Amministrazione	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore

Tabella 25. Funzioni di IBM Intelligent Operations Center e autorizzazioni di gruppo di ruolo utente associate (Continua)

Portlet	Stato	Autorizzazione utente	Autorizzazione utente	Nessuna	Autorizzazione amministratore
	Drill Down KPI (Key Performance Indicator)	Autorizzazione utente	Autorizzazione utente	Nessuna	Autorizzazione amministratore
	Notifiche	Autorizzazione utente	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Contatti	Autorizzazione utente	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Mappa	Autorizzazione utente	Nessuna	Autorizzazione utente	Autorizzazione amministratore
	Dettagli	Autorizzazione utente	Nessuna	Autorizzazione utente	Autorizzazione amministratore
	Attività personali	Autorizzazione utente	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Mappa ubicazioni	Nessuna	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Report	Nessuna	Autorizzazione utente	Autorizzazione utente	Autorizzazione amministratore
	Intelligent Operations Center - Informazioni	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Console di gestione	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Controllo di verifica del sistema	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Riepilogo autorizzazioni utente	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	KPI (Key Performance Indicators)	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Gestore mappa ubicazioni	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	SOP (Standard Operating Procedure)	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Programmazione script di eventi	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Publisher di esempio	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore
	Utenti e gruppi	Nessuna	Nessuna	Nessuna	Autorizzazione amministratore

Le autorizzazioni di IBM Intelligent Operations Center vengono assegnate in base ai gruppi LDAP (Lightweight Directory Access Protocol). Le autorizzazioni sono definite come segue:

- Autorizzazione utente è l'autorità concessa ad un utente per fornire loro l'accesso per visualizzare ed utilizzare le funzioni.
- Autorizzazione amministratore è l'autorità concessa ad un amministratore per fornire loro l'accesso per:
  - Configurare le funzioni
  - Creare, modificare o eliminare utenti e gruppi di utenti

Per accedere ai dati in IBM Intelligent Operations Center un utente deve essere membro di un gruppo di categoria utente che fornisce le autorizzazioni dati richieste.

#### Concetti correlati:

“Riepilogo autorizzazioni utente” a pagina 80

Utilizzare il portlet Riepilogo autorizzazioni utente per visualizzare le autorizzazioni associate agli utenti e gruppi di IBM Intelligent Operations Center.

“Ruoli utente e accesso” a pagina 70

IBM Intelligent Operations Center implementa la sicurezza limitando l'accesso alle funzioni in base ai ruoli utente.

#### Attività correlate:

“Aggiunta di un gruppo o di un utente” a pagina 75

Selezionare un gruppo e creare un profilo utente per aggiungere un nuovo utente a IBM Intelligent Operations Center. Selezionare un nome di gruppo per aggiungere un nuovo gruppo.

“Visualizzazione o modifica dell'appartenenza al gruppo” a pagina 77

Visualizzare o modificare l'appartenenza al gruppo per gestire le autorizzazioni di accesso degli utenti all'interno di IBM Intelligent Operations Center.

#### Riferimenti correlati:

“Gruppi di categoria utente e autorizzazioni ai dati”

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

#### Informazioni correlate:

 Documentazione del prodotto IBM WebSphere Portal 7

## Gruppi di categoria utente e autorizzazioni ai dati

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

Un amministratore assegna l'accesso ai dati ad un utente rendendo l'utente membro del gruppo di categoria utente appropriato. Ad ogni utente viene assegnata l'appartenenza ad uno o più gruppi di categoria utente.

La seguente tabella elenca le categorie di dati coperte da IBM Intelligent Operations Center e i corrispondenti gruppi di categorie utente utilizzati per identificare i dati evento, KPI (key performance indicator) di avviso. Ad esempio, se un utente desidera poter visualizzare gli eventi correlati al dipartimento idrico della città, l'utente deve essere membro del gruppo `ioc_base_infrastructure`.

Tabella 26. Descrizioni e identificativi del gruppo di categoria utente

Categoria dati	Descrizione	Gruppo categoria utente
CBRNE	Minaccia o attacco chimico, biologico, radiologico, nucleare o esplosivo di grossa portata	<code>ioc_base_chemical</code> , <code>ioc_base_biological</code> , <code>ioc_base_radiological</code> , <code>ioc_base_nuclear</code> , <code>ioc_base_explosive</code>
Env	Ambiente: inquinamento ed altra tipologia ambientale	<code>ioc_base_environmental</code>
Incendio	Spegnimento incendi e salvataggio	<code>ioc_base_fire</code>

Tabella 26. Descrizioni e identificativi del gruppo di categoria utente (Continua)

Categoria dati	Descrizione	Gruppo categoria utente
Geo	Geofisico (incluso lo smottamento)	ioc_base_geophysical
Salute	Medicina e salute pubblica	ioc_base_health
Infra	Infrastruttura: servizi, telecomunicazioni, altre infrastrutture non legate ai trasporti	ioc_base_infrastructure
Met	Meteorologico (incluso alluvione)	ioc_base_meteorological
Salvataggio	Salvataggio e recupero	ioc_base_rescue
Incolunità	Emergenze generiche e sicurezza pubblica	ioc_base_safety
Protezione	Applicazione della legge, forze armate, sicurezza interna, locale e privata	ioc_base_security
Trasporto	Trasporti pubblici e privati	ioc_base_transportation
Altro	Altri eventi, KPI o avvisi	ioc_base_other

Per collegarsi ed accedere alle funzioni di IBM Intelligent Operations Center, un utente deve essere membro di un gruppo di ruolo utente che fornisce le autorizzazioni richieste.

#### Concetti correlati:

“Riepilogo autorizzazioni utente” a pagina 80

Utilizzare il portlet Riepilogo autorizzazioni utente per visualizzare le autorizzazioni associate agli utenti e gruppi di IBM Intelligent Operations Center.

“Ruoli utente e accesso” a pagina 70

IBM Intelligent Operations Center implementa la sicurezza limitando l'accesso alle funzioni in base ai ruoli utente.

#### Attività correlate:

“Aggiunta di un gruppo o di un utente”

Selezionare un gruppo e creare un profilo utente per aggiungere un nuovo utente a IBM Intelligent Operations Center. Selezionare un nome di gruppo per aggiungere un nuovo gruppo.

“Visualizzazione o modifica dell'appartenenza al gruppo” a pagina 77

Visualizzare o modificare l'appartenenza al gruppo per gestire le autorizzazioni di accesso degli utenti all'interno di IBM Intelligent Operations Center.

#### Riferimenti correlati:

“Gruppi di ruoli utente e autorizzazioni” a pagina 72

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

#### Informazioni correlate:

 Documentazione del prodotto IBM WebSphere Portal 7

---

## Aggiunta di un gruppo o di un utente

Selezionare un gruppo e creare un profilo utente per aggiungere un nuovo utente a IBM Intelligent Operations Center. Selezionare un nome di gruppo per aggiungere un nuovo gruppo.

### Informazioni su questa attività

Innanzitutto selezionare un gruppo di ruoli utente per impostare il corretto livello di autorizzazioni di accesso quando si aggiunge un nuovo utente. Quindi completare i campi nella pagina **Gestione profili** in modo che IBM Intelligent Operations Center abbia le informazioni richieste per aggiungere un nuovo utente. Seguire il link alla fine dell'argomento per ulteriori informazioni su cosa è possibile immettere nei campi della pagina **Gestione profili**.

## Procedura

1. Collegarsi a <http://app-host/wpsv70/wps/myportal/> come utente di gestione.
2. Fare clic su **Amministrazione** nella barra di navigazione nella parte superiore della pagina.
3. Fare clic su **Accesso** nel menu della barra laterale.
4. Fare clic su **Utenti e gruppi** nel menu secondario.
5. Se si sta aggiungendo un nuovo utente, selezionare un ruolo fornendo l'appartenenza dell'utente ad un gruppo. Cercare il gruppo facendo clic su **Tutti i gruppi di utenti del portale** per un elenco di gruppi e fare clic sul gruppo richiesto.
6. Fare clic su **Nuovo utente** o **Nuovo gruppo**.
7. Se si sta creando un gruppo di utenti, immettere un nome per il gruppo di utenti.
8. Se si sta aggiungendo un nuovo utente, assicurarsi di completare tutti i campi obbligatori del profilo utente come indicato dagli asterischi.
9. Fare clic su **OK** per inoltrare il nuovo profilo o gruppo.

## Risultati

Un messaggio conferma se l'inoltro ha avuto esito positivo. Un nuovo profilo utente viene creato e visualizzato nell'elenco di gruppi o viene visualizzato un nuovo gruppo. Il nuovo utente è autorizzato ad accedere a IBM Intelligent Operations Center in base alle autorizzazioni assegnate al gruppo di ruoli selezionato.

## Operazioni successive

- Fornire al nuovo utente l'appartenenza a gruppi di categorie di dati in base alle autorizzazioni di dati richieste.
- Se è stato aggiunto un nuovo gruppo, aggiungere il gruppo all'ACL di giunzione di WebSphere Application Server Network Deployment.
- Se è stato aggiunto un nuovo gruppo, devono essere impostate anche le autorizzazioni per il gruppo. Le autorizzazioni definiscono quali funzioni i membri di dati del gruppo possono visualizzare e modificare. Per informazioni relative all'impostazione delle autorizzazioni, consultare il link della documentazione del prodotto IBM WebSphere Portal 7 alla fine dell'argomento e ricercare le informazioni relative all'assegnazione dell'accesso alle pagine.
- Assegnare il nuovo utente ad un gruppo di sicurezza e gruppo di persone in Tivoli Service Request Manager.

**Nota:** Per risparmiare tempo è possibile duplicare le assegnazioni ai gruppi per un nuovo utente in base ad un utente esistente. Selezionare il nuovo utente e fare clic sull'icona **Duplica**. Selezionare l'utente esistente per duplicare l'appartenenza al gruppo.

### Concetti correlati:

“Ruoli utente e accesso” a pagina 70

IBM Intelligent Operations Center implementa la sicurezza limitando l'accesso alle funzioni in base ai ruoli utente.

### Attività correlate:

“Configurazione di nuovi utenti in Tivoli Service Request Manager” a pagina 126

Quando si aggiunge un utente in IBM Intelligent Operations Center, assegnare le autorizzazioni e i gruppi di persone per l'utente in Tivoli Service Request Manager.

### Riferimenti correlati:

“Gruppi di ruoli utente e autorizzazioni” a pagina 72

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

“Gruppi di categoria utente e autorizzazioni ai dati” a pagina 74

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

### Informazioni correlate:



Documentazione del prodotto IBM WebSphere Portal 7

---

## Visualizzazione o modifica dell'appartenenza al gruppo

Visualizzare o modificare l'appartenenza al gruppo per gestire le autorizzazioni di accesso degli utenti all'interno di IBM Intelligent Operations Center.

### Informazioni su questa attività

Selezionare il gruppo corrispondente al ruolo o alla categoria di dati per il quale si desidera visualizzare o modificare l'appartenenza. L'appartenenza ad un gruppo di ruolo fornisce agli utenti l'accesso alle parti della soluzione appropriate a quel ruolo. L'appartenenza a un gruppo di categoria fornisce agli utenti l'accesso agli eventi, ai KPI (key performance indicator) e agli avvisi associati a quella categoria.

Passare con il cursore su un'icona per visualizzare la guida a comparsa che indica lo scopo dell'icona.

### Procedura

1. Collegarsi a <http://app-host/wpsv70/wps/myportal/> come utente di gestione.
2. Fare clic su **Amministrazione** nella barra di navigazione nella parte superiore della pagina.
3. Fare clic su **Accesso** nel menu della barra laterale.
4. Fare clic su **Utenti e gruppi** nel menu secondario.
5. Fare clic su **Tutti i gruppi di utenti del portale** per un elenco di gruppi e fare clic sul gruppo richiesto. Vengono elencati i membri del gruppo.
6. In relazione all'appartenenza al gruppo è possibile eseguire le seguenti azioni:
  - Visualizzare l'appartenenza ad altri gruppi facendo clic su **Visualizza appartenenza** per l'ID utente.
  - Aggiungere un utente o più utenti al gruppo facendo clic su **Aggiungi membro** e selezionare l'utente o gli utenti da aggiungere.
  - Rimuovere un utente dal gruppo facendo clic su **Rimuovi** per l'ID utente.

### Riferimenti correlati:

“Gruppi di ruoli utente e autorizzazioni” a pagina 72

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

“Gruppi di categoria utente e autorizzazioni ai dati” a pagina 74

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

### Informazioni correlate:

 [Documentazione del prodotto IBM WebSphere Portal 7](#)

---

## Visualizzazione o modifica di un profilo utente

Visualizzare o modificare il profilo di un utente per impostare o reimpostare uno qualsiasi degli attributi del profilo utente inclusa la password. Non è possibile modificare l'ID utente.

### Informazioni su questa attività

Selezionare l'utente dall'elenco degli utenti autenticati del portale per aprire il profilo utente e modificarne i dettagli. Ciascun utente può inoltre modificare il proprio profilo.

Passare con il cursore su un'icona per visualizzare la guida a comparsa che indica lo scopo dell'icona.

### Procedura

1. Collegarsi a <http://app-host/wpsv70/wps/myportal/> come utente di gestione.
2. Fare clic su **Amministrazione** sulla barra di navigazione superiore.
3. Fare clic sulla voce **Accesso** nel menu della barra laterale.
4. Fare clic su **Utenti e gruppi** nel menu secondario.
5. Fare clic su **Tutti gli utenti autenticati del portale** per un elenco di utenti.
6. Fare clic sull'icona di modifica per visualizzare la pagina **Gestione profili**. Vengono visualizzati i campi degli attributi per il profilo utente.
7. Se si desidera modificare la password, immettere una nuova password nei campi **Nuova password:** e **Conferma password**.
8. È possibile immettere, modificare o eliminare le informazioni in qualsiasi campo tra quelli rimasti.
9. Fare clic su **OK** per inoltrare le modifiche apportate.

### Risultati

Il profilo utente viene aggiornato con le modifiche inoltrate.

### Informazioni correlate:

 [Documentazione del prodotto IBM WebSphere Portal 7](#)

---

## Eliminazione di un utente o di un gruppo

Eliminare un utente o un gruppo da IBM Intelligent Operations Center.

### Informazioni su questa attività

Per eliminare un utente, selezionare l'utente dall'elenco di utenti autenticati del portale ed eliminarlo. Per eliminare un gruppo, selezionare il gruppo dall'elenco di gruppi di utenti del portale ed eliminarlo.

Passare con il cursore su un'icona per visualizzare la guida a comparsa che indica lo scopo dell'icona.



**Nota:** Tenere presente che l'eliminazione di un utente da IBM Intelligent Operations Center rimuove anche il suo accesso alle altre soluzioni all'interno della famiglia di prodotti IBM Smarter Cities™ Software Solutions. L'eliminazione di un gruppo lo rimuove anche dalle altre soluzioni.

## Procedura

1. Collegarsi a `http://app-host/wpsv70/wps/myportal/` come utente di gestione.
2. Fare clic su **Amministrazione** sulla barra di navigazione superiore.
3. Fare clic su **Accesso** nel menu della barra laterale.
4. Fare clic su **Utenti e gruppi** nel menu secondario:
  - Fare clic su **Tutti i gruppi di utenti del portale** per visualizzare un elenco di gruppi.
  - Fare clic su **Tutti gli utenti autenticati del portale** per visualizzare un elenco di utenti.
5. Fare clic sull'icona **Elimina** corrispondente all'utente o al gruppo che si desidera eliminare.

## Risultati

L'utente o il gruppo eliminato non esiste più in IBM Intelligent Operations Center. L'eliminazione di un gruppo non elimina i membri del gruppo.

### Informazioni correlate:

 [Documentazione del prodotto IBM WebSphere Portal 7](#)

---

## Importazione di utenti e gruppi

È possibile importare utenti in massa in IBM Intelligent Operations Center tramite il servizio del portale.

### Informazioni su questa attività

In qualità di amministratore del portale, è possibile importare utenti in massa in IBM Intelligent Operations Center tramite la console di gestione del portale. Il file XML richiesto per questa attività si trova sul server delle applicazioni: `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml`. Questo file XML può essere modificato per aggiungere utenti a IBM Intelligent Operations Center.

**Nota:** Quando si aggiungono più utenti, aggiungere prima tutti gli utenti, prima di aggiungere gli utenti ai gruppi. Vedere l'esempio alla fine dell'argomento.

In alternativa alla procedura riportata di seguito, dalla riga comandi è possibile eseguire lo script `xmlaccess.sh` che si trova sul server delle applicazioni.

## Procedura

1. Aggiornare il file `CreateUser.xml` per contenere i nuovi utenti e i gruppi a cui appartengono.
2. Collegarsi a `http://app-host/wpsv70/wps/myportal/` come utente di gestione.
3. Fare clic su **Amministrazione**.
4. In **Impostazioni portale**, fare clic su **Importa XML**.
5. Individuare il file XML aggiornato.
6. Fare clic su **Importa**.

## Risultati

WebSphere Portal Server crea automaticamente le voci associate nella directory su Tivoli Directory Server e in Tivoli Access Manager WebSEAL.

## Esempio

Il seguente esempio modifica il file XML aggiungendo due utenti a IBM Intelligent Operations Center e aggiungendo ognuno ad un gruppo di ruolo e un gruppo di categoria:

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true">
<portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```


### Concetti correlati:


“Console di gestione” a pagina 203

Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.

### Informazioni correlate:

 [Documentazione del prodotto IBM WebSphere Portal 7](#)

 [Centro informazioni di Tivoli Directory Server](#)

 [Centro informazioni di Tivoli Access Manager](#)

---

## Riepilogo autorizzazioni utente

Utilizzare il portlet Riepilogo autorizzazioni utente per visualizzare le autorizzazioni associate agli utenti e gruppi di IBM Intelligent Operations Center.

Il portlet Riepilogo autorizzazioni utente visualizza i dettagli dell'appartenenza al gruppo e le autorizzazioni concesse agli utenti.

Per accedere al portlet Riepilogo autorizzazioni utente, nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di gestione > Riepilogo delle autorizzazioni dell'utente**.

Utilizzare la scheda **Utente** per controllare le autorizzazioni di un utente. Immettere l'ID utente per visualizzare le seguenti informazioni:

- Un elenco completo di tutte le categorie di dati e tutti i gruppi di categorie utente disponibili in IBM Intelligent Operations Center.

- Un elenco delle autorizzazioni sulle categorie di dati assegnate all'utente specificato.
- Un elenco di tutti i gruppi, dei gruppi di ruoli utente e dei gruppi di categorie utente di cui è membro l'utente specificato.
- Un elenco di ciascuna categoria di dati indica se l'utente specificato dispone dell'autorizzazione per quella categoria.

Utilizzare la scheda **Riepilogo** per controllare le statistiche di riepilogo per autorizzazioni di utenti e gruppi. È possibile visualizzare le seguenti informazioni:

- Numero complessivo di gruppi in IBM Intelligent Operations Center.
- Numero complessivo di utenti autorizzati ad accedere a IBM Intelligent Operations Center.
- Un elenco del numero complessivo di utenti per categoria di dati.
- Un elenco del numero complessivo di utenti per gruppo di ruolo utente.

#### **Riferimenti correlati:**

“Gruppi di ruoli utente e autorizzazioni” a pagina 72

Una serie di autorizzazioni per l'accesso alle funzioni in IBM Intelligent Operations Center è associata a ciascun gruppo di ruolo utente.

“Gruppi di categoria utente e autorizzazioni ai dati” a pagina 74

Ad ogni gruppo di categoria utente viene associata un'autorizzazione ad accedere ad una categoria di dati in IBM Intelligent Operations Center.

## **Panoramica su cyber hygiene**

La funzione cyber hygiene di IBM Intelligent Operations Center è progettata per fornire servizi che pongano rimedio a potenziali rischi nella sicurezza nel sistema installato.

**Nota:** Di solito, il concetto di "vulnerabilità" viene utilizzato per fare riferimento sia alla vulnerabilità nella sicurezza che ai rischi per la sicurezza. Cyber hygiene definisce una vulnerabilità, come un errore di programmazione in un'applicazione che consente violazioni della sicurezza. Cyber hygiene definisce un rischio come una selezione del sistema operativo o della configurazione dell'applicazione meno sicura. I rischi possono essere risolti, scegliendo un'opzione di configurazione più sicura. Ad esempio, una directory può essere configurata in modo da consentire a tutti gli utenti di memorizzare i file. Può anche essere configurata in modo più sicuro consentendo solo al proprietario di memorizzare i file nella directory.

Cyber hygiene dispone di due elementi chiave:

- Riduzione e correzione dei rischi di sicurezza noti nel sistema operativo Linux e negli utenti, nelle directory e nei file associati. Ciò avviene mediante una serie di strumenti e script.
- Documentazione della risoluzione di quasi 1000 tra vulnerabilità e rischi noti nel sistema operativo, nei prodotti e nella configurazione del sistema.

La gestione dei rischi di sicurezza durante il processo di installazione, richiede meno lavoro per il cliente per raggiungere un livello di sicurezza maggiore nel sistema distribuito.

Ad esempio, un'agenzia governativa può utilizzare la riparazione cyber hygiene e la relativa documentazione per contribuire a sostenere la certificazione e l'accreditamento del sistema per la distribuzione su una rete protetta. I clienti di business commerciali possono utilizzare lo stesso processo per migliorare la sicurezza del proprio ambiente.

La sicurezza Cyber fornisce una mitigazione del rischio, non la prevenzione dei rischi. Poiché i sistemi devono essere in esecuzione ed essere accessibile per fornire un valore, c'è sempre il rischio che le informazioni di un sistema o il suo controllo venga compromesso.

Cyber hygiene non affronta vulnerabilità specifiche dell'applicazione, come la gestione di minacce quali Denial of Service, SQL injection e così via. Cyber hygiene, invece, fornisce le basi per la sicurezza dell'applicazione, affrontando i rischi relativi alla sicurezza degli utenti, delle directory e dei file in modo generale; non indirizzando tali procedure in modo particolare ad alcuna applicazione specifica. Cyber hygiene viene eseguito dopo l'installazione del prodotto per correggere tali vulnerabilità generali per gli utenti, le directory ed i file di sistema e delle applicazioni. Qualsiasi applicazione utilizzata con il sistema operativo Linux deve essere corretta separatamente per le vulnerabilità dell'applicazione.

Il catalogo delle vulnerabilità e dei rischi noti di cyber hygiene è basato su elenchi non classificati e non riservati della DISA (United States Defense Information Services Agency). Gli elementi di questi elenchi sono valutati per essere utilizzati in cyber hygiene. La scansione degli script ricerca e registra le istanze di un rischio e quindi, laddove applicabile, i file di log vengono utilizzati come input per gli script di correzione che affrontano il problema. Un piccolo sottoinsieme di risultati di sicurezza richiedono una gestione diversa.

La documentazione che elenca le vulnerabilità note nei componenti IBM Intelligent Operations Center e le azioni intraprese da cyber hygiene per mitigarle, viene fornita da IBM Intelligent Operations Center.

#### **Attività correlate:**

“Elenco di controllo - installazione utilizzando IBM Installation Manager” a pagina 14

Utilizzare questo elenco di controllo per tenere traccia dei passi di installazione durante l'installazione di IBM Intelligent Operations Center utilizzando IBM Installation Manager.

“Elenco di controllo - installazione dettagliata” a pagina 16

Utilizzare questo elenco di controllo per tenere traccia dei passi di installazione durante l'installazione di IBM Intelligent Operations Center utilizzando script e comandi.

“Installazione di IBM Intelligent Operations Center utilizzando Installation Manager” a pagina 26

IBM Intelligent Operations Center può essere installato utilizzando il programma di installazione grafico fornito.

“Installazione ed esecuzione guidata di cyber hygiene” a pagina 62

Cyber hygiene viene installato ed eseguito separatamente da IBM Intelligent Operations Center e deve essere installato ed eseguito dopo che tutti gli altri componenti di IBM Intelligent Operations Center sono stati installati, configurati e operativi. Cyber hygiene modifica la configurazione del sistema operativo predefinito con un insieme più sicuro di opzioni che consentono di assicurare una base più sicura al sistema IBM Intelligent Operations Center.

## **Sicurezza Cyber**

La protezione dell'ambiente IT è stata a lungo una preoccupazione per i governi nazionali e sta diventando sempre più importante per i sistemi di infrastruttura critici. Sarebbe necessario rimuovere dai prodotti e dalle soluzioni che forniscono infrastrutture critiche, come IBM Intelligent Operations Center, le vulnerabilità note, prima di renderli disponibili.

La sicurezza Cyber rappresenta una mitigazione del rischio, non la prevenzione dei rischi. Poiché i sistemi IT devono essere in esecuzione ed essere accessibili per fornire un valore, c'è sempre il rischio che le informazioni o il controllo del sistema vengano compromessi. La sicurezza Cyber consiste di elementi statici e dinamici. Cyber hygiene in IBM Intelligent Operations Center si concentra sugli elementi statici della sicurezza cyber. Sono necessari altri strumenti e processi per la gestione degli elementi dinamici della sicurezza cyber. Questi strumenti e processi possono includere procedure di sicurezza per i materiali ed il personale o strumenti di intrusione di rete.

Le funzioni Cyber hygiene fornite dal IBM Intelligent Operations Center sono progettate per gestire aree quali le configurazioni di sicurezza deboli, errori del software, errori di gestione del sistema e gli errori del processo di sicurezza del sistema. Per offrire questo supporto, cyber hygiene fornisce funzioni di installazione e configurazione che impostano il sistema operativo e funzioni di gestione che configurano le impostazioni di sicurezza ed i fix pack relativi alla sicurezza chiave. Ad esempio, i sistemi sono configurati in modo tale da non consentire l'uso di ID senza password ed i servizi Linux non sicuri, quali,

ftp, snmp e rlogin. Tuttavia, i sistemi non possono essere automaticamente configurati in modo da soddisfare le pratiche di sicurezza aziendale specifiche.

## Elenco di controllo Cyber hygiene

Cyber hygiene utilizza elenchi di controllo basati sugli elenchi di controllo non protetti DISA (Defense Information Systems Agency) e su avvisi di vulnerabilità periodici.

### Analisi degli elementi dell'elenco di controllo

Ciascuna vulnerabilità identificata nell'elenco di controllo non protetto di DISA (Defense Information System Agency) definisce i dati relativi alla vulnerabilità.

Le informazioni fornite per ciascuna vulnerabilità includono quanto segue:

- Un identificativo univoco. L'identificativo è composto da un ID STIG (Security Implementation Technical Guide) e da una chiave VMS (Vulnerability Management System).
- Un nome breve che riassume la vulnerabilità.
- La gravità della vulnerabilità. I livelli di gravità documentati sono:
  - I Gravità elevata
  - II Gravità media
  - III Gravità bassa
- I prodotti influenzati.
- Le versioni dei prodotti influenzati.
- Una descrizione delle vulnerabilità compresi eventuali casi di utilizzo, contesto, o le interazioni con altri software.
- Qualsiasi azione consigliata. Se la soluzione non è disponibile tramite patch o un aggiornamento, potrebbe essere inclusa una procedura di riduzione consigliata.
- Qualsiasi avviso sostituito dall'avviso.

Per ciascuna vulnerabilità è importante comprendere se influisce o meno su IBM Intelligent Operations Center. Ad esempio:

- La release del prodotto e il livello di fix sono inclusi nel IBM Intelligent Operations Center influenzato? È possibile che una release del prodotto o una fix precedenti non siano influenzate perché il problema potrebbe essere stato introdotto in una release o fix successiva.
- Il prodotto incluso con IBM Intelligent Operations Center viene utilizzato in modo da esporlo a vulnerabilità? Ad esempio, un problema potrebbe manifestarsi solo quando il prodotto utilizza i servizi di un altro prodotto. Se tali servizi non sono utilizzati nella configurazione IBM Intelligent Operations Center, la soluzione potrebbe non essere necessaria.
- La vulnerabilità del prodotto influenza il sistema operativo utilizzato? Alcune vulnerabilità potrebbero manifestarsi solo quando sono in esecuzione determinati sistemi operativi.

Per ogni elemento in un elenco di controllo, sono stati analizzati questi fattori per determinare l'azione richiesta per IBM Intelligent Operations Center. Questa analisi e soluzione ha dato luogo a quattro possibili valutazioni:

#### NA (non applicabile)

Le configurazioni o i prodotti interessati non fanno parte dell'ambiente IBM Intelligent Operations Center.

#### NF (Non è un rilevamento)

La versione ed il livello di fix installati del prodotto non sono interessati, o il prodotto non viene utilizzato in modo da esporlo alla vulnerabilità. Questa valutazione viene utilizzata anche se la configurazione non espone alla vulnerabilità.

## Aperta

La vulnerabilità si applica alla versione del prodotto installato ed al livello di fix, tuttavia, non è disponibile alcun rimedio per il prodotto. Questa valutazione viene utilizzata anche se il sistema è configurato da esporre alla vulnerabilità. Ad esempio, assegnando l'autorizzazione world-write su una directory perché richiesta da un prodotto. Questa valutazione viene utilizzata anche quando l'applicazione di una soluzione potrebbe dipendere dalle politiche dell'organizzazione come le politiche password sul mix di caratteri e sulla lunghezza.

## Corretto

Una soluzione di una vulnerabilità aperta è stata applicata e verificata.

Tabella 27 mostra un'analisi di esempio. Il secondo esempio mostra la gestione di un prodotto non installato su nessun server IBM Intelligent Operations Center.

Tabella 27. Valutazioni della vulnerabilità di esempio

ID	Nome	Gravità	Server delle applicazioni	Server eventi	Server di dati	Server di gestione	Spiegazione
2011-B-0082	Vulnerabilità multiple in IBM Websphere Application Server	I	NF	Aperta	NA	NF	Interessa le versioni precedenti alla 6.1.0.39 e 7.0.0.19
2011-B-0085	Vulnerabilità multiple di tipo Denial of Service in Wireshark	I	NA	NA	NA	NA	Wireshark non installato

## Selezione elenco di controllo

Gli elenchi di controllo utilizzati per ciascun server si basano sul software installato su tale server. Alcuni elenchi di controllo specifici si riferiscono a vulnerabilità relative a tipi di prodotti, ad esempio, database. Altri fanno riferimento a problemi con prodotti specifici in una categoria, ad esempio DB2.

Non tutti i tipi di prodotti hanno elenchi di controllo specifici. Le vulnerabilità generiche sono documentate nell'elenco di controllo Sicurezza applicazione o in un elenco relativo al sistema operativo.

I seguenti tipi di elenchi di controllo vengono utilizzati da cyber hygiene:

### Sicurezza applicazione

Elenca le vulnerabilità a livello di sistema. Alcune si riferiscono allo sviluppo software ed alle pratiche di test, altre sono specifiche delle applicazioni, come ad esempio l'utilizzo delle password codificate durante l'autenticazione utente.

### Unix/Linux

Elenca le vulnerabilità relative alla configurazione, alla gestione delle password, al partizionamento del file system e così via.

### Server Web

Elenca le vulnerabilità relative al server HTTP.

### Database

Elenca le vulnerabilità relative ai server database.

### Server di directory

Elenca le vulnerabilità relative ai server LDAP.

### Enterprise System Management

Elenca le vulnerabilità relative agli strumenti di enterprise system management e system management processes.

La sicurezza di rete non viene affrontata dagli elenchi di controllo poiché la configurazione di sicurezza di rete deve essere determinata da una politica del cliente e dall'architettura di rete. Configurazione della sicurezza di rete deve essere gestita in base alle esigenze di ciascuna installazione.

## Configurazione predefinita di Cyber hygiene

La funzione cyber hygiene imposta le configurazioni ed le politiche di Linux con opzioni più sicure di quelle impostate nell'installazione del sistema operativo predefinita. Queste impostazioni predefinite possono essere facilmente modificate dagli amministratori di sistema in modo da adattarle alle politiche di sicurezza dell'installazione.

Un gruppo di gestione delle operazioni IT dell'azienda è responsabile della sicurezza dei propri sistemi. Ciò comprende la gestione dell'accesso di rete e le politiche di sicurezza ed i processi interni.

Se le impostazioni predefinite cyber hygiene non sono coerenti con la politica aziendale, le politiche aziendali devono avere la precedenza. Tenere presente che le impostazioni della politica di sicurezza locale non sono state verificate per l'impatto sulla funzionalità del sistema. La stessa attenzione che si ha quando si applica una politica di sicurezza ai prodotti non distribuiti con cyber hygiene si deve avere quando si applica una politica di sicurezza a IBM Intelligent Operations Center.

Mentre IBM Intelligent Operations Center non può essere configurato automaticamente per le politiche di sicurezza aziendali individuali, IBM Intelligent Operations Center può essere configurato per rimuovere le vulnerabilità note. Cyber hygiene configura IBM Intelligent Operations Center con un insieme di politiche consigliate predefinite creando una base per gli amministratori di sistema da utilizzare quando si applicano specifiche politiche e pratiche organizzative.

### Politiche di gestione della password predefinite

Cyber hygiene configura le politiche di gestione della password del sistema operativo Linux predefinite.

Le politiche di gestione della password predefinite impostate da cyber hygiene vengono mostrate in Tabella 28.

Tabella 28. Politiche di gestione della password di cyber hygiene predefinite

Politica	Valore o impostazione
Lunghezza minima della password	8 caratteri
Caratteri accettati	lettere maiuscole, minuscole, numeri e caratteri speciali (: ; ! ` ~ @ # \$ % ^ & * ( ) - _ = + [ { ] } \   ' " , < . > / ? ed il carattere spazio)
Regole sul contenuto	nessuna
Numero di tentativi di accesso non riusciti prima di bloccare l'utente	3
Tempo minimo tra le modifiche della password	1 giorno
Tempo massimo tra le modifiche della password	60 giorni
Le password sugli account sono obbligatorie?	sì
Quando è possibile riutilizzare una password?	dopo 5 password diverse
Accesso richiesto dopo l'inattività	15 minuti di inattività
Ritardo tra registrazione ed errore	4 secondi

I file `/etc/pam.d/system-auth` e `/etc/login.defs` sono stati modificati durante l'impostazione delle politiche predefinite cyber hygiene.

Queste impostazioni sono destinate ad essere il minimo necessario per delle pratiche di sicurezza ragionevoli. È necessario modificare queste impostazioni in modo che corrispondano alle politiche di sicurezza della propria organizzazione. Alcune aree in cui potrebbe essere necessario modificare le impostazioni predefinite sono le seguenti:



- Mentre la configurazione predefinita imposta la lunghezza minima della password a 8 caratteri, le procedure ottimali per proteggere i sistemi generalmente ritengono una password sicura quando questa supera i 14 caratteri in lunghezza.
- Il tempo massimo tra le modifiche della parola d'ordine dovrebbe essere impostato su un valore appropriato per la propria organizzazione. Questo viene definito nel parametro **inactive** nel file `/etc/shadow`. Dopo il periodo di tempo definito l'utente è costretto a modificare la password all'accesso. Se l'utente non riesce a modificare la password, questa dovrà essere reimpostata da un utente privilegiato. Se il valore specificato nel file `/etc/shadow` viene utilizzato dipende dall'azione predefinita specificata nel file `/etc/default/useradd`. Se il file `/etc/default/useradd` specifica `-1`, la password non scade. Se `/etc/default/useradd` specifica `0`, l'account viene bloccato. Se nel file `/etc/default/useradd` viene definito qualsiasi altro valore, per la scadenza della password viene utilizzato il valore del parametro **inactive** in `/etc/shadow`.
- Le regole concernenti la complessità ed il contenuto delle password devono essere affrontate e applicate in base alla politica di sicurezza aziendale.

Consultare la documentazione Linux per ulteriori informazioni sulla gestione delle politiche delle password.

## Servizi Linux disabilitati

Cyber hygiene disabilita o disinstalla i servizi Linux vulnerabili. Questi servizi possono consentire l'accesso al sistema e devono essere avviati o installati solo se sono necessari.

I seguenti servizi Linux (daemon) non vengono avviati per impostazione predefinita. Possono essere avviati se necessario.

- `inetd/xinetd`
- `portmap`
- `avahi-daemon`
- `bluetooth`
- `cups`
- `hidd`
- `isdn`
- `rhnsd`
- `canna`
- `pcmcia`
- `yplib`
- `autofs`
- `smartd`
- `netfs`
- `snmpd`
- `nfs`
- `samba`

Questi servizi possono essere avviati utilizzando il comando **`service service_name start`**.

**Nota:** Questi servizi, se non correttamente configurati, possono essere compromessi e consentire l'accesso non autorizzato al sistema. Questo è il motivo per cui, per la sicurezza del sistema, non vengono avviati per impostazione predefinita.

I seguenti servizi Linux vengono rimossi. Possono essere reinstallati se necessario utilizzando i comandi **`rpm`** o **`yum`**. Ad esempio il comando **`yum install httpd`** installerà il package del daemon HTTP.

- `tcpdump`



- sendmail
- squid
- vnc-server
- httpd
- mod\_python
- mod\_perl
- mod\_ssl
- swebalizer
- httpd-manual

**Nota:** Questi servizi vengono rimossi da Linux perché rappresentano una potenziale causa di esposizione della sicurezza in ambienti server.

### **ID utente rimossi**

Una installazione Linux standard contiene un numero di ID utente che non è consigliabile avere in un ambiente di produzione sicuro. Cyber Hygiene rimuove questi ID utente dal registro utente Linux e dal file `/etc/passwd`. Vengono rimosse anche le directory home associate.

I seguenti ID utente vengono eliminati e possono essere ricreati se necessario.

- games
- news
- ftp
- halt
- shutdown
- reboot
- who
- gopher
- lp
- rpcuser
- uucp

Se questi ID utente sono necessari, è possibile utilizzare le procedure standard di amministrazione Linux per crearli.

### **Regole di verifica**

La verifica standard in Linux è ridotta al minimo poiché i file di verifica possono crescere in fretta. Tuttavia, quando la sicurezza è un problema, è essenziale effettuare verifiche aggiuntive per essere in grado di determinare ciò che è accaduto in un incidente. Gli script Cyber hygiene aggiungono una serie di regole di verifica aggiuntive per tutti i livelli di esecuzione di Linux. Eventi corrispondenti a queste regole verranno registrati nei file di log di sistema standard.

Vengono aggiunte le seguenti regole di verifica Linux che è possibile modificare.

- Tentativi di accesso a programmi e file non riusciti
- L'eliminazione di programmi e file
- Azioni di gestione, sicurezza e privilegiate
- Modifiche alle autorizzazioni di controllo accessi

Dei buoni log di verifica rappresentano una buona pratica di sicurezza. Se per qualche motivo la verifica definita da cyber hygiene deve essere modificata, è necessario modificare i file `/etc/audit/auditd.conf` e `/etc/audit/audit.rules`. Cyber hygiene attiva la verifica per tutti i cinque livelli di Red Hat Enterprise Linux.

### **Autorizzazioni file e directory**

Cyber Hygiene modifica le autorizzazioni dei file e delle directory esistenti in modo che soddisfino le autorizzazioni di sicurezza ottimali.

Le modifiche apportate alle autorizzazioni di file e directory da cyber hygiene sono le seguenti:

### **Limitazioni degli script di sistema**

Gli script del sistema di sicurezza sensibili non possono essere acceduti dagli utenti senza privilegi appropriati.

### **Rimozione dell'autorizzazione world-write**

Gli utenti non possono scrivere in directory che non sono pubbliche. Le applicazioni e gli utenti che richiedono di modificare i file e le directory devono esserne i proprietari o un membro del gruppo del file o della directory.

### **Rimozione dell'autorizzazione world-read e execute**

Le autorizzazioni world-read e world-execute sono rimosse da molti file e cartelle. In particolare, tali autorizzazioni sono rimosse dalle directory home degli utenti. Le applicazioni e gli utenti che richiedono di leggere o eseguire i file devono esserne i proprietari o un membro del gruppo del file o della directory.

### **Altre modifiche**

Cyber hygiene apporta altre modifiche per affrontare i rischi per la sicurezza.

### **Programmi batch – comando in**

Per evitare che gli utenti senza privilegi utilizzino il comando **at** per eseguire programmi batch ad un'ora in particolare, cyber hygiene elimina il file `at.deny` e crea un file `at.allow` vuoto.

Il file `at.allow` definisce gli utenti autorizzati ad eseguire il comando **at**. Un file `at.allow` che non contiene alcun ID implica che nessun utente, che non abbia un ID di sistema privilegiato, possa eseguire il comando **at**. Se esiste il file `at.deny`, che definisce gli utenti a cui non è esplicitamente consentito di utilizzare il comando **in**, ma non esiste il file `at.allow`, tutti gli utenti, tranne quelli contenuti nel file `at.deny`, possono eseguire il comando **at**. Se nessuno dei due file esiste, solo il superuser potrà eseguire il comando **at**.

Per impostazione predefinita Red Hat Enterprise Linux viene configurato per consentire agli utenti di eseguire il comando **at**.

### **Programmi batch – comando cron**

Gli utenti senza privilegi di amministratore non sono autorizzati ad eseguire il comando **cron** per pianificare i programmi batch.

### **Ctrl-Alt-Canc**

La combinazione di tasti Ctrl-Alt-Canc è disabilitata in modo che non può essere utilizzata per arrestare il sistema.

## Strumenti di soluzione

La funzionalità Cyber Hygiene IBM Intelligent Operations Center fornisce gli strumenti di soluzione delle vulnerabilità presenti nel sistema IBM Intelligent Operations Center installato.

Gli strumenti di soluzione vengono eseguiti quando Cyber Hygiene viene eseguito dopo che l'installazione di IBM Intelligent Operations Center è stata completata. Tali strumenti possono essere eseguiti anche quando il sistema è in produzione, per individuare e correggere le vulnerabilità che si potrebbero creare quando altri prodotti vengono installati sui server o come risultato dell'utilizzo del sistema.

### Scanner della vulnerabilità

Lo scanner è composto da script che esaminano il sistema IBM Intelligent Operations Center e identificano le vulnerabilità. Ad esempio, lo scanner identifica le directory con privilegi di scrittura per un qualsiasi utente.

Lo scanner crea un file di risultati utilizzato dagli script di soluzione. L'elenco dei file di risultati ha identificato le vulnerabilità all'interno del sistema IBM Intelligent Operations Center.

Gli script degli scanner non apportano modifiche al sistema IBM Intelligent Operations Center. Lo scanner identifica solo le vulnerabilità. Può essere utilizzato dopo la soluzione per convalidare le modifiche apportate dagli script di soluzione.

### Script di soluzione delle vulnerabilità

Cyber Hygiene dispone di tre tipi di script di soluzione:

- Script che effettuano modifiche alla configurazione che non richiedono la scansione, che possono essere facilmente ripristinate o che non presentano alcun impatto runtime rilevante sul sistema. Ad esempio, la modifica dell'autorizzazione di accesso al file delle pagine man in 644.
- Uno script per disabilitare l'accesso remoto con l'account root.
- Uno script che elabora il file dei risultati creato dallo scanner e risolve le vulnerabilità identificate.

Prestare cautela quando si utilizza questo script dopo che sono stati aggiunti ulteriori progetti. Alcuni prodotti richiedono impostazioni meno restrittive e potrebbero non funzionare correttamente dopo l'esecuzione di questi script. Esaminare i file dei risultati creati dagli script dello scanner per potenziali rischi prima di eseguire eventuali script di soluzione.

### Log di soluzione

Gli script di scansione e di soluzione registrano le relative azioni in quattro file di log su ciascun server IBM Intelligent Operations Center. Questi log si trovano nella directory `/var/BA15/CH/results`. Le sottodirectory contengono copie di lavoro dei risultati della scansione e della soluzione.


Lo scanner viene eseguito due volte: una volta per risolvere le vulnerabilità e una seconda volta per registrare le soluzioni non eseguite. Il log della seconda esecuzione può essere utilizzato dall'amministratore per determinare se sono richieste operazioni di soluzione manuali.

## Documentazione Cyber hygiene

È disponibile della documentazione per aiutare il cliente nella valutazione delle modifiche applicate al sistema installato IBM Intelligent Operations Center. Questa documentazione fornisce assistenza con la certificazione e l'accreditamento dei sistemi per l'utilizzo di produzione.

La documentazione include una panoramica della strategia cyber hygiene generale, la logica dietro l'implementazione di alcuni valori predefiniti ed un foglio di lavoro che documenta lo stato di ciascuna vulnerabilità DISA indicata. Il foglio di lavoro può essere utilizzato durante la definizione della sicurezza del prodotto.

**Informazioni correlate:**

 Implementazione di Cyber hygiene in IBM Intelligent Operations Center 1.5

---

## Capitolo 4. Integrazione della soluzione

I prodotti e servizi possono essere integrati con il IBM Intelligent Operations Center che incorpora i dati correlati agli eventi.

I dati evento comunicati al IBM Intelligent Operations Center possono essere nel CAP (Common Alerting Protocol) o in altri protocolli.

Gli eventi possono essere correlati a KPI (key performance indicators) monitorati dal IBM Intelligent Operations Center. Gli eventi nel IBM Intelligent Operations Center possono essere correlati anche a procedure operative standard e alle risorse disponibili. La soluzione fornisce un servizio amministrazione di report pertanto l'utente può produrre report e riepiloghi aggiornati dei propri dati evento.

---

### Esempi dei sistemi che possono essere integrati

Prodotti e servizi possono essere integrati con il IBM Intelligent Operations Center.

Esempi di sistemi e servizi comprendono:

- Sistemi che informano sui problemi di incolumità pubblica.
- Sistemi che informano sugli eventi del traffico
- Sistemi che informano sull'utilizzo e la qualità dell'acqua.
- Sistemi che forniscono dati sull'interruzione e lo stato dei relativi ordini di lavoro.

Questi sistemi devono essere in grado di comunicare con il IBM Intelligent Operations Center e di inviare gli eventi e le misurazioni nel protocollo supportato alla coda eventi in ingresso IBM Intelligent Operations Center.

#### Concetti correlati:

“Utilizzo della coda eventi in entrata definita per il IBM Intelligent Operations Center” a pagina 100

Gli eventi CAP possono essere pubblicati nel IBM Intelligent Operations Center indirizzandoli nell'istanza inclusa WebSphere Message Broker.

“Integrazione con CAP (Common Alerting Protocol)” a pagina 93

Il CAP (Common Alerting Protocol) viene utilizzato per scambiare informazioni evento tra il IBM Intelligent Operations Center e i sistemi esterni.

---

### Integrazione punti e protocolli

Altri sistemi possono essere integrati con la soluzione attraverso i servizi e le politiche IBM Intelligent Operations Center. I dati possono essere ricevuti nel formato CAP (Common Alerting Protocol); sono anche supportati altri protocolli.

### Eventi e KPI

IBM Intelligent Operations Center elabora gli eventi e i KPI (key performance indicators) per determinare come visualizzare le informazioni.

Altri prodotti e servizi possono essere integrati con il IBM Intelligent Operations Center attraverso il servizio di bus dei messaggi. I KPI vengono monitorati dal servizio di monitoraggio del business.

Gli eventi ricevuti dal IBM Intelligent Operations Center. Questi eventi possono essere visualizzati in un portlet Dettagli e possono influenzare su ciò che viene visualizzato nei portlet della mappa.

Una definizione KPI determina come vengono visualizzati i KPI in Stato e portlet Drill Down KPI (Key Performance Indicator). La definizione KPI può anche determinare quali informazioni relative agli eventi vengono visualizzate. Ad esempio, se viene superata una soglia KPI, l'evento dovrebbe essere contrassegnato con un'alta urgenza o gravità. Gli eventi senza corrispondenti definizioni KPI vengono visualizzate in base alle informazioni relative all'evento ricevute.

Per ulteriori informazioni relative ai KPI che vengono creati e integrati, consultare il link alla fine di questo argomento.

**Concetti correlati:**

“Creazione ed integrazione dei KPI” a pagina 109

I modelli KPI (Key performance indicator) possono essere creati e modificati utilizzando un toolkit di sviluppo del monitoraggio di business e un portlet di gestione KPI.

**Politica per gli aggiornamenti del KPI**

La politica IBM Intelligent Operations Center determina se un evento in ingresso è un aggiornamento dell'evento KPI, quindi lo invia per l'elaborazione per generare un aggiornamento KPI o un avviso a seconda dei parametri. Un evento KPI viene determinato da `<code>KPI</code>` nel blocco avvisi dell'XML CAP (Common Alerting Protocol).

Se l'evento è confermato come un aggiornamento KPI, la politica verifica i parametri KPI e genera un XML evento KPI da inviare a IBM WebSphere Business Monitor per l'elaborazione.

La seguente tabella mostra un aggiornamento di evento KPI di esempio.

*Tabella 29. Proprietà evento KPI di esempio*

Proprietà	Valore
Mittente	security@rtp.city.gov
Tipo evento	Tempo di risposta al crimine
Stato evento	Effettivo - attivabile da tutti i destinatari
Ambito evento	Pubblico - Per la distribuzione generale a destinatari non ristretti
Categoria	Sicurezza
Gravità	Grave
Certezza	Probabile
Urgenza	Immediato
Tipo di messaggio	Avviso - informativa iniziale che richiede attenzione da parte dei destinatari
Descrizione	Furto
Inviato data/ora	12 -02- 2012 17T17:06:00+01:00
data /ora di inizio	02-2012 - 16T15:47:00+01:00
Data /ora di risposta	02-2012 - 17T17:06:00+01:00

La seguente tabella mostra i parametri KPI di esempio associati all'aggiornamento evento KPI in Tabella 29.

*Tabella 30. Parametri evento KPI di esempio*

Parametro	Valore
Numero report	1111
Distretto	Distretto uno
Risposta	02-2011 15T15:05:07-05:00

**Concetti correlati:**

“Stato” a pagina 291

Utilizzare il portlet Stato per visualizzare lo stato degli indicatori KPI (key Performance Indicator) per una singola organizzazione o per più organizzazioni.

“Notifiche” a pagina 287

Utilizzare il portlet Notifiche per visualizzare i messaggi di avviso ed i relativi dettagli.

## Integrazione con CAP (Common Alerting Protocol)

Il CAP (Common Alerting Protocol) viene utilizzato per scambiare informazioni evento tra il IBM Intelligent Operations Center e i sistemi esterni.

Il CAP è un formato generico per lo scambio di avvisi di emergenza e gli avvisi pubblici su diverse reti. Fornisce un formato messaggio digitale non proprietario, aperto per tutti i tipi di avvisi e di notifiche. Il CAP è compatibile con le nuove tecniche come ad esempio i servizi web offrendo funzionalità avanzate. Queste funzionalità comprendono:

- Destinazione geografica flessibile che utilizza le forme latitudine e longitudine e altre rappresentazioni geospaziali in tre dimensioni.
- Messaggistica multilingue e per più destinatari
- Tempi di validità e scadenze tempificati e ritardati
- Funzioni avanzate di aggiornamento e cancellazione dei messaggi
- Supporto di template per strutturare messaggi di avviso validi e completi
- Codifica digitale e compatibilità di firma
- Immagini digitali e funzioni audio

Gli eventi sono messaggi di dati contenuti autonomamente che possono essere inviati o utilizzati da tutti i componenti. Gli eventi possono essere pubblicati in code argomento e letti da tutti i sistemi IT di sottoscrizione potenzialmente interessati. Il CAP guida a standardizzare il contenuto evento in modo che più domini possono inviare e ricevere eventi in un formato comune che utilizza convenzioni comuni. Lo standard definisce i campi facoltativi ed obbligatori nel record evento e i valori accettabili per tali campi. La gestione dell'elaborazione dell'evento può mediare tra i formati legacy e il formato standardizzato. Il CAP può essere esteso per gestire operazioni correnti oltre alle situazioni di emergenza.

Gli eventi devono contenere almeno:

- un identificativo univoco che contiene:
  - il mittente (sistema o persona)
  - Organizzazione che invia l'evento
  - Numero seriale all'interno del sistema di invio
  - Data/ora di creazione dell'evento
- Informazioni che consentono ai destinatari di definire e assegnare la priorità alle risposte:
  - Urgenza – quanto rapidamente i destinatari devono rispondere all'avviso
  - Il livello di pericolo per la vita e la proprietà
  - Certezza – una probabilità che va dal 100%, l'evento è stato osservato, allo 0%, non si prevede che si verifichi l'evento.
  - Previsione temporale per gli eventi che possono accadere in futuro.
  - Durata degli eventi che sono stati precedentemente riportati e la cui continuità è stata riportata.
  - Durata prevista degli eventi che rappresentano una situazione che non può essere risolta rapidamente.
  - Azioni e direttive consigliate e obbligatorie
- Informazioni per consentire di correlare l'evento:

- Riferimenti al modello semantico della città (se esiste)
- Coordinate geospaziali
- Riferimento all'evento prerequisito o ad un evento che è stato la causa scatenante.
- Identificativi asset univoci per gli asset interessati.
- Descrizioni testuali leggibili dall'uomo:
  - Descrizione ubicazione
  - Descrizione attività

L'utilizzo di CAP aiuta a rendere minimo lo scambio di dati per l'evento. Poiché gli eventi sono formattati in XML, il formato dei dati può essere scritto e letto da diversi sistemi evitando così lo scambio di dati inutili o di generare confusione.

Il IBM Intelligent Operations Center fornisce un archivio persistente degli avvisi CAP e un'interfaccia standard per la loro presentazione.

Mentre l'intera struttura CAP è accettata dal IBM Intelligent Operations Center, vengono utilizzati solo alcuni dati dal IBM Intelligent Operations Center durante il calcolo di KPI (key performance indicators).

Il IBM Intelligent Operations Center utilizza il WebSphere Message Broker per integrare gli eventi che utilizzano il CAP.

Il IBM Intelligent Operations Center supporta OASIS CAP (Common Alerting Protocol) Versione 1.2.

#### Concetti correlati:

“Utilizzo CAP per eventi KPI” a pagina 96

Il WebSphere Message Broker, che è fornito come parte di IBM Intelligent Operations Center, accetta messaggi di evento CAP ed utilizza i dati nei calcoli KPI (Key performance indicator).

“Utilizzo del CAP per gli eventi non KPI” a pagina 99

È possibile anche utilizzare i dati CAP per fornire i dati per gli eventi non associati ai calcoli KPI.

#### Informazioni correlate:

 OASIS Common Alerting Protocol Versione 1.2

### Struttura CAP

Ogni messaggio di avviso CAP è costituito da un segmento <alert> che può contenere uno o più segmenti <info>. Ciascun segmento <info> può includere uno o più segmenti <area>. Nella maggior parte dei casi, i messaggi CAP con un <msgType>, con un valore *alert* include almeno un elemento <info>.

Di seguito sono riportati gli elementi principali del messaggio.

- <alert>

Il segmento <alert> fornisce informazioni di base relative al messaggio corrente: lo scopo, l'origine e il relativo stato. Inoltre, ha un identificativo univoco per il messaggio e link a tutti gli altri messaggi correlati. Un segmento <alert> può essere utilizzato da solo per le conferme del messaggio, per gli annullamenti o per altre funzioni di sistema; tuttavia, la maggior parte dei segmenti degli avvisi includono almeno un segmento <info>.

- <info>

Il segmento <info> descrive un evento attuale o anticipato in termini di urgenza (il tempo disponibile per preparare), gravità (l'intensità dell'impatto) e certezza (la fiducia nell'osservazione o previsione). Inoltre fornisce sia le descrizioni della categoria e testuale dell'evento. Il segmento <info> potrebbe inoltre fornire istruzioni per una risposta adeguata dai destinatari dei messaggi e altri dettagli, ad esempio durata del pericolo, i parametri tecnici, informazioni di contatto e link a fonti di informazioni aggiuntive. Più segmenti <info> possono essere utilizzati per descrivere i diversi parametri, ad esempio bande di intensità o probabilità differenti o per fornire le informazioni in più lingue.



- <resource>

Il segmento <resource> fornisce un riferimento facoltativo per informazioni aggiuntive relative al segmento <info>. Potrebbe fare riferimento a un asset digitale come un file di immagini o audio.

- <area>

Il segmento <area> descrive un'area geografica a cui viene applicato il segmento <info>. Le descrizioni di testo e codificate (ad esempio i codici postali) sono supportate, ma la rappresentazione preferita utilizza forme geospaziali, poligoni e cerchi e un'altitudine o un intervallo di altitudini espresso in termini di latitudine, longitudine e altitudine standard conformemente ad un dato geospaziale specificato.

#### Concetti correlati:

“Utilizzo CAP per eventi KPI” a pagina 96

Il WebSphere Message Broker, che è fornito come parte di IBM Intelligent Operations Center, accetta messaggi di evento CAP ed utilizza i dati nei calcoli KPI (Key performance indicator).

“Utilizzo del CAP per gli eventi non KPI” a pagina 99

È possibile anche utilizzare i dati CAP per fornire i dati per gli eventi non associati ai calcoli KPI.

## Tipi di evento

Numerosi tipi di evento CAP sono supportati da IBM Intelligent Operations Center.

### Evento effettivo/previsto

I messaggi di evento effettivi/previsti sono messaggi non richiesti inviati da diversi domini sulle condizioni anomale o sulle eccezioni. Questi messaggi riguardano anche le violazioni KPI (Key Performance Indicator) in cui viene creato un evento.

### Conferma

Una conferma è un messaggio CAP con i seguenti valori di campo nell'elemento <alert>:

- Il valore <msgType> è impostato su **ACK**, che significa che il mittente ha confermato la ricezione e l'accettazione dei messaggi identificati in <references>.
- Il campo <references> contiene gli identificativi di messaggio esteso (nel formato sender, identifier, sent) di un messaggio CAP precedente o di messaggi a cui fa riferimento la conferma.
- 

**Nota:** L'elemento <info> è facoltativo per una conferma.

### Risposta

Una risposta è un messaggio CAP con i seguenti valori del campo nell'elemento <alert>:

- Il valore <msgType> è **Avviso**.
- Il valore <note> è **Risposta**.
- L'elemento <references> deve contenere gli identificativi del messaggio CAP per il quale questa è una risposta

Ad esempio, quando un operatore città invia un **City Brownout Advisory** ai diversi domini, tali domini restituiscono una risposta all'advisory dopo l'esecuzione di un'analisi dell'impatto sulle singole funzioni.

### Incidente

Gli incidenti vengono utilizzati per raccogliere i messaggi che fanno riferimento ai diversi aspetti dello stesso incidente. I messaggi CAP dell'incidente agiscono come contenitore di tutti gli eventi che sono correlati ad un evento specifico. Questi eventi possono trovarsi in domini differenti.

Un advisory viene promosso ad incidente quando i domini restituiscono all'advisory risposte indicando un impatto multi-dominio che richiede un'azione coordinata. L'elemento <incident> in tutti gli eventi correlati viene popolato con il valore <identifier> dell'evento incidente. Gli eventi correlati sono eventi in cui il valore <references> è uguale al valore <identifier> dell'evento incidente.

Un incidente è un messaggio CAP con i seguenti valori del campo nell'elemento <alert>:

- Il valore <msgType> è **Avviso**.
- Il valore <note> è **Incidente**.
- L'elemento <references> deve contenere gli identificativi del messaggio CAP che è l'elemento principale (la causa principale) di questo evento
- L'elemento <incidents> deve contenere il proprio identificativo

## Aggiorna

Un aggiornamento è un messaggio CAP con i seguenti valori di campo nell'elemento <alert>:

- L'elemento <msgType> è impostato su **aggiorna**, che significa che questo aggiornamento sostituisce i precedenti i messaggi identificati nell'elemento <references>.
- L'elemento <references> contiene gli identificativi di messaggio esteso (nel formato sender, identifier, sent) di un messaggio CAP precedente o di messaggi a cui fa riferimento l'aggiornamento.

## Annulla

Un annullamento è un messaggio CAP con i seguenti valori del campo nell'elemento <alert>:

- L'elemento <msgType> è impostato su **Annulla** che significa che questo messaggio annulla i messaggi precedenti i messaggi identificati nell'elemento <references>.
- L'elemento <references> contiene gli identificativi di messaggio esteso (nel formato sender, identifier, sent) di un messaggio CAP precedente o di messaggi a cui fa riferimento l'annullamento.
- L'elemento <note> contiene una spiegazione del perché o del come questo avviso viene cancellato.

### Informazioni correlate:

 OASIS Common Alerting Protocol Version 1.2

## Utilizzo CAP per eventi KPI

Il WebSphere Message Broker, che è fornito come parte di IBM Intelligent Operations Center, accetta messaggi di evento CAP ed utilizza i dati nei calcoli KPI (Key performance indicator).

Tabella 31 elenca gli elementi di dati utilizzati nei calcoli KPI.

Tabella 31. Gli elementi CAP utilizzati nei calcoli KPI IBM Intelligent Operations Center

Obbligatorio o facoltativo	Elemento di dati (normativo)	Descrizione
Obbligatorio	Message_ID (identificativo)	Identificativo univoco del messaggio
Obbligatorio	Sender_ID (mittente)	Identificativo univoco del mittente

Tabella 31. Gli elementi CAP utilizzati nei calcoli KPI IBM Intelligent Operations Center (Continua)

Obbligatorio o facoltativo	Elemento di dati (normativo)	Descrizione
Obbligatorio	SentDateTime (inviato)	data ed ora il cui il messaggio è stato inviato.  Ad esempio: 02-2011 -07T 16:49:00-05:00 contiene la data e l'ora in cui è stato inviato un messaggio. Gli ultimi sei caratteri indicano il fuso orario dell'evento CAP rispetto a GMT (Greenwich Mean Time) In questo caso, l'evento si è verificato alle 16:49:00, al GMT meno 5 ore che è EST (Eastern Standard Time). Questo codice indica che quando l'evento viene visualizzato, viene convertito da EST al fuso orario dell'utente. Se invece si desidera codificare gli eventi CAP in GMT, modificare il suffisso in -00:00 come in questo esempio: 2011-02-07T 16:49:00-00:00.
Obbligatorio	MessageStatus (stato)	Stato del messaggio, può essere una delle seguenti opzioni: <ul style="list-style-type: none"> <li>• Effettivo</li> <li>• Esercizio</li> <li>• Sistema</li> <li>• Test</li> <li>• Bozza</li> </ul>
Obbligatorio	MessageType (msgType)	Tipo di messaggio, può essere una delle seguenti opzioni: <ul style="list-style-type: none"> <li>• Avviso</li> <li>• Aggiorna</li> <li>• Annulla</li> <li>• Ack</li> <li>• Errore</li> </ul>
Facoltativo	Origine (origine)	Origine del messaggio
Obbligatorio	Ambito (ambito)	Contiene il valore Pubblico
Obbligatorio	Codice (codice)	Contiene il valore KPI per nascondere questo evento dall'elenco del portlet Eventi
Obbligatorio	EventCategory (categoria)	Una delle seguenti: <ul style="list-style-type: none"> <li>• Geo</li> <li>• Met</li> <li>• Incolunità</li> <li>• Sicurezza</li> <li>• Salvataggio</li> <li>• Incendio</li> <li>• Salute</li> <li>• Env</li> <li>• Trasporti</li> <li>• Infra</li> <li>• CBRNE</li> <li>• Altro</li> </ul>
Obbligatorio	EventType (evento)	Descrizione dell'evento o KPI.  Ad esempio: Budget_Distretto_di_Polizia

Tabella 31. Gli elementi CAP utilizzati nei calcoli KPI IBM Intelligent Operations Center (Continua)

Obbligatorio o facoltativo	Elemento di dati (normativo)	Descrizione
Obbligatorio	Urgency (urgenza)	Una delle seguenti: <ul style="list-style-type: none"> <li>• Immediata</li> <li>• Prevista</li> <li>• Futura</li> <li>• Passata</li> <li>• Sconosciuta</li> </ul>
Obbligatorio	Severity (gravità)	La gravità viene indicata da una delle seguenti opzioni: <ul style="list-style-type: none"> <li>• Estrema</li> <li>• Grave</li> <li>• Moderata</li> <li>• Minore</li> <li>• Sconosciuta</li> </ul>
Obbligatorio	Certainty (certezza)	La certezza viene indicata da una delle seguenti opzioni: <ul style="list-style-type: none"> <li>• Osservata</li> <li>• Probabile</li> <li>• Possibile</li> <li>• Improbabile</li> <li>• Sconosciuta</li> </ul>
Facoltativo	EventCode (eventCode)	coppie nome-valore per l'immissione evento.
Facoltativo	OnsetDateType (data di inizio)	Data e ora in cui inizia l'evento Ad esempio: 02-2011 -08T16:49:00-05:00
Facoltativo	SenderName (senderName)	Nome dell'entità che ha inviato l'avviso. Ad esempio Distretto di polizia
Facoltativo	EventDescription (descrizione)	Descrizione dettagliata dell'evento o KPI
Facoltativo	Parameter (parametro)	Ulteriori dati associati all'evento o KPI.
Facoltativo	AreaGeocode (geocode)	Un campo che è possibile utilizzare per fornire le informazioni quando l'evento o KPI dipendono dall'ubicazione.

Per ulteriori informazioni, consultare il link correlato alla fine di questo argomento alla specifica CAP (Common Alerting Protocol) OASIS.

Il seguente codice rappresenta un esempio di un evento che riporta un incidente automobilistico.

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
  <cap:identifier>1112</cap:identifier>
  <cap:sender>Transportation</cap:sender>
  <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
  <cap:status>Actual</cap:status>
  <cap:msgType>Alert</cap:msgType>
  <cap:scope>Public</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
```

```

<cap:category>Transport</cap:category>
<cap:event>Traffic_Accident</cap:event>
<cap:urgency>Unknown</cap:urgency>
<cap:severity>Extreme</cap:severity>
<cap:certainity>Unknown</cap:certainity>
<cap:eventCode>
  <cap:valueName>OwningOrg</cap:valueName>
  <cap:value>Police</cap:value>
</cap:eventCode>
<cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
<cap:senderName>Transportation</cap:senderName>
<cap:description>Single car crash</cap:description>
<cap:parameter>
  <cap:valueName>accident number</cap:valueName>
  <cap:value>1112</cap:value>
</cap:parameter>
</cap:info>
</cap:alert>

```

#### Concetti correlati:

“Localizzazione dell'interfaccia utente” a pagina 141

Le impostazioni del browser determinano le impostazioni di lingua, data e ora per l'interfaccia utente di IBM Intelligent Operations Center. Un amministratore può personalizzare il formato di data e ora.

“Problemi noti e soluzioni” a pagina 328

Questa sezione contiene un elenco di problemi che si verificano comunemente e una soluzione per ciascun elemento.

#### Informazioni correlate:

 OASIS Common Alerting Protocol Versione 1.2

### Utilizzo del CAP per gli eventi non KPI

È possibile anche utilizzare i dati CAP per fornire i dati per gli eventi non associati ai calcoli KPI.

I dati CAP ricevuti dal IBM Intelligent Operations Center che non sono associati a KPI definiti, vengono aggiunti ai portlet Eventi eMappa nel IBM Intelligent Operations Center.

Il seguente codice è un esempio di evento non KPI. Considerare che per gli eventi non KPI, è necessario impostare il valore del tag code a Event.

```

<p>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T15:47:24-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <restriction/>
  <code>Event</code>
  <info>
    <language>en_US</language>
    <category>Infra</category>
    <event>Water Main Break</event>
    <urgency>Immediate</urgency>
    <severity>Moderate</severity>
    <certainity>Observed</certainity>
    <headline>Major water line leak at NW 20th St.</headline>
    <description>Leak is located at the intersection of NW 20th Street and NW 9th Avenue. Street flooding starting to occur. Immediate action required.</description>
    <area>
      <circle>25.79518,-80.21110 0</circle>

```

```
</area>
</info>
</alert>
</p>
```

## Utilizzo della coda eventi in entrata definita per il IBM Intelligent Operations Center

Gli eventi CAP possono essere pubblicati nel IBM Intelligent Operations Center indirizzandoli nell'istanza inclusa WebSphere Message Broker.

I client di pubblicazione possono essere configurati per puntare direttamente alla coda di input dell'evento CAP oppure possono utilizzare le risorse JMS WebSphere Message Broker WebSphere Application Server definite nel server portale. Queste risorse JMS puntano alla coda WebSphere Message Broker che riceve gli eventi CAP. Le seguenti risorse JMS vengono create quando viene installato IBM Intelligent Operations Center:

- Factory di connessione alla coda
  - Nome: `ioc.mb.con.factory`
  - Nome JNDI: `jms/ioc.mb.con.factory`
- Coda
  - Nome: `ioc.cap.in.q`
  - Nome JNDI: `jms/ioc.cap.in.q`

### Concetti correlati:

“Comunicazione evento KPI tra IBM WebSphere Business Monitor e IBM Intelligent Operations Center” a pagina 116

IBM WebSphere Business Monitor può inviare eventi in uscita da un contesto di monitoraggio o di KPI (key performance indicator) a IBM Intelligent Operations Center.

## Creazione di eventi utilizzando il servizio Publisher

È possibile inoltrare gli eventi a IBM Intelligent Operations Center attraverso i servizi web al servizio Publisher.

È possibile creare le applicazioni client che possono essere integrate nell'istanza distribuita di IBM Intelligent Operations Center. È possibile utilizzare un'applicazione client per passare gli avvisi CAP da un'applicazione client di terze parti a IBM Intelligent Operations Center chiamando i metodi illustrati dalla classe del programma di utilità del servizio Publisher e il servlet IBM Intelligent Operations Center.

## Sviluppo con le classi del programma di utilità comuni

Se si desidera creare un'applicazione client che chiama il servizio Publisher, prima di iniziare è necessario impostare le classi del programma di utilità comuni. Una volta terminato lo sviluppo dell'applicazione client, esportarla come un file WAR che poi si importa in WebSphere Application Server.

### Informazioni su questa attività

Utilizzare la seguente procedura se si desidera sviluppare un'applicazione client con le classi del programma di utilità comuni.

- Prima di sviluppare l'applicazione client, aggiungere i file JAR `iss_common` e `icu4j-4_4_2` al percorso di build del progetto. I file JAR sono richiesti durante la compilazione.
- Una volta sviluppata l'applicazione client, esportarla come un file WAR.
- Importare il file WAR in WebSphere Application Server e configurarlo per fare riferimento alle librerie condivise.

### Procedura

1. Individuare il file `iss_common.jar` e il file `icu4j-4_8_1_1.jar` nella directory di installazione IBM Intelligent Operations Center, `/opt/IBM/iss/common/lib`.

2. Copiare il file `iss_common.jar` e il file `icu4j-4_8_1_1.jar` in un'ubicazione sulla propria macchina di sviluppo.
3. Per aggiungere i file JAR al percorso di build del progetto, nell'API IBM Intelligent Operations Center, eseguire le seguenti operazioni secondarie per `iss_common.jar` e `icu4j-4_8_1_1.jar`:
  - a. Fare clic con il tasto destro del mouse su **Progetto portlet**.
  - b. Fare clic su **Percorso di build > Configura percorso di build**.
  - c. Fare clic nella scheda **Librerie** e fare clic su **Aggiungi JAR esterni ....**
  - d. Cercare la directory che contiene il file JAR.
  - e. Fare clic sul file JAR e quindi fare clic su **Apri**.
4. Una volta terminato lo sviluppo dell'applicazione client, esportarla come un file WAR.
5. Nella console di gestione WebSphere Application Server utilizzare la procedura guidata di importazione per importare il file WAR dell'applicazione client.
6. Per configurare il file WAR per fare riferimento ai riferimenti della libreria condivisa, eseguire le seguenti operazioni.
  - a. Nella console di gestione WebSphere Application Server selezionare la casella di spunta accanto al file WAR importato e quindi fare clic su **Aggiorna**.
  - b. Fare clic su **Riferimenti libreria condivisa**.
  - c. Nella finestra Riferimenti libreria condivisa, selezionare la casella di spunta **Applicazione**.
  - d. Fare clic su **Fai riferimento alle librerie condivise**.
  - e. Spostare **ISSCommonJars** e **IOCCCommonJars** dall'elenco Disponibile all'elenco Selezionato e quindi fare clic su **OK**.
  - f. Per salvare le modifiche fare clic su **OK**.

## Utilizzo del servizio Publisher

Lo strumento iniettore evento del servizio Publisher viene fornito come un programma di utilità Java. È possibile creare un'applicazione client che passa l'XML CAP al IBM Intelligent Operations Center chiamando i metodi presentati dal servizio Publisher. È possibile anche passare le notifiche.

Il servizio Publisher è una classe del programma di utilità nel progetto `iss_common_utils`, che è creata nel file `iss_common.jar`. Il servizio Publisher espone i metodi statici `publishEvent` e `publishNotification`. Prima di creare le applicazioni client per il servizio Publisher, è necessario impostare le classi comuni del programma di utilità. Per ulteriori informazioni, consultare il link alla fine di questo argomento.

Per garantire che il codice utilizzato per chiamare il servizio Publisher ha accesso alle configurazioni coda JMS corrette, è necessario distribuirlo sul server delle applicazioni.

Il seguente esempio di codice mostra come chiamare il servizio Publisher.

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);

if (status == Publisher.STATUS_SUCCESS) {
    logger.traceFine(this, methodName, "Event submit request was performed successfully");
}
else if (status == Publisher.STATUS_EXCEPTION_NAMING) {
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Requires defining JMS Resources.");
}
else if (status == Publisher.STATUS_EXCEPTION_JMS) {
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Failed to connect to JMS resources.");
}
else { //Other error code
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Returned status = " + status);
}
```

Se si utilizza il portlet Publisher di esempio, non è necessario creare il codice per chiamare il servizio Publisher o per scrivere i messaggi CAP.

#### Concetti correlati:

“Publisher di esempio” a pagina 103

Utilizzare il portlet Publisher di esempio per pubblicare gli eventi CAP (Common Alerting Protocol) su IBM Intelligent Operations Center.

#### Attività correlate:

“Sviluppo con le classi del programma di utilità comuni” a pagina 100

Se si desidera creare un'applicazione client che chiama il servizio Publisher, prima di iniziare è necessario impostare le classi del programma di utilità comuni. Una volta terminato lo sviluppo dell'applicazione client, esportarla come un file WAR che poi si importa in WebSphere Application Server.

### Utilizzo del servlet Publisher

Il servlet Publisher accetta i parametri nelle richieste POST per pubblicare XML CAP, creare nuovi eventi o creare eventi modificati da eventi o incidenti esistenti.

### Invio di richieste POST al servlet Publisher

Il servlet Publisher chiama il servizio Publisher per inserire l'XML CAP nelle code che alimentano nel IBM Intelligent Operations Center. Il servlet Publisher è ubicato in `/ibm/iss/common/rest/publisher`. La seguente tabella mostra in che modo inviare le richieste POST al servlet Publisher.

Tabella 32. Richieste POST del servlet Publisher

Tipo di evento da pubblicare	Codice richiesta POST
Pubblica un nuovo evento CAP	<code>action=publishEvent&amp;source=xml&amp;xml=CAP_event_XML</code>
Modifica un evento esistente	<code>action=publishEvent&amp;source=existing&amp;id=event_id</code>
Pubblica un nuovo evento vuoto	<code>action=publishEvent&amp;source=new</code>

### Parametri facoltativi

È possibile applicare i parametri facoltativi per ognuna delle opzioni di pubblicazione accodando il codice di seguito riportato alla richiesta POST: `&nome_parametro=nuovo_valore`

Sono disponibili i seguenti parametri facoltativi:

- areaDesc
- categoria
- certezza
- codice
- contatto
- descrizione
- evento
- titolo
- latitudine
- longitudine
- msgType
- rendi casuale
- reso casuale
- randomizeArea
- randomizeTime



- mittente
- senderName
- gravità
- stato
- urgenza

Ad esempio, per pubblicare un nuovo evento vuoto e quindi impostare il titolo su Traffic, il codice della richiesta POST è: `servletURL&action=publishEvent&source=new&headline=Traffic Accident`

---

## Creazione e pubblicazione degli eventi di test

Il IBM Intelligent Operations Center fornisce il portlet Publisher di esempio e il portlet Programmazione script di eventi per la creazione e pubblicazione degli eventi di test.

### Concetti correlati:

“Creazione di eventi utilizzando il servizio Publisher” a pagina 100

È possibile inoltrare gli eventi a IBM Intelligent Operations Center attraverso i servizi web al servizio Publisher.

## Publisher di esempio

Utilizzare il portlet Publisher di esempio per pubblicare gli eventi CAP (Common Alerting Protocol) su IBM Intelligent Operations Center.

Il portlet Publisher di esempio è uno strumento di test automatizzato rivolto a un amministratore che gestisce o verifica la soluzione. Un amministratore può utilizzare il portlet Publisher di esempio come applicazione client per eseguire il test della pubblicazione di messaggi CAP in IBM Intelligent Operations Center. Il portlet Publisher di esempio può eliminare il requisito per la creazione manuale di un'applicazione client del test.

## Creazione di eventi e notifiche

Per avviare il portlet Publisher di esempio, nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di dimostrazione > Publisher eventi di esempio**.

Nella scheda **CAP evento** del portlet Publisher di esempio, è possibile completare un modulo per progettare eventi con XML. Inoltrare il modulo per attivare un flusso di eventi CAP di esempio nel sistema.

Il portlet Publisher di esempio contiene inoltre una scheda **Modulo evento** per la creazione di nuovi eventi quando non è necessario modificare l'XML. Completare il modulo nella scheda **Modulo evento** per inoltrare i dettagli dell'evento CAP. Se si desidera creare nuovi eventi con proprietà basate sulle proprietà di un evento esistente, immettere l'ID avviso CAP per l'evento esistente nel campo **ID**.

Il portlet Publisher di esempio contiene la scheda **Notifica** per la verifica del sottosistema di notifiche di IBM Intelligent Operations Center. Nella scheda **Notifica** è possibile completare un modulo per l'inoltro di una notifica di avviso per i gruppi specificati. I valori immessi nel campo **Inviato a gruppi** devono corrispondere ai gruppi di utenti esistenti, ad esempio CityWideOperator, CityWideExecutive, poiché solo gli avvisi corrispondenti vengono visualizzati nell'elenco di portlet Notifiche.

## Valori casuali

Nelle schede **CAP evento** e **Modulo evento**, se si seleziona la casella di spunta **Rendi evento casuale**, il portlet modifica automaticamente le proprietà degli eventi che pubblica nel modo seguente:

- **ID**: il portlet genera una stringa ID univoca per ciascun evento poiché gli ID evento devono essere univoci in IBM Intelligent Operations Center.

- **Data/ora:** il portlet incrementa il valore di data/ora per ciascun evento inviato nella sequenza, in modo che l'arrivo avvenga in momenti diversi.
- **Ubicazione:** il portlet esegue la randomizzazione della latitudine e della longitudine per ciascun evento, all'interno di un intervallo, per essere conformi con il formato richiesto per latitudine, longitudine e raggio; ad esempio, 32.9525,-115.5527 5. L'impostazione del raggio non viene modificata.

## Personalizzazione del portlet Publisher di esempio

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

### Riferimenti correlati:

“Impostazioni portlet Publisher di esempio” a pagina 163

Personalizzare il portlet Publisher di esempio modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Creazione di eventi di esempio con XML

Nella scheda **CAP evento** è possibile selezionare un template di evento CAP che è possibile utilizzare per visualizzare, modificare e pubblicare eventi.

## Prima di iniziare

Inizialmente scegliere una categoria di evento. Le categorie rappresentano le aree principali in cui vengono divisi gli eventi.

Tabella 33. Categorie di evento

Categoria	Descrizione
CBRNE	Minaccia o attacco CBRNE (chemical, biological, radiological, nuclear o high-yield explosive)
Ambientale	Inquinamento e altri eventi ambientali
Incendio	Spegnimento incendio e salvataggio
Geofisico	Evento geofisico incluso le frane
Salute	Evento medicina e salute pubblica
Infrastruttura	Evento servizi, telecomunicazioni ed altre infrastrutture non legate ai trasporti
Meteorologico	Evento meteorologico compreso le inondazioni
Salvataggio	salvataggio e recupero
Incolunità	Emergenza generale e incolumità pubblica
Protezione	Applicazione della legge, forze armate, sicurezza interna, locale e privata
Trasporti	Trasporti pubblici e privati
Altro	Altri eventi

## Informazioni su questa attività

Per ulteriori informazioni sulle proprietà di eventi, consultare il link alla fine dell'argomento per l'argomento del portlet **Dettagli**.

## Procedura

1. Nell'interfaccia di gestione WebSphere Portal fare clic su **Intelligent Operations > Strumenti di dimostrazione > Publisher eventi di esempio**.
2. Fare clic sulla scheda **CAP evento**.

3. Dall'elenco **Categoria** selezionare una categoria di evento.
4. Per il campo **Messaggio evento** scegliere una delle seguenti opzioni:
  - Per inserire l'XML per il corrispondente messaggio CAP scritto in precedenza automaticamente nel campo **Messaggio evento** dall'elenco **Evento di esempio** selezionare un evento. Se si desidera modificare l'XML per adattarlo alle proprie esigenze.
  - Nel campo **Messaggio evento** immettere manualmente l'XML per il messaggio CAP da zero.
5. Nel campo **Conteggio istanza evento**, immettere il numero di messaggi richiesti o utilizzare le frecce per selezionare il numero di messaggi richiesti. È possibile inoltrare un singolo messaggio CAP o una sequenza automatica di messaggi.
6. Opzionale: Selezionare la casella di spunta **Rendi evento casuale**. Se si seleziona **Rendi evento casuale**, viene pubblicata una sequenza di messaggi CAP con gli ID casuali utilizzati. I messaggi vengono pubblicati ad intervalli di tempo incrementali e in ubicazioni casuali all'interno di un intervallo.
7. Fare clic su **Inoltra evento**.

## Risultati

Il Publisher di esempio completa il IBM Intelligent Operations Center con gli eventi e può attivare i KPI.

### Concetti correlati:

“Dettagli” a pagina 272

Utilizzare il portlet Dettagli per visualizzare, monitorare e gestire gli eventi in IBM Intelligent Operations Center.

## Creazione di eventi CAP o aggiornamento di eventi esistenti senza XML

Nella scheda **Modulo evento**, è possibile completare un modulo per creare nuovi eventi CAP o aggiornare eventi esistenti senza utilizzare XML.

## Informazioni su questa attività

È possibile utilizzare il modulo per creare un nuovo evento o un evento basato sui valori di un evento esistente. Quando si crea un evento basato su un evento esistente, utilizzare l'ID avviso CAP per fare riferimento all'evento esistente. Qualsiasi valore immesso nel modulo sovrascrive i valori ereditati dall'evento CAP esistente. Per ulteriori informazioni sulle proprietà di eventi, consultare il link alla fine dell'argomento per l'argomento del portlet Dettagli.

## Procedura

1. Nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di dimostrazione > Publisher eventi di esempio**.
2. Fare clic sulla scheda **Modulo evento**.
3. Per specificare un'origine per l'evento, accanto ad Origine fare clic su una delle seguenti opzioni:
  - Per creare un nuovo evento con i valori basati sui valori immessi nel modulo, fare clic su **Nuovo**.
  - Per creare un evento con i valori basati sull'evento esistente nella tabella degli eventi CAP ed utilizzando l'ID avviso CAP, fare clic su **Esistente**.
4. Nel campo **ID**, immettere un ID a seconda che si sta creando un nuovo evento o un evento basato su un ID avviso CAP esistente.
  - Se si sta creando un nuovo evento, facoltativamente immettere un valore per **ID**. Se non si immette un valore, viene generato un identificativo univoco.
  - Se si sta creando un evento basato su un valore ID avviso CAP esistente, immettere il valore ID avviso CAP per **ID**. Qualsiasi valore immesso nel modulo sovrascrive i valori ereditati dall'evento CAP esistente.
5. Se si sta creando un nuovo evento, nel campo **Tipo di evento**, immettere uno dei seguenti tipi di evento:

### **Avviso**

Un nuovo evento.

### **Aggiornamento**

Un aggiornamento ad un evento precedentemente creato

### **Cancellazione**

Una cancellazione di un evento precedentemente creato.

6. Nel campo **Titolo**, immettere un titolo.
7. Dall'elenco **Tipo di messaggio**, selezionare un tipo di messaggio.
8. Se si sta creando un nuovo evento, dall'elenco **Codice evento**, selezionare **Evento** o **Incidente**. Un incidente è più importante di un evento.
9. Dall'elenco **Categoria**, selezionare una categoria.
10. Dall'elenco **Urgenza**, selezionare l'urgenza.
11. Dall'elenco **Gravità**, selezionare la gravità.
12. Dall'elenco **Certezza**, selezionare la certezza
13. Nel campo **Descrizione**, immettere una descrizione.
14. Nel campo **Mittente**, immettere una descrizione del mittente dell'evento.
15. Nel campo **Conteggio istanza evento**, selezionare il numero di messaggi richiesti. È possibile inoltrare un singolo messaggio CAP o una sequenza automatica di messaggi.
16. Opzionale: Selezionare la casella di spunta **Rendi evento casuale**. Se si seleziona **Rendi evento casuale**, una sequenza di messaggi CAP viene pubblicata con gli ID casuali utilizzati. I messaggi vengono pubblicati ad intervalli di tempo incrementali e in ubicazioni casuali all'interno di un intervallo.
17. Fare clic su **Inoltra evento**.

### **Concetti correlati:**

“Dettagli” a pagina 272

Utilizzare il portlet Dettagli per visualizzare, monitorare e gestire gli eventi in IBM Intelligent Operations Center.

### **Notifiche di test**

Utilizzare la scheda **Notifica** per creare le notifiche di test per eseguire il test del sottosistema di notifiche nel IBM Intelligent Operations Center.

### **Informazioni su questa attività**

Nella scheda **Notifica**, completare il modulo per inoltrare un avviso per i gruppi specificati. Per un particolare utente, viene visualizzato un messaggio di notifica di avviso nel portlet Notifiche solo se l'utente è un membro di Inviato ai gruppi specificato nella notifica.

### **Procedura**

1. Nell'interfaccia di gestione WebSphere Portal fare clic su **Intelligent Operations > Strumenti di dimostrazione > Publisher eventi di esempio**.
2. Fare clic sulla scheda **Notifica**.
3. Per creare un avviso dall'elenco **Tipo**, selezionare **Avviso**.
4. Opzionale: Dall'elenco **Categoria**, selezionare una categoria.
5. Opzionale: Nel campo **Titolo**, immettere un titolo.
6. Opzionale: Nel campo **Descrizione**, immettere una descrizione.
7. Opzionale: Nel campo **Mittente**, immettere una descrizione del mittente dell'evento.
8. Opzionale: Nel campo **Inviato ai gruppi**, immettere un elenco dei gruppi separato da punto e virgola per inviare l'avviso, ad esempio ;CityWideOperator;CityWideExecutive;.

**Nota:** Oltre ad inserire un punto e virgola tra ogni nome di gruppo, accertarsi di inserire un punto e virgola all'inizio dell'elenco e alla fine dell'elenco.

Quando questa notifica di avviso è pubblicata, viene visualizzata nel portlet Notifiche solo per gli utenti che sono membri dei gruppi CityWideOperator e CityWideExecutive

9. Opzionale: Eseguire una delle seguenti operazioni come richiesto:
  - Nel campo **Riferimenti agli avvisi**, immettere un elenco di identificativi di eventi CAP separato da punto e virgola a cui fa riferimento il nuovo avviso.
  - Nel campo **Riferimenti agli indicatori KPI**, immettere un elenco di KPI separato da punto e virgola a cui fa riferimento il nuovo avviso.
10. Fare clic su **Inoltra notifica**.

#### **Concetti correlati:**

"Notifiche" a pagina 287

Utilizzare il portlet Notifiche per visualizzare i messaggi di avviso ed i relativi dettagli.

## **Programmazione script di eventi**

Utilizzare il portlet Programmazione script di eventi per scrivere uno script e creare un elenco sequenziale di eventi da pubblicare a intervalli di tempo predefiniti.

Per avviare il portlet Programmazione script di eventi, nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di dimostrazione > Programmazione script di eventi**.

Nel portlet Programmazione script di eventi, è possibile scrivere uno script che faccia riferimento ad eventi da pubblicare per ID evento che sono registrati in tabella eventi di esempio nel IBM Intelligent Operations Center. Nello script è possibile specificare un ritardo tra gli eventi da pubblicare. Quando si esegue lo script, il sistema pubblica gli eventi attraverso il backend. Tuttavia, il flusso di eventi è lo stesso per eventi che entrano nel sistema da fonti esterne.

È possibile inoltre cancellare gli eventi da IBM Intelligent Operations Center. Se si cancellano gli eventi da IBM Intelligent Operations Center, tutti gli eventi visualizzati nel portlet Mappa e Dettagli vengono eliminati.

Prima di utilizzare il portlet Programmazione script di eventi, è possibile visualizzare gli eventi di tabella eventi di esempio in IBM Intelligent Operations Center.

Nel portlet Programmazione script di eventi, seguire l'esempio riportato per creare uno script JSON che definisca un elenco sequenziale di eventi da pubblicare a intervalli di tempo predefiniti. Prima di eseguire lo script, è necessario ripulire e convalidare lo script facendo clic sul pulsante **Elimina e convalida**.

È possibile pubblicare una sola volta un evento con un ID particolare. È necessario eliminare tutti gli eventi da IBM Intelligent Operations Center prima di poter pubblicare di nuovo un evento con lo stesso ID. Tuttavia, se si seleziona la casella di spunta **Rendi casuale gli ID**, il portlet dello script eventi pubblica nuovamente gli stessi eventi e applica gli ID casuali agli eventi.

### **Visualizzazione di eventi di esempio ed eventi KPI nel tabella eventi di esempio**

Il portlet Programmazione script di eventi pubblica gli eventi di esempio dal tabella eventi di esempio nel IBM Intelligent Operations Center. Utilizzare la seguente procedura per visualizzare gli eventi nel tabella eventi di esempio.

#### **Procedura**

1. Utilizzare un client VNC per accedere al server di dati come utente root ed aprire una finestra comandi. Nelle seguenti operazioni, immettere i comandi nella finestra comandi che è stata appena aperta nel server di dati.
2. Per poter aprire DB2 Control Center, è necessario temporaneamente disattivare il controllo accessi; immettere il seguente comando: xhost +

3. In DB2 Control Center, visualizzare gli eventi di esempio che sono nella tabella eventi di esempio, ed ottenere i numeri di ID evento di esempio:
  - a. Per aprire DB2 Control Center, immettere i seguenti comandi:
 

```
su - db2inst1
db2cc
```
  - b. In DB2 Control Center, fare clic su **Tutti i database > IOCDB > Tabelle > REF\_SAMPLEEVENTS**.
  - c. Fare clic con il tasto destro del mouse sulla tabella **REF\_SAMPLEEVENTS** e quindi fare clic su **Apri**. Esistono 40 righe nella tabella eventi di esempio, ma una volta che gli eventi sono pubblicati, vengono visualizzati solo gli eventi da 1 a 8 nel portlet Dettagli. Gli altri eventi sono per i KPI di test. Se si seleziona la casella di spunta **Rendi casuali gli ID** nel portlet Programmazione script di eventi, è possibile pubblicare, gli stessi 8 eventi ripetutamente.
  - d. Considerare **SAMPLEID** per ogni evento di esempio a cui fare riferimento quando si creano gli script di evento nel portlet Programmazione script di eventi. Il valore di **SAMPLEID** corrisponde all'ID evento.
4. Una volta terminata la visualizzazione degli eventi di esempio, chiudere DB2 Control Center.
5. Per ritornare all'utente root, immettere il seguente comando: `exit`
6. Per attivare nuovamente il controllo accessi, immettere il seguente comando:-

#### Concetti correlati:

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

## Creazione di uno script di evento

Creare uno script di evento che pubblica una sequenza di eventi ad intervalli di tempo predefiniti.

### Prima di iniziare

Prima di utilizzare il portlet Programmazione script di eventi per pubblicare gli eventi, è possibile visualizzare gli eventi nella tabella eventi di esempio nel IBM Intelligent Operations Center.

### Informazioni su questa attività

Utilizzare le seguenti operazioni per creare uno script di evento nel portlet Programmazione script di eventi.

**Nota:** È possibile pubblicare un evento con un ID particolare una sola volta. Per poter pubblicare nuovamente un evento con lo stesso ID, fare clic su **Reimposta database** per eliminare tutti gli eventi dal IBM Intelligent Operations Center. Alternativamente, per pubblicare nuovamente gli stessi eventi con degli ID casuali applicati, selezionare la casella di spunta **Rendi casuali gli ID**.

### Procedura

1. Nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di dimostrazione > Programmazione script di eventi**.
2. Utilizzare l'esempio fornito nel portlet Programmazione script di eventi per creare uno script JSON che definisce un elenco sequenziale di eventi da pubblicare ad intervalli di tempo predefiniti, immettere lo script nel campo sul lato sinistro dell'esempio. Lo script JSON di esempio fornito nel portlet Programmazione script di eventi, è mostrato anche nel seguente codice:

```
[
  {
    "id": 2
    //ID of element in Sample Events table
    "delayAfter": 4000
```



```

    //Milliseconds to wait after publishing the event with the current ID
  },
  {}, //Empty objects are ignored
  {
    "id": 1
    //If the command specifies only an ID, the next command is processed
    //directly after the previous command
  },
  {
    "delayAfter": 0
    //If the command specifies only a delay, no event is published and the
    //script waits until the next command is due
  }
]

```

3. Opzionale: Per pubblicare nuovamente gli stessi eventi con ID casuali applicati, selezionare la casella di spunta **Rendi casuali gli ID**.
4. Richiesto: Per ripulire e convalidare lo script prima di eseguirlo, fare clic su **Elimina e Convalida**. La sintassi dello script è convalidata ed i commenti sono rimossi. Se nello script viene rilevata una markup non corretta che non può essere risolta, viene visualizzato un messaggio.
5. Per eseguire lo script, fare clic su **Esegui script dell'evento**.
6. Per eliminare tutti gli eventi dal IBM Intelligent Operations Center e per evitare che lo script pubblichi più eventi fare clic su **Reimposta database**.

#### Attività correlate:

“Visualizzazione di eventi di esempio ed eventi KPI nel tabella eventi di esempio” a pagina 107

Il portlet Programmazione script di eventi pubblica gli eventi di esempio dal tabella eventi di esempio nel IBM Intelligent Operations Center. Utilizzare la seguente procedura per visualizzare gli eventi nel tabella eventi di esempio.

---

## Creazione ed integrazione dei KPI

I modelli KPI (Key performance indicator) possono essere creati e modificati utilizzando un toolkit di sviluppo del monitoraggio di business e un portlet di gestione KPI.

Il Development Toolkit IBM WebSphere Business Monitor può essere installato con Rational Application Developer, entrambi sono forniti con IBM Intelligent Operations Center. Il Development Toolkit IBM WebSphere Business Monitor può anche essere installato con WebSphere Integration Developer.

Prima di definire o modificare un KPI è necessario comprendere l'avviso CAP CAP (Common Alerting Protocol) su cui si baserà il KPI. Ad esempio, se si definisce un KPI che tiene traccia del livello di una risorsa idrica, sarà necessario conoscere gli elementi CAP contenenti gli elementi di cui è necessario tenere traccia come ad esempio il nome della risorsa idrica e la profondità dell'acqua espressa in piedi. Una volta che un KPI è aggiunto o modificato in questo modo, è necessario distribuirlo al server IBM WebSphere Business Monitor.

Per ulteriori informazioni relative all'utilizzo di IBM WebSphere Business Monitor e del Development Toolkit IBM WebSphere Business Monitor, consultare il centro informazioni IBM WebSphere Business Monitor.

Una volta definiti i modelli KPI e le metriche tramite IBM WebSphere Business Monitor, è possibile utilizzare il portlet KPI (Key Performance Indicators) per sviluppare e modificare i KPI.

### Concetti correlati:

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

“Eventi e KPI” a pagina 91

IBM Intelligent Operations Center elabora gli eventi e i KPI (key performance indicators) per determinare come visualizzare le informazioni.

“Personalizzazione dei KPI” a pagina 167

In IBM Intelligent Operations Center è possibile personalizzare i modelli KPI (Key Performance Indicator) per adattarlo ai processi business.

### Riferimenti correlati:

“Strumenti di installazione forniti con la soluzione” a pagina 66

Toolkit e strumenti di sviluppo sono inclusi con il IBM Intelligent Operations Center. Questi sono utilizzati quando si personalizza il IBM Intelligent Operations Center.

### Informazioni correlate:

 Centro informazioni di IBM WebSphere Business Process Management versione 7.0

## Monitoraggio dei modelli e KPI

Un modello di monitoraggio definisce metriche e KPI (performance indicators) le relative dipendenze per gli eventi in ingresso; le condizioni che richiedono azioni di business e gli eventi in uscita che riportano le condizioni che potrebbero attivare le azioni di business.

Un modello di monitoraggio può contenere i seguenti modelli secondari:

- Modello dei dettagli di monitoraggio
- Modello KPI
- Modello dimensionale
- Modello visivo
- Modello evento

Il modello dei dettagli di monitoraggio contiene la maggior parte delle informazioni del modello di monitoraggio

I modelli di monitoraggio di esempio forniti dal IBM Intelligent Operations Center non utilizzano i modelli dimensionali e visivi.

Il modello dei dettagli di monitoraggio definisce uno o più contesti di monitoraggio. Un contesto di monitoraggio definisce le informazioni da raccogliere e monitorate da uno o più eventi in ingresso. Per le entità IBM Intelligent Operations Center monitorate sono avvisi CAP. Le informazioni raccolte da questi avvisi vengono utilizzate per calcolare un KPI.

Il modello KPI contiene uno o più contesti PKI. Questi definiscono i KPI e i relativi trigger ed eventi associati. I contesti KPI possono elaborare eventi in ingresso, valutare i trigger ricorrenti del tempo di attesa e gli eventi in uscita. Ad esempio, il contesto può verificare se un KPI è al di fuori dell'intervallo definito e inviare una notifica.

Il modello evento fa riferimento a tutte le definizioni di eventi in ingresso e in uscita utilizzate nel modello di monitoraggio. Si fa riferimento a schemi che descrivono la struttura di singole parti di eventi.



#### Concetti correlati:

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

#### Informazioni correlate:



Centro informazioni IBM Business Monitor

## Monitoraggio istanze di contesto

Un'istanza del contesto di monitoraggio sono le informazioni raccolte in uno specifico momento all'interno del contesto di monitoraggio.

Per IBM Intelligent Operations Center un'istanza del contesto di monitoraggio corrisponde ad un avviso CAP. Quando si riceve un avviso CAP, viene creata o riutilizzata un'istanza del contesto di monitoraggio e le metriche all'interno dell'istanza del contesto vengono popolate con i valori di avviso CAP basati sul contesto del monitoraggio.

Un contesto di monitoraggio può essere definito per creare una nuova istanza per ogni avviso CAP o per riutilizzare un'istanza esistente. Ad esempio, se si desidera un KPI per calcolare il livello medio settimanale di acqua per una determinata risorsa con il livello dell'acqua giornaliero campionato, si dovrebbe creare una nuova istanza del contesto di monitoraggio per ogni avviso CAP. Ogni istanza dovrebbe contenere il livello di acqua giornaliero e il KPI dovrebbe fare una media delle misurazioni per un periodo di sette giorni.

I KPI vengono calcolati utilizzando le metriche definite per un contesto di monitoraggio. Quando si definisce un KPI di aggregazione, specificare il contesto di monitoraggio e la metrica utilizzata come input per la funzione di aggregazione del KPI. Quando si valuta il KPI, vengono utilizzati i valori della metrica per le istanze del contesto di monitoraggio dalla funzione di aggregazione per calcolare il valore del KPI.

#### Concetti correlati:

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

#### Informazioni correlate:



centro informazione IBM Business Monitor

## Modellazione dei PKI

Modellare i KPI con Rational Application Developer or WebSphere Integration Developer, con il toolkit di sviluppo IBM WebSphere Business Monitor installato. Rational Application Developer e il toolkit di sviluppo IBM WebSphere Business Monitor sono inclusi come parte di IBM Intelligent Operations Center.

## Informazioni su questa attività

I KPI vengono modellati utilizzando Rational Application Developer o WebSphere Integration Developer con il toolkit di sviluppo IBM WebSphere Business Monitor. Per ulteriori informazioni relative all'utilizzo di questi strumenti, consultare i centri informazione di questi prodotti.

I modelli di monitoraggio sono contenuti all'interno dei progetti di monitoraggio del business. I modelli e progetti vengono creati utilizzando le procedure guidate di monitoraggio del business Rational Application Developer fornite dal toolkit di sviluppo IBM WebSphere Business Monitor.

Per modellare un KPI, fare quanto di seguito riportato.

## Procedura

1. Comprendere l'avviso CAP ricevuto da IBM Intelligent Operations Center.
2. Comprendere lo scopo del KPI. Il KPI genererà un'azione se è raggiunto o superato un limite? Sarà il KPI utilizzato per calcolare i dati statistici o cronologici?
3. Determinare il nome per il contesto di monitoraggio. La convenzione di denominazione IBM Intelligent Operations Center è utilizzare il tipo di evento CAP come nome. Gli esempi forniti da IBM Intelligent Operations Center creano un separato contesto di monitoraggio per ogni messaggio di avviso CAP inviato a IBM WebSphere Business Monitor.
4. In Rational Application Developer o WebSphere Integration Developer, con installato Toolkit di sviluppo IBM WebSphere Business Monitor, definire l'evento in ingresso, la chiave e l'insieme di metriche per il contesto di monitoraggio. L'evento in ingresso definisce il messaggio di avviso CAP monitorato dal contesto, una chiave che definisce univocamente l'istanza del contesto e le metriche che definiscono le informazioni estratte dal messaggio di avviso CAP.
5. Specificare lo schema CAP per l'evento. Lo schema deve esistere nel progetto di monitoraggio. Il IBM Intelligent Operations Center fornisce una copia dello schema CAP v1.2 nel progetto di modellazione `icoc_sample_monitor_models` di esempio.
6. Specificare il nome e l'ID per ciascun evento in ingresso di monitoraggio del business. Gli ID evento non possono contenere spazi o caratteri speciali. Per impostazione predefinita, l'ID viene creato dal nome con i caratteri di sottolineatura sostituiti dagli spazi. Tutti gli esempi forniti da IBM Intelligent Operations Center utilizzano gli ID dell'elemento predefinito.
7. Specificare lo schema. Lo schema definisce la struttura dell'evento in ingresso per IBM WebSphere Business Monitor.
8. Definire il filtro desiderato per i messaggi CAP. Ad esempio, limitare il monitoraggio a tipi di eventi specifici o in base alla gravità.
9. Specificare le metriche da estrarre dal messaggio CAP.
10. Definire una chiave di contesto per identificare univocamente l'istanza del contesto di monitoraggio. I valori della chiave vengono specificati dall'evento in ingresso quando viene creato il contesto di monitoraggio.
11. Specificare se gli eventi in ingresso devono essere correlati.
12. Specificare il contesto di KPI. Un contesto di KPI è un contenitore per i KPI ed i relativi trigger ed eventi associati. A differenza di un contesto di monitoraggio, un contesto di KPI non contiene chiavi o metriche. Un contesto di KPI deve essere creato come contenitore prima di creare i KPI.
13. Creare il KPI all'interno del contesto di KPI precedentemente definito.
14. Specificare il tipo di KPI: **Decimale** o **Durata**.
15. Definire gli intervalli KPI, i valori e gli indicatori di colore. La maggior parte di esempi KPI IBM Intelligent Operations Center definiscono tre intervalli e i colori associati.

Tabella 34. Definizioni dell'intervallo e colore del KPI di esempio.

Nome	Colore	RGB
Accettabile	verde	699037
Attenzione	giallo	FDBA1A
Richiede un'azione	rosso	C32E14

16. Definire in che modo viene calcolato il valore KPI. I valori KPI vengono determinati in uno dei due seguenti modi: Se il valore proviene da una metrica che utilizza la funzione di aggregazione, il KPI

viene indicato come un KPI aggregato. Se il valore viene calcolato sulla base di altri KPI o dalle funzioni XPath definite dall'utente, il KPI viene indicato come un KPI espressione.

Negli esempi IBM Intelligent Operations Center, i KPI di livello inferiore (i KPI senza alcun elemento secondario) vengono definiti come KPI aggregati. I KPI di livello superiore (i KPI con elementi secondari) vengono definiti come KPI espressione.

I valori del KPI aggregato vengono calcolati dalle metriche completate con i dati inviati nei messaggi di avviso CAP inviati al server e IBM WebSphere Business Monitor. Viene quindi eseguita una funzione di aggregazione su questi dati. La funzione di aggregazione include:

- media
- massimo
- minimo
- somma
- numero di ricorrenze
- deviazione standard

I valori sono espressi come misurazioni quantificabili. Ad esempio, tempo medio di risposta al crimine (5 minuti, 7 secondi) o livello medio dell'acqua (100.5).

I valori del KPI espressione vengono calcolati dagli intervalli e calcoli del KPI. Negli esempi IBM Intelligent Operations Center i KPI principali hanno calcoli in base ai quali la valutazione del KPI assume il valore 0, 1 o 2 a seconda dei valori dei relativi KPI secondari. Un valore 0 è associato ad un intervallo accettabile, il valore 1 ad un intervallo di attenzione e 2 ad un intervallo che richiede un'azione. Gli esempi utilizzano le espressioni di calcolo per impostare il valore KPI alla massima urgenza dei relativi elementi secondari.

17. Opzionale: Specificare il filtro temporale per un KPI aggregato. I KPI aggregati possono avere filtri temporali facoltativi che limitano il periodo di tempo durante il quale viene calcolato il valore del KPI. Il periodo di tempo può essere un intervallo di ripetizione (ad esempio l'ultimo trascorso o il periodo corrente), un intervallo dinamico o un intervallo fisso. Tutti i KPI aggregati IBM Intelligent Operations Center di esempio hanno dei filtri temporali definiti.
18. Opzionale: Specificare un filtro di dati per il KPI. Ad esempio, se il tempo medio di risposta al crimine deve essere calcolato per il Distretto di polizia Uno e non per altri distretti, è possibile utilizzare un filtro di dati per rimuovere tutti gli altri contesti di monitoraggio.
19. Definire in che modo i valori KPI vengono aggiornati incluso i trigger, gli eventi in ingresso per il server IBM WebSphere Business Monitor e gli eventi in uscita per IBM Intelligent Operations Center.
20. Eseguire il test del KPI. Il toolkit di sviluppo IBM WebSphere Business Monitor dispone di un ambiente di test per la verifica di KPI precedenti alla distribuzione; per i dettagli, vedere il link alla fine dell'argomento.
21. Distribuire l'applicazione del modello di monitoraggio.

### Concetti correlati:

“Definizione delle gerarchie KPI”

È possibile definire relazioni padre-figlio tra KPI e progettare come i KPI vengono visualizzati nel IBM Intelligent Operations Center. Progettare le proprie gerarchie KPI per poter ricercare i KPI in un modo adatto al proprio processo di business.

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

“Comunicazione evento KPI tra IBM WebSphere Business Monitor e IBM Intelligent Operations Center” a pagina 116

IBM WebSphere Business Monitor può inviare eventi in uscita da un contesto di monitoraggio o di KPI (key performance indicator) a IBM Intelligent Operations Center.

### Attività correlate:

“Distribuzione dei modelli di monitoraggio” a pagina 119

Una volta definiti i KPI (Key Performance Indicators) e i relativi modelli di monitoraggio, i modelli di monitoraggio devono essere distribuiti al IBM WebSphere Business Monitor in esecuzione sul IBM Intelligent Operations Center server delle applicazioni.

### Riferimenti correlati:

“Strumenti di installazione forniti con la soluzione” a pagina 66

Toolkit e strumenti di sviluppo sono inclusi con il IBM Intelligent Operations Center. Questi sono utilizzati quando si personalizza il IBM Intelligent Operations Center.

### Informazioni correlate:

 [Centro informazione Rational Application Developer](#)

 [Centro informazione IBM Business Monitor](#)

 [XPath \(XML Path Language\) 2.0 \(Seconda Edizione\)](#)

## Definizione delle gerarchie KPI

È possibile definire relazioni padre-figlio tra KPI e progettare come i KPI vengono visualizzati nel IBM Intelligent Operations Center. Progettare le proprie gerarchie KPI per poter ricercare i KPI in un modo adatto al proprio processo di business.

Mentre IBM WebSphere Business Monitor consente un KPI basato sul valore di un altro KPI, non consente la definizione di una relazione padre-figlio tra KPI. Per semplificare questa attività, il IBM Intelligent Operations Center fornisce un portlet KPI (Key Performance Indicators) per l'amministratore. Per le informazioni relative a questo portlet, consultare il link alla fine di questo argomento.

I KPI di esempio IBM Intelligent Operations Center definiscono una serie di KPI del distretto di polizia con un disegno gerarchico come quello di seguito riportato:

```
Police Department ----- level 1
  Crime Response Time ----- level 2
    Crime Response Time Precinct One ----- level 3
    Crime Response Time Precinct Two ----- level 3
```

In questo caso Distretto di polizia ha un elemento secondario: Tempo di risposta al crimine. Tempo di risposta al crimine ha due elementi secondari: Tempo di risposta al crimine Distretto uno e Tempo di risposta al crimine Distretto due.

I KPI dei due livelli 3 vengono definiti nel modello KPI come KPI aggregati. Ossia i loro valori vengono calcolati utilizzando un valore di metrica e una funzione di aggregazione. Tutti gli altri KPI in questa serie sono KPI espressione con i loro valori calcolati dai valori di altri KPI. Ad esempio:

- Tempo di risposta al crimine è basato sui valori di Tempo di risposta al crimine Distretto uno e Tempo di risposta al crimine Distretto due.
- Distretto di polizia è basato sul valore di Tempo di risposta al crimine.

Il IBM Intelligent Operations Center supporta un'alternativa all'utilizzo del portlet KPI (Key Performance Indicators) per definire le relazioni tra KPI. Il portlet KPI (Key Performance Indicators) è il metodo predefinito con il parametro **UseDBModelReader** impostato su true nel tabella proprietà di sistema. Per le informazioni relative all'impostazione nel tabella proprietà di sistema, fare clic sul link alla fine di questo argomento. Per informazioni relative al metodo alternativo per definire le relazioni tra KPI, fare clic sul link alla fine di questo argomento.

#### Concetti correlati:

"KPI (Key Performance Indicators)" a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

"Specifica dei dati di configurazione del sistema" a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

"Definizione di gerarchie KPI con OWL"

Il IBM Intelligent Operations Center supporta l'utilizzo di OWL (Web Ontology Language), come un'alternativa all'utilizzo del portlet KPI (Key Performance Indicators) per definire le relazioni padre-figlio tra KPI.

## Definizione di gerarchie KPI con OWL

Il IBM Intelligent Operations Center supporta l'utilizzo di OWL (Web Ontology Language), come un'alternativa all'utilizzo del portlet KPI (Key Performance Indicators) per definire le relazioni padre-figlio tra KPI.

Le relazioni padre-figlio tra KPI possono essere definite in OWL che viene letto ed elaborato dal IBM Intelligent Operations Center. Le definizioni vengono memorizzate in un file RDF (Resource Description Framework)

È possibile specificare se o meno il modello di database KPI deve essere letto da un file RDF. Per ulteriori informazioni relative al modo in cui modificare questa proprietà in tabella proprietà di sistema, consultare il link alla fine di questo argomento.

Un esempio delle definizioni OWL per la serie di KPI di esempio Distretto di polizia è riportato di seguito:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
    rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
```

```
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

**Nota:** OWL è un linguaggio costruito su RDF. OWL e RDF sono simili, ma OWL è un linguaggio più potente. OWL fornisce rispetto a RDF un vocabolario più ampio, sintassi più potente e maggiore capacità di interpretazione della macchina.

#### **Concetti correlati:**

“Definizione delle gerarchie KPI” a pagina 114

È possibile definire relazioni padre-figlio tra KPI e progettare come i KPI vengono visualizzati nel IBM Intelligent Operations Center. Progettare le proprie gerarchie KPI per poter ricercare i KPI in un modo adatto al proprio processo di business.

“KPI (Key Performance Indicators)” a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

“Specifica dei dati di configurazione del sistema” a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

## **Comunicazione evento KPI tra IBM WebSphere Business Monitor e IBM Intelligent Operations Center**

IBM WebSphere Business Monitor può inviare eventi in uscita da un contesto di monitoraggio o di KPI (key performance indicator) a IBM Intelligent Operations Center.

Gli eventi in uscita dal server IBM WebSphere Business Monitor vengono posizionati nella coda messaggi esterna. Il IBM Intelligent Operations Center utilizza questo meccanismo per ricevere in modo asincrono gli aggiornamenti KPI.

**Nota:** È possibile specificare se la connessione a IBM WebSphere Business Monitor deve utilizzare o meno SSL per una connessione protetta. Per ulteriori informazioni relative al modo in cui modificare questa proprietà nella tabella delle proprietà di sistema, consultare il link alla fine di questo argomento.

#### **Concetti correlati:**

“Specifica dei dati di configurazione del sistema” a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

“Utilizzo della coda eventi in entrata definita per il IBM Intelligent Operations Center” a pagina 100

Gli eventi CAP possono essere pubblicati nel IBM Intelligent Operations Center indirizzandoli nell'istanza inclusa WebSphere Message Broker.

## **Trigger**

Un trigger è un meccanismo che rileva una ricorrenza e può determinare un'ulteriore elaborazione nella risposta a tale ricorrenza.

Gli esempi KPI forniti con il IBM Intelligent Operations Center definiscono due tipi di trigger. Il primo trigger viene attivato quando si riceve un messaggio di avviso CAP, anche conosciuto come evento in ingresso, dal server IBM WebSphere Business Monitor per una determinata serie di KPI. Il messaggio di avviso CAP potrebbe o non potrebbe modificare il KPI. Il IBM Intelligent Operations Center determina se il KPI viene modificato quando riceve la notifica dell'evento dal server IBM WebSphere Business Monitor.

Per gli eventi in uscita, un trigger determina quando verrà inviato l'evento.



I trigger basati sull'evento possono essere utilizzati per inviare le notifiche al IBM Intelligent Operations Center quando viene modificato l'input per un calcolo KPI. Tuttavia, i trigger di eventi non possono essere utilizzati per indirizzare la situazione quando il valore KPI viene modificato quando scade dopo un definito periodo di tempo. Negli esempi IBM Intelligent Operations Center, i trigger basati sul tempo vengono utilizzati per inviare le notifiche al IBM Intelligent Operations Center per quei KPI con definizioni a breve termine.

Ad esempio, KPI per incidente stradale grave è definito per scadere ogni ora. Se il KPI ha un valore di 3 meno dieci e non si riceve nessun messaggio di avviso CAP per tale KPI entro la prossima ora, allora il tempo scade e il valore KPI viene reimpostato a zero.

### **Definizione degli eventi in entrata in IBM WebSphere Business Monitor**

In IBM Intelligent Operations Center vengono utilizzati gli eventi in entrata di esempio per determinare quando è attivato un trigger. Gli eventi in entrata per un contesto KPI vengono definiti in modo simile a quelli di un contesto di monitoraggio.

### **Informazioni su questa attività**

Gli eventi vengono definiti utilizzando Rational Application Developer o WebSphere Integration Developer con il Toolkit di sviluppo IBM WebSphere Business Monitor. Per ulteriori informazioni relative all'utilizzo di questi strumenti, consultare i centri informazione per questi prodotti.

Per definire un evento in entrata, eseguire le seguenti operazioni.

### **Procedura**

1. Selezionare il contesto KPI per l'evento in entrata.
2. Creare l'evento in entrata e specificare il nome evento e l'ID.
3. Specificare lo schema CAP.
4. Specificare la condizione di filtro.
5. Selezionare il contesto KPI e creare un nuovo evento in entrata.
6. Creare un nuovo trigger per l'evento in entrata.
7. Accertarsi che il trigger sia ripetitivo così che il trigger venga attivato ogni volta che l'origine del trigger è aggiornata e la condizione di trigger soddisfatta.
8. Selezionare l'origine del trigger.
9. Definire la condizione del trigger. Quando è soddisfatta la condizione del trigger, il trigger viene attivato.

### **Esempio**

Vengono definiti i modelli di monitoraggio IBM Intelligent Operations Center di esempio in modo che venga attivato un trigger ogni volta che si riceve un messaggio di avviso CAP dal server IBM WebSphere Business Monitor.

### Attività correlate:

“Modellazione dei PKI” a pagina 111

Modellare i KPI con Rational Application Developer or WebSphere Integration Developer, con il toolkit di sviluppo IBM WebSphere Business Monitor installato. Rational Application Developer e il toolkit di sviluppo IBM WebSphere Business Monitor sono inclusi come parte di IBM Intelligent Operations Center.

### Informazioni correlate:

 Centro informazioni IBM Business Monitor

 Centro informazioni Rational Application Developer

## Definizione degli eventi in uscita per il IBM Intelligent Operations Center

Gli eventi in uscita definiscono le informazioni inviate da IBM WebSphere Business Monitor al IBM Intelligent Operations Center quando viene attivato un trigger.

### Informazioni su questa attività

Il IBM Intelligent Operations Center utilizza le notifiche in uscita inviate dal server IBM WebSphere Business Monitor per determinare se il KPI è stato modificato. Se il KPI viene modificato, il IBM Intelligent Operations Center ottiene i dati KPI dal server IBM WebSphere Business Monitor, aggiorna le informazioni della cache KPI ed aggiorna i dati IBM Intelligent Operations Center.

Gli eventi in uscita vengono definiti utilizzando Rational Application Developer o WebSphere Integration Developer con Toolkit di sviluppo IBM WebSphere Business Monitor. Per ulteriori informazioni relative all'utilizzo di questi strumenti, consultare i centri informazione per questi prodotti.

Per definire un evento in uscita, eseguire le seguenti operazioni.

### Procedura

1. Selezionare il contesto KPI per l'evento in uscita.
2. Creare l'evento in uscita e specificare il nome evento e l'ID.
3. Specificare lo schema di notifica. Lo schema si trova nel file `ioc-notification-v1.0.xsd`. Lo schema si trova nel progetto `icoc_sample_monitor-models`.
4. Definire il contenuto dell'evento in uscita. Il contenuto è basato sullo schema di notifica.
5. In **notifica**, per il valore di **sentfrom** immettere Monitor.
6. Aggiungere gli elementi del parametro al contenuto dell'evento come definito nelle seguenti operazioni.
  - a. Per il primo parametro, specificare `modelID` per **parameterName** e l'ID del modello di monitoraggio per **parameterValue**. Ad esempio, `icoc_sample_public_safety_monitor_model`.
  - b. Per ogni KPI nella serie di KPI aggiungere i parametri per specificare l'ID KPI e il valore KPI. L'ID KPI viene specificato utilizzando l'elemento **parameterName** e il valore KPI è specificato utilizzando l'elemento `parameterValue`. L'ID KPI deve essere associato ad un KPI nella serie di KPI. Utilizzare la funzione `xs:string()` per specificare il valore KPI come una stringa. Ad esempio, **parameterName** può essere `Police_Department` e **parameterValue** può essere `xs:string(Police_Department)`.

### Esempio

Di seguito è riportato un esempio di notifica da inviare al IBM Intelligent Operations Center:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
```



```

<ns1:kpiLink> Police Department</ns1:kpiLink>
<ns1:category> Safety</ns1:category>
<ns1:parameter>
  <ns1:parameterName> modelId</ns1:parameterName>
  <ns1:parameterValue>
    icoc_sample_public_safety_monitor_model</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Police_Department</ns1:parameterName>
  <ns1:parameterValue> 0</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
  <ns1:parameterValue> 0</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
  <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
  <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
</ns1:parameter>
</ns1:notification>

```

#### Attività correlate:

“Modellazione dei PKI” a pagina 111

Modellare i KPI con Rational Application Developer or WebSphere Integration Developer, con il toolkit di sviluppo IBM WebSphere Business Monitor installato. Rational Application Developer e il toolkit di sviluppo IBM WebSphere Business Monitor sono inclusi come parte di IBM Intelligent Operations Center.

#### Informazioni correlate:



Centro informazioni IBM Business Monitor



Centro informazioni Rational Application Developer

## Distribuzione dei modelli di monitoraggio

Una volta definiti i KPI (Key Performance Indicators) e i relativi modelli di monitoraggio, i modelli di monitoraggio devono essere distribuiti al IBM WebSphere Business Monitor in esecuzione sul IBM Intelligent Operations Center server delle applicazioni.

### Informazioni su questa attività

Per distribuire un modello di monitoraggio che verrà utilizzato IBM WebSphere Business Monitor, è necessario generare progetti JEE (Java Enterprise Edition) dai modelli definiti. Una volta che i progetti JEE sono generati, l'applicazione del modello può essere esportata come un file EAR. Il file EAR può quindi essere distribuito nel IBM WebSphere Business Monitor in esecuzione sul IBM Intelligent Operations Center server delle applicazioni.

### Procedura

1. In Rational Application Developer o WebSphere Integration Developer con Toolkit di sviluppo IBM WebSphere Business Monitor installato, fare clic con il tasto destro del mouse sul modello di monitoraggio che richiede la generazione del progetto nella scheda **Enterprise Explorer**. Ad esempio, `icoc_sample_public_safety_monitor_model`.
2. Fare clic su **Genera progetti JEE di monitoraggio**. Verranno creati i seguenti progetti: `modelApplication`, `modelLogic`, e `modelModerator`.
3. Esportare l'applicazione del modello di monitoraggio facendo clic con il tasto destro del mouse sul progetto `modelApplication` e selezionando **Esporta > EAR**.
4. Verificare i KPI prima di distribuire il file EAR in IBM WebSphere Business Monitor.

5. Distribuire il file EAR sul server IBM WebSphere Business Monitor utilizzando le istruzioni nel centro informazioni IBM WebSphere Business Monitor.

**Informazioni correlate:**

 Centro informazioni IBM Business Monitor

 Centro informazioni Rational Application Developer

## Valori di visualizzazione KPI

Il raggruppamento di risorsa IBM Intelligent Operations Center può essere utilizzato per fornire valori di visualizzazione alternativi rispetto a quelli forniti dai modelli. IBM WebSphere Business Monitor.

I nomi di visualizzazione KPI e i nomi intervallo vengono definiti nei modelli IBM WebSphere Business Monitor di esempio forniti con IBM Intelligent Operations Center. Esempi di nomi di visualizzazione KPI sono:

- Acqua
- Qualità dell'acqua

Esempi di nomi intervallo sono:

- valore di stato accettabile
- valore di stato di attenzione
- valore di stato esegui azione

Ogni risorsa, ad esempio, KPI ed intervallo, definita in IBM WebSphere Business Monitor ha un ID associato al nome di visualizzazione. Gli ID non possono contenere spazi mentre i valori di visualizzazione possono contenerli. Gli ID vengono utilizzati come chiavi per ricercare valori in un raggruppamento di risorse. Il IBM Intelligent Operations Center utilizza questi ID per selezionare i valori di visualizzazione KPI. Se non viene specificato alcun valore nel raggruppamento di risorse per l'ID, viene utilizzato il valore specificato nella definizione IBM WebSphere Business Monitor.

I valori di visualizzazione KPI vengono localizzati da IBM WebSphere Business Monitor utilizzando il linguaggio ISO e i codici paese del server IBM WebSphere Business Monitor. Ad esempio, un valore percentuale dovrebbe essere visualizzato nel formato 12.61% quando la locale è en\_US e 12,61% quando la locale è fr\_FR. Le definizioni del raggruppamento di risorse non vengono utilizzate per questi valori.

Il raggruppamento di risorse delle proprietà IBM Intelligent Operations Center predefinito è `com.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. Il raggruppamento può essere trovato in `icoc_rest_monitor_resources_utils`.

Questo è un raggruppamento di risorse di esempio:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

In questo esempio, i valori di `kpi.NO.VALUE` e `kpi.RANGE.UNDETERMINED` sono utilizzati dal IBM Intelligent Operations Center quando i KPI IBM WebSphere Business Monitor restituiscono un valore null. Ad esempio, il KPI Livello acqua lago cittadino è definito con un periodo di tempo ricorrente giornaliero basato sull'ultimo periodo completo. Se per la domenica non si riceve nessun evento CAP per tale KPI e il KPI è richiesto il lunedì, viene restituito il valore null poiché nessun dato è disponibile per il giorno precedente. Il valore di visualizzazione è impostato su "Nessun dato per determinare il valore KPI" e il nome di visualizzazione dell'intervallo è impostato su "indeterminato".

Le altre voci `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River`, e `Water_Level_City_Lake`, definiscono i valori di visualizzazione per gli ID KPI definiti nel modello di monitoraggio di esempio `icoc sample water monitor model` fornito dal IBM Intelligent Operations Center. Queste voci possono specificare un testo alternativo dai valori specificati nel monitoraggio IBM WebSphere Business Monitor. Ad esempio, il raggruppamento di risorse può essere utilizzato per fornire i valori convertiti invece di modificare il modello stesso.

#### Concetti correlati:

“KPI di esempio”

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

## Memorizzazione nella cache dei KPI

Le impostazioni di configurazione IBM Intelligent Operations Center interessano quando i valori KPI vengono richiamati dal IBM WebSphere Business Monitor.

Il IBM Intelligent Operations Center conserva i valori KPI nella cache. Per impostazione predefinita, i KPI sono caricati da IBM WebSphere Business Monitor nella cache e la cache viene aggiornata in base all'intervallo di tempo specificato dalla proprietà `KpiCacheRefreshInterval` nella tabella delle proprietà di sistema. Il tempo di aggiornamento può essere modificato a seconda dei requisiti di consegna dei KPI aggiornati al IBM Intelligent Operations Center. Per ulteriori informazioni relative alla modifica delle proprietà nella tabella proprietà di sistema, consultare il link alla fine di questo argomento.

Considerare che quando si crea un KPI nel portlet KPI (Key Performance Indicators), gli aggiornamenti al KPI dipendono esclusivamente dall'aggiornamento della cache. Quando un KPI è definito in IBM WebSphere Business Monitor, può essere definito un meccanismo di trigger per implementare ulteriori elaborazioni in risposta alle modifiche in tale KPI.

#### Concetti correlati:

“Specifica dei dati di configurazione del sistema” a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

---

## KPI di esempio

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

I KPI di livello più basso sono definiti come KPI aggregati. I KPI aggregati vengono calcolati dai valori contenuti nei messaggi di avviso CAP in entrata ed una funzione di aggregazione, come media, massimo, minimo, somma, numero di ricorrenze o deviazione standard. I loro valori vengono espressi come misurazioni quantificabili. I valori KPI di livello inferiore vengono localizzati nel formato appropriato in base alla locale del server IBM WebSphere Business Monitor. I KPI di livello superiore vengono associati ai valori in base all'associazione definita durante la creazione del KPI di esempio.

Il valore del KPI di esempio di livello superiore è un numero che si identifica con il colore e il livello della risposta consigliata. Il valore 0 è Accettabile, il valore 1 è Attenzione e il valore 2 è Esegui azione. Il valore del KPI di livello più basso è una durata, un valore decimale, una percentuale o una valuta, a seconda del KPI che rappresenta. Ad esempio:

- 15% è il valore effettivo di un KPI che rappresenta la percentuale dei voli in ritardo in un particolare aeroporto in un periodo di tempo.

- 5 minuti, 7 secondi è il valore effettivo di un KPI che rappresenta il tempo di risposta medio al crimine per una determinata ubicazione in un periodo di tempo.

I file di origine per i modelli di monitoraggio IBM Intelligent Operations Center di esempio vengono forniti in un file di archivio che può essere importato in Rational Application Developer or WebSphere Integration Developer con IBM WebSphere Business Monitor Toolkit installato. Il file di archivio può essere modificato per cambiare, aggiungere o eliminare definizioni KPI. Le definizioni possono quindi essere generate e distribuite nuovamente in IBM Intelligent Operations Center.

I modelli di esempio forniti con IBM Intelligent Operations Center sono:

- icoc\_sample\_public\_safety\_monitor\_model
- icoc\_sample\_transportation\_monitor\_model
- icoc\_sample\_water\_monitor\_model

Questi modelli contengono i seguenti esempi di KPI:

- Acqua
  - Controllo delle piene
    - Livelli dell'acqua
      - Flusso di scarico del fiume cittadino
      - Livello acqua lago cittadino
  - Gestione acque
    - Pianificazione strategica
      - Perdite di acqua
      - Fornitura acqua rispetto alla domanda
  - Qualità dell'acqua
    - Indicatori fisici
      - Torbidezza
      - pH
- Trasporto
  - Aeroporti
    - Voli in ritardo
      - Voli in ritardo aeroporto uno
      - Voli in ritardo aeroporto due
  - Strade e traffico
    - Eventi stradali
      - Incidenti stradali gravi
  - Gestione trasporti
    - Entrate
      - Pedaggio ponti e tunnel
      - Ricavi parcheggi
- Sicurezza pubblica
  - Vigili del fuoco
    - Ferite dei vigili del fuoco
      - Ferite vigili del fuoco stazione vigili uno
      - Ferite vigili del fuoco stazione vigili due
  - Dipartimento di polizia
    - Tempo di risposta al crimine

- Tempo di risposta al crimine Distretto uno
- Tempo di risposta al crimine Distretto due
- Gestione della sicurezza pubblica
  - Budget per la sicurezza pubblica
    - Budget pronto soccorso
    - Budget vigili del fuoco
    - Budget distretto di polizia

#### **Concetti correlati:**

“Stato” a pagina 291

Utilizzare il portlet Stato per visualizzare lo stato degli indicatori KPI (key Performance Indicator) per una singola organizzazione o per più organizzazioni.

“Drill Down KPI (Key Performance Indicator)” a pagina 275

Utilizzare il portlet Drill Down KPI (Key Performance Indicator) per visualizzare ulteriori informazioni su una categoria KPI, lo stato dei KPI sottostanti.

“Creazione ed integrazione dei KPI” a pagina 109

I modelli KPI (Key performance indicator) possono essere creati e modificati utilizzando un toolkit di sviluppo del monitoraggio di business e un portlet di gestione KPI.

“Personalizzazione dei KPI” a pagina 167

In IBM Intelligent Operations Center è possibile personalizzare i modelli KPI (Key Performance Indicator) per adattarlo ai processi business.

#### **Attività correlate:**

“Distribuzione dei modelli di monitoraggio” a pagina 119

Una volta definiti i KPI (Key Performance Indicators) e i relativi modelli di monitoraggio, i modelli di monitoraggio devono essere distribuiti al IBM WebSphere Business Monitor in esecuzione sul IBM Intelligent Operations Center server delle applicazioni.

“Visualizzazione di eventi di esempio ed eventi KPI nel tabella eventi di esempio” a pagina 107

Il portlet Programmazione script di eventi pubblica gli eventi di esempio dal tabella eventi di esempio nel IBM Intelligent Operations Center. Utilizzare la seguente procedura per visualizzare gli eventi nel tabella eventi di esempio.

---

## **Configurazione di Tivoli Service Request Manager**

Nell'interfaccia utente Tivoli Service Request Manager, è possibile gestire procedure operative standard, flussi di lavoro e le risorse.

Se si aggiunge un prefisso comune ai nomi di procedure operative standard, flussi di lavoro e delle risorse, è più facile filtrare i dati in una ricerca. Ad esempio, per i progetti del cliente, utilizzare il prefisso comune CX.

È possibile specificare se la connessione a Tivoli Service Request Manager utilizza SSL impostando la proprietà **TSRMServerSecurityEnabled**. Per ulteriori informazioni relative a questa proprietà ed ad altre proprietà Tivoli Service Request Manager, andare al link alla fine dell'argomento.

## Concetti correlati:

“Server eventi” a pagina 208

“Specifica dei dati di configurazione del sistema” a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

## Utilizzo dell'interfaccia utente Tivoli Service Request Manager.

Informazioni per accedere all'interfaccia utente Tivoli Service Request Manager. Semplificare e rendere più veloce Tivoli Service Request Manager Start Center per utilizzarlo mediante la personalizzazione con i link alle funzioni che più si utilizzano.

### Apertura delle applicazioni Tivoli Service Request Manager

È possibile aprire le applicazioni Tivoli Service Request Manager attraverso l'interfaccia di gestione WebSphere Portal attraverso gli strumenti di gestione soluzioni oppure attraverso il portlet SOP (Standard Operating Procedure). È possibile anche visualizzare una risorsa in Tivoli Service Request Manager tramite l'interfaccia IBM Intelligent Operations Center.

### Prima di iniziare

Per essere in grado di visualizzare una risorsa in Tivoli Service Request Manager tramite IBM Intelligent Operations Center l'interfaccia, è necessario configurare sign-on singoli.

### Procedura

- Per aprire Tivoli Service Request Manager Start Center tramite l'interfaccia di gestione WebSphere Portal, utilizzare le seguenti operazioni secondarie:
  1. Fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**.
  2. Fare clic su **Amministrazione della procedura operativa standard**.
  3. Accedere a Tivoli Service Request Manager Start Center come amministratore.
- Per aprire le applicazioni Tivoli Service Request Manager relative a procedure operative standard, utilizzare il portlet SOP (Standard Operating Procedure):
  1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.
  2. Selezionare una delle opzioni riportate di seguito:
    - Per aprire l'applicazione SOP(Standard Operating Procedure), fare clic su **SOP (Standard Operating Procedure)**.
    - Per aprire l'applicazione della matrice di selezione SOP (Standard Operating Procedure), fare clic su **Matrice di selezione SOP (Standard Operating Procedure)**.
    - Per aprire l'applicazione designer flusso di lavoro, fare clic su **Designer flusso di lavoro**.
- Per visualizzare una risorsa nell'interfaccia utente Tivoli Service Request Manager tramite l'interfaccia IBM Intelligent Operations Center, eseguire le seguenti operazioni:
  1. Nel portlet Dettagli, nella scheda **Eventi e incidenti**, fare clic con il tasto destro del mouse sulla riga nell'elenco eventi.
  2. Per visualizzare un elenco delle risorse in prossimità di un evento fare clic su **Visualizza risorse vicine** e selezionare il raggio dell'area interessata. Viene visualizzato un elenco di risorse nella scheda **Risorse**.
  3. Nella scheda **Risorse**, fare clic con il tasto destro del mouse sulla riga nell'elenco risorse e quindi fare clic su **Proprietà**. La risorsa viene visualizzata nella scheda Tivoli Service Request Manager **Risorse**.

**Nota:** Per uscire completamente da Tivoli Service Request Manager, è necessario chiudere la finestra del browser web dell'interfaccia utente Tivoli Service Request Manager.

### Attività correlate:

“Configurazione di SSO (Single Sign-On) per i servizi di collaborazione” a pagina 54  
Importare il token LTPA SSO di WebSphere Portal in server eventi per consentire agli utenti di accedere ai servizi di collaborazione senza dover immettere nuovamente le credenziali.

## Impostazione delle applicazioni preferite in Tivoli Service Request Manager Start Center

Aggiornare le applicazioni preferite in Tivoli Service Request Manager Start Center in modo che sia possibile accedervi più facilmente.

### Informazioni su questa attività

Ogni utente Tivoli Service Request Manager dispone di propri Tivoli Service Request Manager Start Center con un proprio elenco personalizzato in Applicazioni preferite.

### Procedura

1. Per visualizzare Tivoli Service Request Manager Start Center, nella parte superiore dell'interfaccia utente Tivoli Service Request Manager fare clic su **Centro di avvio**.
2. In Tivoli Service Request Manager Start Center, fare clic sull'icona **Modifica portlet** accanto alle Applicazioni preferite.
3. Nella finestra Impostazione applicazioni preferite, fare clic su **Seleziona applicazioni**.
4. Nella finestra Seleziona applicazioni, selezionare le applicazioni che si desidera visualizzare sotto Applicazioni preferite. Il seguente elenco mostra le applicazioni utili per gli utenti IBM Intelligent Operations Center:

#### CRONTASK

Impostazione attività cron

#### DOMAINADM

Domini

#### PERSON

Persone

#### PERSONGR

Gruppi di persone

#### PLUSIMTRIX

Matrice di selezione SOP

#### PLUSIRES

Risorse

#### PLUSIWO

Attività SOP

#### USER

Utenti

#### WFDESIGN

Designer flusso di lavoro

5. Per definire la posizione in cui le applicazioni vengono elencate sotto Applicazioni preferite, eseguire le seguenti operazioni:
  - a. Nella finestra Impostazione applicazioni preferite, selezionare un'applicazione.
  - b. Nel campo **Ordine** immettere un numero.
6. Per salvare gli aggiornamenti fare clic su **Fine**.



## Configurazione di nuovi utenti in Tivoli Service Request Manager

Quando si aggiunge un utente in IBM Intelligent Operations Center, assegnare le autorizzazioni e i gruppi di persone per l'utente in Tivoli Service Request Manager.

### Impostazione del Sede di inserimento predefinita

Perché un nuovo utente sia in grado di aggiungere nuove risorse e utilizzare procedure operative standard, è necessario impostare Sede di inserimento predefinita per l'utente.

#### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Sicurezza > Utenti**.
3. Per ricercare l'utente, nella scheda **Elenco**, nel campo **Utente**, immettere alcune o tutte le lettere nel nome dell'utente.
4. Nell'elenco fare clic sul nome dell'utente e quindi fare clic sulla scheda **Utente**.
5. In Impostazioni utente, accanto al campo **Sede di inserimento predefinita** fare clic sull'icona **Seleziona valore**.
6. Nella finestra Seleziona valore, ricercare e fare clic sul nome del Sede di inserimento predefinita; ad esempio, **PMSCRTP**. PMSCRTP è una sede di esempio che viene installata con IBM Intelligent Operations Center.
7. Fare clic sull'icona **Salva utente**.

### Assegnazione di un utente ad un gruppo di sicurezza

Aggiungere gli utenti agli appropriati gruppi di sicurezza in modo che hanno accesso alle appropriate applicazioni in Tivoli Service Request Manager.

#### Informazioni su questa attività

Per aggiungere un utente ad un gruppo, utilizzare la seguente procedura.

#### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Sicurezza > Utenti**.
3. Per ricercare l'utente, nella scheda **Elenco**, nel campo **Utente** immettere alcune o tutte le lettere nel nome dell'utente.
4. Nell'elenco, fare clic sul nome dell'utente e quindi fare clic sulla scheda **Gruppi**.
5. Per ricercare il gruppo a cui si desidera aggiungere l'utente, nel campo **Gruppo** immettere alcune o tutte le lettere nel nome del gruppo.
6. Se il nome del gruppo richiesto non è presente nell'elenco, fare clic su **Nuova riga**.
7. In Dettagli, accanto al campo **Gruppo**, fare clic sull'icona **Menu dettagli** e quindi fare clic su **Seleziona valore**.
8. Nella finestra Seleziona valore, ricercare e fare clic sul nome del gruppo richiesto.
9. Fare clic sull'icona **Salva utente**.

### Assegnazione di un utente a gruppo di persone

In un procedura operativa standard, le attività possono essere assegnate ad un predefinito gruppi di persone. Un utente deve essere un membro di un particolare gruppo di persone in modo da visualizzare le attività assegnate a tale gruppo di persone.



## Prima di iniziare

È possibile utilizzare l'esempio gruppi di persone fornito durante l'installazione di IBM Intelligent Operations Center o crearne uno proprio gruppi di persone. Per le informazioni relative al modo in cui creare un gruppo di persone in Tivoli Service Request Manager, consultare il centro informazioni Maximo Asset Management.

**Nota:** Accertarsi che i nomi di tutti i gruppi di persone siano di uguale lunghezza. Ciò assicura che agli utenti vengono assegnate solo le attività assegnate al gruppo di persone di cui essi sono membri.

## Informazioni su questa attività

Per assegnare un utente ad un gruppo di persone, utilizzare la seguente procedura.

### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **vai a > Amministrazione > Risorse > Gruppi di persone**.
3. Per ricercare il gruppo di persone richiesto, nella scheda **Elenco**, nel campo **Gruppi di persone**, immettere alcune o tutte le lettere nel nome del gruppo di persone.
4. Nell'elenco, fare clic sul nome del gruppo di persone.
5. Nella scheda **Gruppo di persone**, in **Persone**, fare clic su **Nuova riga**.
6. In **Dettagli**, accanto al campo **Persone**, fare clic sull'icona **Menu dettagli** e quindi fare clic su **Seleziona valore**.
7. Nella finestra **Seleziona valore**, ricercare e fare clic sul nome che si desidera aggiungere al gruppo di persone.
8. Nel campo **Sequenza**, immettere il prossimo numero incrementale disponibile.
9. Fare clic sull'icona **Salva gruppo di persone**.

### Informazioni correlate:



Centro informazioni di Maximo Asset Management

## SOP (Standard Operating Procedure)

È possibile definire procedure operative standard e le attività per la gestione degli eventi inseriti in IBM Intelligent Operations Center. Utilizzare il portlet SOP (Standard Operating Procedure) per accedere alle applicazioni procedura operativa standard, matrice di selezione procedura operativa standard e designer flusso di lavoro in Tivoli Service Request Manager.

Per avviare il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.

Una procedura operativa standard definisce una sequenza di attività attivate in risposta ad un evento i cui parametri soddisfano determinate condizioni predefinite, in cui ciascuna attività corrisponde a un'attività manuale o automatizzata. È possibile assegnare un flusso di lavoro a un'attività automatizzata. Ciascuna attività viene assegnata a un gruppo proprietario, mentre gli utenti vengono assegnati a un gruppo proprietario mediante la loro appartenenza a un gruppo di persone. Tutti gli utenti assegnati al gruppo proprietario possono gestire le attività attraverso il portlet **Attività personali**.

È possibile specificare l'ordine in cui alcune o tutte le attività in una procedura operativa standard vengono eseguite. Ad esempio, è possibile specificare di non avviare una particolare attività fino a quando non è stata completata o ignorata la precedente attività.

Per aprire l'applicazione procedura operativa standard, nel portlet SOP (Standard Operating Procedure) fare clic su **SOP (Standard Operating Procedure)**.

## Matrice di selezione procedura operativa Standard

In matrice di selezione procedura operativa standard, si definiscono i parametri di eventi che determinano se una procedura operativa standard viene avviata per un particolare evento. Ogni procedura operativa standard può avere uno o più serie di criteri di selezione. Tuttavia, ciascuna serie di criteri di selezione deve essere univoca.

Per aprire l'applicazione matrice di selezione procedura operativa standard, nel portlet SOP (Standard Operating Procedure) fare clic su **Matrice di selezione SOP (Standard Operating Procedure)**.

## Designer flusso di lavoro

Utilizzare designer flusso di lavoro per designare flussi di lavoro che possono essere assegnati alle attività procedura operativa standard come attività automatizzate.

Per aprire l'applicazione designer flusso di lavoro, fare clic su **Workflow Designer** nel portlet SOP (Standard Operating Procedure).

## Personalizzazione del portlet SOP (Standard Operating Procedure)

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

### Concetti correlati:

“Attività personali” a pagina 284

Il portlet Attività personali visualizza un elenco dinamico di attività di proprietà del gruppo di cui l'utente collegato all'interfaccia è membro.

### Riferimenti correlati:

“Impostazioni portlet SOP (Standard Operating Procedure)” a pagina 164

Personalizzare il portlet SOP (Standard Operating Procedure) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Creazione di flussi di lavoro

In Tivoli Service Request Manager, è possibile creare flussi di lavoro che è possibile includere come attività automatizzate nelle attività procedura operativa standard.

## Informazioni su questa attività

Per le informazioni dettagliate relative al modo in cui creare i flussi di lavoro, visualizzare il link al centro informazioni Maximo Asset Management alla fine della sezione.

## Procedura

1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.
2. Per aprire l'applicazione designer flusso di lavoro, fare clic su **Designer flusso di lavoro**.
3. Nella finestra Designer flusso di lavoro, fare clic sulla scheda **Canvas**.
4. Nella scheda **Canvas**, fare clic sulle appropriate icone per inserire i nodi e le frecce richiesti per flusso di lavoro.

## Informazioni correlate:

 Centro informazioni di Maximo Asset Management

## Creazione di procedure operative standard

Creare una procedura operativa standard ed assegnarla ad un gruppo proprietario. Gli utenti vengono assegnati ad un gruppo proprietario mediante la relativa appartenenza ad un gruppo di persone.

### Procedura

1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione di WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.
2. Per aprire l'applicazione procedura operativa standard, fare clic su **SOP (Standard Operating Procedure)**.
3. Nella finestra SOP (Standard Operating Procedure), nella scheda **Elenco**, fare clic sull'icona **Nuova SOP**. Nella scheda **SOP (Standard Operating Procedure)** viene visualizzata una procedura operativa standard vuota.
4. Immettere un nome nel campo **Nome SOP** ed immettere una descrizione nel campo visualizzato accanto a **Nome SOP**. Per i nomi di procedure operative standard, utilizzare un formato coerente simile ai nomi dell'esempio procedure operative standard; ad esempio, Preparazione per l'evacuazione per gravi condizioni del tempo (Prepara). Inoltre, se l'ultimo carattere del nome è una parentesi di chiusura, aggiungere il carattere LRM (left-to-right mark) per evitare possibili problemi relativi alla visualizzazione del testo bidirezionale. Ad esempio, immettere il nome utilizzato nell'esempio precedente come Preparazione per l'evacuazione per gravi condizioni del tempo (Prepara)&#x200E;. Il carattere LRM non viene visualizzato nell'interfaccia utente dopo il salvataggio della procedura operativa standard. Inoltre, se si aggiunge un prefisso comune ai nomi di tutte le procedure operative standard, è più semplice filtrare le procedure operative standard in una ricerca. Ad esempio, per i progetti del cliente, utilizzare il prefisso comune CX.
5. Per immettere una descrizione più lunga, fare clic sull'icona accanto al campo della descrizione ed immettere una descrizione nella finestra visualizzata.
6. In **Dettagli**, dall'elenco **Tipo di template**, selezionare **Attività**.
7. In **Dettagli**, assegnare un gruppo proprietario alla procedura operativa standard:
  - a. Fare clic sull'icona accanto al campo **Gruppo proprietario**.
  - b. Nella finestra **Seleziona valore**, fare clic su un valore nell'elenco per selezionarlo.
8. Opzionale: Per **Durata**, immettere un limite di tempo entro il quale la procedura operativa standard deve essere completata. Il formato per il limite di tempo è *hh:mm*, dove *hh* è il numero di ore e *mm* è il numero di minuti. La data di fine viene calcolata in base alla durata.
9. Aggiungere attività alla procedura operativa standard, come richiesto:
  - a. Nella parte inferiore destra dell'interfaccia utente di Tivoli Service Request Manager, fare clic su **Nuova riga**. Nelle procedure SOP, viene aggiunta una nuova riga di attività all'elenco di sequenze dell'attività.
  - b. In **Sequenza** ed in **Attività**, immettere lo stesso numero. Assegnare i numeri alle attività in base al seguente modello: 10, 20, 30 e così via. Utilizzando tale modello, si dispone di una maggiore flessibilità per l'aggiunta e la rimozione delle attività.
  - c. In **Istruzione**, immettere una descrizione dell'attività. Per effettuare una selezione dalle descrizioni immesse precedentemente, fare clic sull'icona accanto al campo della descrizione.
  - d. Opzionale: Assegnare un flusso di lavoro:
    - 1) Per **Nome del flusso di lavoro**, fare clic sull'icona **Seleziona valore**.
    - 2) Nella finestra **Seleziona valore**, fare clic su un valore nell'elenco per selezionarlo. Per ridurre l'elenco, nel campo relativo al filtro visualizzato nella parte superiore dell'elenco, immettere le prime lettere del nome di un flusso di lavoro che si desidera utilizzare.

- 3) Espandere la riga dell'attività e, in Dettagli, immettere ulteriori dettagli, come richiesto. Se si desidera, è possibile specificare un gruppo proprietario e le impostazioni di controllo del flusso. Se per l'attività non vengono specificati un gruppo proprietario e le impostazioni di controllo del flusso, l'attività eredita le impostazioni dalla procedura operativa standard principale.
10. Per salvare la procedura operativa standard, nella parte superiore dell'interfaccia utente di Tivoli Service Request Manager, fare clic sull'icona **Salva SOP**.
11. Per applicare la procedura operativa standard agli eventi specificati nella matrice di selezione procedura operativa standard, verificare di modificare lo stato da DRAFT ad ACTIVE:
  - a. Fare clic sull'icona **Modifica stato**.
  - b. Nella finestra Modifica stato, dall'elenco **Nuovo stato**, selezionare **Attivo**.
  - c. Opzionale: Immettere i valori per **A partire da** e **Memo**.
  - d. Fare clic su **OK**.
12. Per esaminare le procedure operative standard disponibili, effettuare le operazioni riportate di seguito:
  - a. Fare clic sulla scheda **Elenco**.
  - b. Nei piani di lavoro SOP, selezionare una delle seguenti opzioni:
    - Nel campo relativo al filtro, premere Invio per visualizzare tutte le procedure operative standard disponibili.
    - Nel campo relativo al filtro, immettere le prime lettere del nome di una procedura operativa standard.
  - c. Per visualizzare i dettagli per una procedura operativa standard, fare clic sul nome della procedura operativa standard nell'elenco. I dettagli vengono visualizzati nella scheda **SOP (Standard Operating Procedure)**.

## Operazioni successive

Se si desidera specificare l'ordine in cui vengono eseguite alcune o tutte le attività in una procedura operativa standard, in Dettagli, selezionare la casella di spunta **Flusso controllato?**. Per ulteriori informazioni relative al modo in cui ordinare le attività assegnate ad utenti o gruppi in base alle procedure operative standard, consultare il centro informazioni di Maximo Asset Management e ricercare *controllo del flusso*.

Nella matrice di selezione procedura operativa standard, definire i parametri degli eventi che determinano gli eventi per cui viene selezionata la procedura operativa standard.

### Attività correlate:

“Assegnazione di un utente a gruppo di persone” a pagina 126

In un procedura operativa standard, le attività possono essere assegnate ad un predefinito gruppi di persone. Un utente deve essere un membro di un particolare gruppo di persone in modo da visualizzare le attività assegnate a tale gruppo di persone.

### Informazioni correlate:



Centro informazioni di Maximo Asset Management

## Revisione delle voci nella matrice di selezione procedura operativa standard

Nella matrice di selezione procedura operativa standard, esaminare i criteri di selezione per ciascuna procedura operativa standard. I criteri di selezione sono basati sui parametri degli eventi.

## Procedura

1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione di WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.

2. Per aprire l'applicazione Matrice di selezione SOP (Standard Operating Procedure), fare clic su **Matrice di selezione SOP (Standard Operating Procedures)**.
3. Nella finestra Matrice di selezione SOP (Standard Operating Procedure), per visualizzare la riga del filtro, fare clic sull'icona **Filtro**.
4. Determinare il campo del filtro da utilizzare:
  - Categoria
  - Gravità
  - Urgenza
  - Certezza
  - Nome SOP
5. Selezionare una delle opzioni riportate di seguito:
  - Nel campo relativo al filtro, premere Invio per visualizzare tutte le voci esistenti relative al nome della procedura operativa standard o al parametro scelto.
  - Nel campo relativo al filtro, immettere le prime lettere di un valore su cui eseguire il filtro.
  - Se si sta eseguendo il filtro su un valore del parametro, immettere i valori mediante la finestra Seleziona valore:
    - a. Accanto al campo del filtro, fare clic sull'icona **Seleziona valore**.
    - b. Nella finestra Seleziona valore, fare clic su un valore nell'elenco per selezionarlo.
  - Per selezionare il nome di una procedura operativa standard su cui eseguire il filtro mediante la finestra SOP (Standard Operating Procedure):
    - a. Accanto al campo del filtro **NOME SOP**, fare clic sull'icona **Menu Dettagli**, quindi fare clic su **Passa a SOP (Standard Operating Procedure)**.
    - b. Nella finestra SOP (Standard Operating Procedure), fare clic sulla scheda **Elenco**.
    - c. Nei piani di lavoro SOP, nel campo relativo al filtro, immettere le prime lettere del nome di una procedura operativa standard.
    - d. Per visualizzare i dettagli per una procedura operativa standard, fare clic sul nome della procedura operativa standard nell'elenco. I dettagli vengono visualizzati nella scheda **SOP (Standard Operating Procedure)**.
    - e. Per restituire il nome della procedura operativa standard visualizzato nella scheda **SOP (Standard Operating Procedure)**, nell'angolo in alto a destra, fare clic su **Ripristina con valore**. Il nome viene visualizzato nel campo del filtro **Nome SOP** nella matrice di selezione.
6. Per affinare ulteriormente l'elenco delle voci dei criteri di selezione visualizzati, ripetere il Passo 5 utilizzando uno degli altri campi relativi al filtro elencati nel Passo 4.

### **Definizione dei parametri nella matrice di selezione procedura operativa standard**

Nella matrice di selezione procedura operativa standard, definire i parametri degli eventi che determinano se una procedura operativa standard è selezionata per un particolare evento.

### **Informazioni su questa attività**

Non è possibile salvare una matrice di selezione procedura operativa standard che contiene due righe di criteri di selezione identiche. Se appropriato, viene visualizzato un messaggio di convalida che indica che è necessario definire un insieme univoco di criteri di selezione per una procedura operativa standard.

### **Procedura**

1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione di WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.
2. Per aprire l'applicazione Matrice di selezione SOP (Standard Operating Procedure), fare clic su **Matrice di selezione SOP (Standard Operating Procedures)**.

3. Nella finestra Matrice di selezione SOP (Standard Operating Procedure), per visualizzare la riga del filtro, fare clic sull'icona **Filtro**.
4. Nella finestra **Matrice di selezione SOP**, nell'angolo in basso a destra, fare clic su **Nuova riga**. Una nuova riga viene aggiunta alla matrice di selezione.
5. Immettere i valori per ciascuno dei seguenti parametri:
  - Categoria
  - Gravità
  - Urgenza
  - Certezza

Utilizzare una delle seguenti opzioni per immettere i valori per ciascuno dei parametri:

- Per immettere i valori mediante la finestra Seleziona valore:
    - a. Accanto al campo relativo al parametro, fare clic sull'icona **Seleziona valore**.
    - b. Nella finestra Seleziona valore, fare clic su un valore nell'elenco per selezionarlo.
  - Per immettere manualmente il nome del parametro:
    - a. Immettere le prime lettere del valore del parametro nel campo.
    - b. Premere il tasto di tabulazione per spostare il cursore nel campo successivo; il valore del parametro viene completato automaticamente.
6. Per immettere il nome della procedura operativa standard nel campo **Nome SOP**, selezionare una delle seguenti opzioni:
    - Per immettere il nome della procedura operativa standard mediante la finestra SOP (Standard Operating Procedure):
      - a. Accanto al campo **NOME SOP**, fare clic sull'icona **Menu Dettagli**, quindi fare clic su **Passa a SOP (Standard Operating Procedure)**.
      - b. Nella finestra SOP (Standard Operating Procedure), fare clic sulla scheda **Elenco**.
      - c. Nei piani di lavoro SOP, nel campo relativo al filtro, immettere le prime lettere del nome di una procedura operativa standard.
      - d. Per visualizzare i dettagli per una procedura operativa standard, fare clic sul nome della procedura operativa standard nell'elenco. I dettagli vengono visualizzati nella scheda **SOP (Standard Operating Procedure)**.
      - e. Per restituire il nome della procedura operativa standard visualizzato nella scheda **SOP (Standard Operating Procedure)**, nell'angolo in alto a destra, fare clic su **Ripristina con valore**. Il nome è visualizzato nel campo **Nome SOP** della nuova riga nella matrice di selezione.
    - Immettere manualmente il nome della procedura operativa standard.
  7. Fare clic sull'icona **Salva matrice**.

## Gestione risorse

Gestire le risorse in Tivoli Service Request Manager.

### Sincronizzazione delle risorse di esempio al database IBM Intelligent Operations Center

Se si desidera utilizzare le risorse di esempio installate con IBM Intelligent Operations Center, è necessario sincronizzarle manualmente con il database IBM Intelligent Operations Center.

#### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Asset > Risorse IOC (IntOpCtr)**.
3. Per visualizzare tutte le risorse di esempio IBM Intelligent Operations Center, nella finestra Risorse (IntOpCtr) nella scheda **Elenco**, fare clic sul campo **Risorsa** e premere Invio.



4. Per ogni risorsa che si desidera sincronizzare al database IBM Intelligent Operations Center, aggiornare la risorsa. Ad esempio, modificare **Descrizione** e salvare la modifica.
5. Verificare che le risorse sincronizzate vengano elencate nelle seguenti tabelle del database IBM Intelligent Operations Center:
  - IOC.RESOURCE
  - IOC.RESOURCE\_X\_CAPABILITY

## Operazioni successive

Se le risorse di esempio non sono correttamente sincronizzate al database IBM Intelligent Operations Center, esaminare il file di log del probe Tivoli Netcool/Impact. Immettere il seguente comando:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Esaminare anche il file di log della politica Tivoli Netcool/Impact `/opt/IBM/netcool/impact/log/NCI_policylogger.log`. Per abilitare il file di log della politica Tivoli Netcool/Impact eseguire le seguenti operazioni:

1. Accedere alla console di gestione Tivoli Netcool/Impact all'indirizzo `http://event_server:9080/nci`. Accedere come utente `admin` con la password `netcool`.
2. Fare clic su **Progetto IOC**.
3. Nella scheda **Servizi**, fare clic su **Programma di registrazione politica**.
4. Per **Più alto livello di log**, modificare il valore da 0 a 3.
5. Salvare le modifiche.
6. Eseguire il test.

Per ulteriori informazioni relative alla risoluzione dei problemi dei file di log consultare il link alla fine dell'argomento.

### Concetti correlati:

“File di log del Server eventi” a pagina 296

Utilizzare le seguenti procedure per abilitare le tracce e visualizzare i log per alcuni dei sistemi sul server eventi.

## Creazione o modifica della categoria di evento per l'associazione alla funzionalità

Le risorse vengono visualizzate nel portlet Mappa a seconda della categoria dell'evento selezionato e alle funzionalità della risorsa associata. Prima di creare una risorsa, associare la funzionalità della risorsa all'appropriata categoria di evento.

### Prima di iniziare

Per garantire che le funzionalità della risorsa siano aggiornate, è necessario impostare il valore della password per l'utente amministrativo Tivoli Service Request Manager ad esempio, `maxadmin`, per `maxadmin`.

### Informazioni su questa attività

L'associazione di una funzionalità della risorsa alla categoria di evento garantisce che quando si visualizzano risorse vicine nel portlet IBM Intelligent Operations Center Dettagli, le risorse opportune vengono visualizzate nel portlet Mappa. Ad esempio, se si visualizzano risorse vicine per una categoria di evento meteorologico, viene visualizzato un warehouse che memorizza i sacchetti di sabbia laddove il warehouse rappresenta il tipo di risorsa e i sacchetti di sabbia sono una funzionalità associata del warehouse.

### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Configurazione di sistema > Configurazione piattaforma > Domini**.



3. Scegliere l'opzione opportuna:
  - Per creare una categoria di evento per l'associazione alla funzionalità, fare clic su **Nuova riga** e immettere i dettagli appropriati nei campi.
  - Per modificare una categoria di evento esistente per l'associazione alla funzionalità, utilizzare il campo Filtro per visualizzare le associazioni appropriate alla categoria di evento, quindi fare clic sulla riga che si desidera modificare e modificare i dettagli.
  - Per eliminare una categoria di evento esistente per l'associazione alla funzionalità, utilizzare il campo Filtro per visualizzare le appropriate associazioni alla categoria di evento, quindi fare clic sull'icona **Contrassegna riga da eliminare** alla fine della riga che si desidera eliminare.
4. Fare clic sull'icona **Salva dominio**.
5. Verificare che le risorse associate siano elencate nelle seguenti tabelle di database IBM Intelligent Operations Center:
  - IOC.RESOURCE
  - IOC.RESOURCE\_X\_CAPABILITY

## Risultati

Le nuove risorse la cui funzionalità è associata alla categoria di evento dell'evento attualmente selezionato vengono immediatamente visualizzate nel portlet IBM Intelligent Operations Center Mappa. Le risorse aggiornate la cui funzionalità è associata alla categoria di evento dell'evento attualmente selezionato vengono visualizzate solo dopo che la pagina contenente il portlet IBM Intelligent Operations CenterMappa viene ricaricata.

## Operazioni successive

- Se le risorse associate non sono attualmente elencate nel database IBM Intelligent Operations Center, esaminare il file di log Tivoli Netcool/Impact. Immettere il seguente comando:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Per ulteriori informazioni relative alla risoluzione dei problemi dei file di log, consultare il link alla fine di questo argomento.

- Se si desidera associare più di due categorie di evento ad una funzionalità, utilizzare un comando DB2 per eseguire l'associazione. Utilizzare le seguenti operazioni:

1. Accedere a server di dati come un utente di database Tivoli Service Request Manager, immettere il seguente comando: `su - db2inst6`

2. Per connettersi al database IBM Intelligent Operations Center, immettere il seguente comando: `db2 connect to maximo`

3. Per associare una categoria di evento ad una funzionalità, immettere il seguente comando:

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'category_name', 'capability_name',
'mapping_description', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|mapping_key');
```

Nel precedente comando sostituire le variabili *nome\_categoria*, *nome\_funzionalità*, *descrizioneAssociazione* e *chiaveAssociazione* con i valori appropriati. Per *mapping\_key*, creare un valore appropriato. Ad esempio, il seguente comando associa la categoria di evento Met alla funzionalitàCOT, ed assegna il valore METCOT a *mapping\_key*.

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|METCOT');
```

4. Per completare la scrittura nel database, immettere il seguente comando: `db2 commit;`

## Creazione di una risorsa

Creare una risorsa nell'interfaccia utente Tivoli Service Request Manager.

### Prima di iniziare

Accertarsi che la funzionalità della nuova risorsa sia associata ad una categoria in modo che la risorsa venga visualizzata nel portlet Mappa nell'interfaccia utente IBM Intelligent Operations Center.

### Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Asset > Risorse (IntOpCtr)**.
3. Nella finestra Risorse IOC fare clic sull'icona **Nuova risorsa**.
4. Nella scheda **Risorsa** immettere i seguenti dettagli:

#### Risorsa

Un ID univoco per la risorsa.

#### Descrizione completa

Il nome della risorsa visualizzata nell'interfaccia utente IBM Intelligent Operations Center nel portlet Dettagli nella scheda **Risorse**.

#### Descrizione breve

Una breve descrizione della risorsa viene visualizzata come guida al passaggio del mouse se avviene il passaggio del mouse sulla risorsa nel portlet Mappa nell'interfaccia utente IBM Intelligent Operations Center.

#### Latitudine

La posizione di latitudine dell'ubicazione della risorsa.

#### Longitudine

La posizione longitudinale dell'ubicazione della risorsa.

5. Fare clic sulla scheda **Funzionalità**.
6. Accanto al campo **Classificazione**, fare clic sull'icona **Menu dettagli** e quindi fare clic su **Classifica**.
7. Nella finestra Classifica esplorare la struttura ad albero di navigazione per individuare l'appropriata classificazione della risorsa.
8. Fare clic sul nome classificazione, ad esempio warehouse. Una tabella delle funzionalità associate alla classificazione viene visualizzata nella finestra Risorse IOC.
9. Nella tabella Funzionalità, fare clic sulle funzionalità appropriate ed immettere il **Valore numerico**.
10. Fare clic sull'icona **Salva risorsa**.

### Operazioni successive

Verificare che la risorsa viene elencata nelle tabelle del database IBM Intelligent Operations Center:

- IOC.RESOURCE
- IOC.RESOURCE\_X\_CAPABILITY

#### Attività correlate:

“Creazione o modifica della categoria di evento per l'associazione alla funzionalità” a pagina 133

Le risorse vengono visualizzate nel portlet Mappa a seconda della categoria dell'evento selezionato e alle funzionalità della risorsa associata. Prima di creare una risorsa, associare la funzionalità della risorsa all'appropriata categoria di evento.

### Visualizzazione, aggiornamento o eliminazione di una risorsa

Accedere all'interfaccia utente Tivoli Service Request Manager tramite l'interfaccia utente IBM Intelligent Operations Center e visualizzare, aggiornare o eliminare le risorse.

## Informazioni su questa attività

La procedura di seguito riportata descrive il modo in cui accedere ai dati risorse in Tivoli Service Request Manager tramite l'interfaccia utente IBM Intelligent Operations Center. Per accedere ai dati risorse direttamente tramite Tivoli Service Request Manager, eseguire le seguenti operazioni:

1. Accedere a Tivoli Service Request Manager Start Center.
2. Fare clic su **Vai a > Asset > Risorse (IntOpCtr)**.
3. Per elencare tutte le risorse IBM Intelligent Operations Center, nella finestra Risorse (IntOpCtr), nella scheda **Elenco**, fare clic sul campo **Risorsa** e premere il tasto Invio.
4. Nell'elenco, fare clic sulla riga della risorsa che si desidera modificare.
5. Fare clic sulla scheda **Risorsa** o sulla scheda **Funzionalità** come appropriato.

## Procedura

1. Aprire l'interfaccia utente IBM Intelligent Operations Center.
2. Nel portlet Dettagli, nella scheda **Eventi e incidenti**, identificare un evento nell'elenco le cui risorse si desidera visualizzare, aggiornare o eliminare.
3. Per visualizzare un elenco delle risorse in prossimità di un evento, fare clic con il tasto destro del mouse sull'evento e quindi fare clic su **Visualizza risorse vicine** e selezionare il raggio dell'area su cui si desidera concentrarsi. Viene visualizzato un elenco di risorse nella scheda **Risorse**.
4. Nella scheda **Risorse**, fare clic con il tasto destro del mouse su una riga nell'elenco risorse e selezionare un'opzione dal menu:
  - Per aggiornare le informazioni relative ad una risorsa, fare clic su **Aggiorna**.
  - Per rimuovere una risorsa dall'elenco e dalla mappa, fare clic su **Elimina**.
  - Per visualizzare le informazioni relative a una risorsa, fare clic su **Proprietà**.

Qualsiasi opzione si scelga la risorsa viene visualizzata in Tivoli Service Request Manager, nella scheda **Risorsa**.

5. Nella scheda Tivoli Service Request Manager, **Risorsa**, è possibile scegliere di eseguire le seguenti azioni sulla risorsa:
  - Aggiornare il nome risorsa, le descrizioni, la latitudine e longitudine.
  - Per eliminare la risorsa, selezionare **Elimina risorsa** dall'elenco **Seleziona azione**.
6. Nella scheda **Funzionalità**, è possibile scegliere di eseguire le seguenti azioni sulle funzionalità della risorsa.
  - Fare clic sulle funzionalità appropriate e modificare **Valore numerico**. Per una funzionalità da associare alla risorsa, il valore deve essere 1 o più.
  - Selezionare una funzionalità e quindi fare clic sull'icona **Contrassegna riga da eliminare** alla fine della riga.
7. Una volta terminato l'aggiornamento della risorsa, fare clic sull'icona **Salva risorsa**.

## Operazioni successive

Per poter visualizzare i dati della risorsa aggiornata nell'interfaccia utente IBM Intelligent Operations Center, reimpostare il Mappa. Quindi, esaminare le risorse per un evento tramite il portlet Dettagli.

## Creazione del tipo di risorsa

Creare un tipo di risorsa in Tivoli Service Request Manager.

## Informazioni su questa attività

È possibile definire una gerarchia di tipi di risorsa pertanto i tipi di risorsa possono avere tipi di risorse secondari e così via.

## Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Amministrazione > Classificazioni**.
3. Per visualizzare tutti i tipi di risorse IBM Intelligent Operations Center esistenti, nella scheda **Elenco**, nel campo **Descrizione**, immettere RESOURCE. Vengono visualizzati tutti i tipi di risorse nella gerarchia.
4. Fare clic sul tipo di risorsa o sul tipo di risorsa secondario per cui si desidera creare un tipo di risorsa secondario. I dettagli della classificazione per il tipo di risorsa principale del nuovo tipo di risorsa vengono visualizzati nella scheda **Classificazioni**.
5. Nella scheda **Classificazioni**, in Elementi secondari fare clic su **Nuova riga**.
6. Nella riga vuota che viene aggiunta all'elenco, immettere i seguenti valori per il nuovo tipo di risorsa:
  - a. Nella colonna **Classificazione**, immettere un nome.
  - b. Nella colonna Descrizione classificazione, immettere una descrizione.
  - c. Per evitare che il nome del tipo di risorsa sia modificato quando si salva il tipo di risorsa, deselezionare la casella di spunta **Genera descrizione**.
7. Fare clic sull'icona **Salva classificazione**.
8. Per aggiungere un'icona grafica per il nuovo tipo di risorsa, eseguire le seguenti operazioni secondarie.
  - a. Salvare le copie del grafico in due dimensioni in formato PNG. L'icona grafica più grande viene visualizzata nel portlet Mappa e l'icona grafica più piccola viene visualizzata nell'elenco eventi nel portlet Dettagli.

### Dimensione 24 pixel x 24 pixel

Ad esempio *new\_resource\_24.png*

### Dimensione 16 pixel x 16 pixel

Ad esempio *new\_resource\_16.png*

- b. Copiare ogni file PNG nell'appropriata directory nel server delle applicazioni:
  - /opt/IBM/WebSphere/wp\_profile/installedApps/ICPWPSNode/iss\_portal\_ear.ear/iss\_common\_widgets\_web.war/images/resource\_icons/PNG-24x24/Normal\_State
  - /opt/IBM/WebSphere/wp\_profile/installedApps/ICPWPSNode/iss\_portal\_ear.ear/iss\_common\_widgets\_web.war/images/resource\_icons/PNG-16x16/Normal\_State
- c. Verificare che ogni icona viene visualizzata correttamente nell'appropriato link del browser web.
  - [http://appserver/ibm/iss/common/widgets/images/resource\\_icons/PNG-24x24/Normal\\_State/new\\_resource\\_24.png](http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png)
  - [http://appserver/ibm/iss/common/widgets/images/resource\\_icons/PNG-16x16/Normal\\_State/new\\_resource\\_16.png](http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png)

## Aggiunta di una funzionalità ad un tipo di risorsa

Creare una funzionalità in Tivoli Service Request Manager.

## Procedura

1. Accedere a Tivoli Service Request Manager Start Center come amministratore.
2. Fare clic su **Vai a > Amministrazione > Classificazioni**.
3. Per visualizzare tutte le classificazioni della risorsa IBM Intelligent Operations Center esistenti, nella scheda **elenco** applicare il filtro per RESOURCE.
4. Fare clic nella scheda **Classificazioni**.
5. In Elementi secondari, nell'elenco, fare clic sul tipo di risorsa per cui si desidera aggiungere una funzionalità
6. Per impedire che il nome della risorsa viene modificato quando si salva la classificazione, annullare la casella di spunta **Genera descrizione**.
7. In Attributi, fare clic su **Nuova riga**.

8. Immettere i dettagli per la nuova funzionalità:
  - a. Per **Attributo**, immettere un nome.
  - b. Nel campo a destra del campo **Attributo**, immettere una descrizione.
  - c. Per immettere un valore per **Tipo di dati**, fare clic sull'icona Seleziona valore e scegliere un valore nella finestra Seleziona valore.
  - d. Per specificare che le risorse elementi secondari ereditano questa funzionalità, selezionare **Applica gerarchia sotto?**.
9. Fare clic sull'icona **Salva classificazione**.

## Esempi e risorse procedure operative standard, flussi di lavoro

Esempi e risorse procedure operative standard, flussi di lavoro sono forniti quando si installa IBM Intelligent Operations Center Versione 1.5.

### Procedure operative Standard

Sono forniti i tre seguenti procedure operative standard:

#### **PLUSIMITIG: Preparazione iniziale per maltempo grave (Riduzione)**

PLUSIMITIG include le seguenti operazioni:

1. Convalida della gravità del maltempo. Operazione manuale non associata a flussi di lavoro.
2. Se necessario, incrementare il tasso di gravità. Operazione manuale non associata a flussi di lavoro.

#### **PLUSIPREPA: Preparazione per l'evacuazione in caso di maltempo grave (Preparazione)**

PLUSIPREPA include le seguenti operazioni:

1. Preparazione dei rifugi per l'evacuazione. Operazione manuale associata a flusso di lavoro PLUSISOP00.
2. Individuazione delle risorse di supporto all'evacuazione. Operazione manuale associata a flusso di lavoro PLUSISOP00.
3. Valutazione della disponibilità delle risorse di supporto. Operazione manuale associata a flusso di lavoro PLUSISOP00.

#### **PLUSIRESPO: Aree interessate all'evacuazione (Rispondere e recuperare)**

PLUSIRESPO include le seguenti operazioni:

1. Approvazione delle direttive di evacuazione. Operazione manuale non associata a flussi di lavoro.
2. Accertarsi che i percorsi di uscita siano chiari. Operazione manuale non associata a flussi di lavoro.

Il matrice di selezione procedura operativa standard viene completato con i dati che attivano la selezione delle tre procedure operative standard, come mostrato nella seguente tabella:

*Tabella 35. Matrice di selezione procedura operativa Standard dati di esempio*

Categoria	Gravità	Urgenza	Certezza	Nome Procedura operativa Standard
Met	Grave	Futura	Osservata	PLUSIMITIG
Met	Grave	Futura	Probabile	PLUSIMITIG
Met	Estrema	Futura	Osservata	PLUSIPREPA
Met	Estrema	Futura	Probabile	PLUSIPREPA
Met	Estrema	Immediata	Osservata	PLUSIRESPO

## Esempio flusso di lavoro

Esiste un esempio di flusso di lavoro:

### PLUSISOP00: Completare l'azione attività

Il PLUSISOP00 flusso di lavoro attiva un'azione per modificare lo stato di un'attività in COMP (completata).

Il PLUSISOP00 flusso di lavoro è associato ad ogni operazione nell'esempio PLUSIPREPA procedura operativa standard. Se si inizia una delle operazioni, lo stato dell'operazione viene automaticamente contrassegnato come completata.

## Risorse di esempio

La tabella di seguito riportata elenca le risorse di esempio fornite nel dominio PLUSICATCPLMAP:

Tabella 36. Risorse di esempio

Risorsa	Descrizione	Tipo di risorsa
BASCOMEYE	Istituto oculistico Bascombe	RESOURCES\HOSPITAL
BLUEFISHW	Warehouse pesce azzurro	RESOURCES\WAREHOUSE
DOCTORSH	Medico dell'ospedale	RESOURCES\HOSPITAL
MERYCYH	Ospedale di beneficenza	RESOURCES\HOSPITAL
MAMICHILD	Ospedale pediatrico di Miami	RESOURCES\HOSPITAL
SFFOODDIST	Distribuzione cibo sud della Florida	RESOURCES\WAREHOUSE
TITLEASING	Tropical Trailer Leasing Corporation	RESOURCES\WAREHOUSE
UNIMIAMI	Università dell'ospedale di Miami	RESOURCES\HOSPITAL
WTDCDIST	WTDC Distribution Center Miami	RESOURCES\WAREHOUSE





---

## Capitolo 5. Personalizzazione della soluzione

La personalizzazione della soluzione in modo che si adatti alla propria operazione particolare, comprende le attività trattate in questa sezione in relazione all'interfaccia utente e alla tabella delle proprietà di sistema. La personalizzazione è strettamente legata all'integrazione della soluzione e i link appropriati sono inclusi nell'evento e negli argomenti KPI (key performance indicator) riportati in questa sezione.

---

### Personalizzazione dell'interfaccia utente

È possibile personalizzare gli elementi dell'interfaccia utente di IBM Intelligent Operations Center per adattarli alla propria operazione

Oltre a personalizzare il layout e l'aspetto dei portlet, è possibile anche creare nuove pagine. Per ulteriori informazioni, consultare la documentazione del prodotto WebSphere Portal.

#### Informazioni correlate:



Documentazione del prodotto IBM WebSphere Portal 7

### Localizzazione dell'interfaccia utente

Le impostazioni del browser determinano le impostazioni di lingua, data e ora per l'interfaccia utente di IBM Intelligent Operations Center. Un amministratore può personalizzare il formato di data e ora.

In IBM Intelligent Operations Center, le impostazioni del browser determinano la lingua del testo. Nel caso in cui la lingua non è disponibile in IBM Intelligent Operations Center, viene utilizzata quella con una correlazione più vicina; ad esempio, francese canadese ritorna al francese che a sua volta ritorna all'inglese che è sempre disponibile. Le impostazioni del browser, determinano anche il fuso orario per tutte le date e le ore visualizzate. Data e ora in IBM Intelligent Operations Center vengono automaticamente regolati con il fuso orario del browser.

Tutte le date e le ore vengono presentate in base al fuso orario nel formato specificato nella tabella di database delle proprietà di sistema. Le proprietà di sistema mantengono le stringhe del formato data e ora. Per modificare il valore nel database modificando la proprietà, seguire il link alla fine dell'argomento.

#### Concetti correlati:

“Specifica dei dati di configurazione del sistema” a pagina 178

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

“Utilizzo CAP per eventi KPI” a pagina 96

Il WebSphere Message Broker, che è fornito come parte di IBM Intelligent Operations Center, accetta messaggi di evento CAP ed utilizza i dati nei calcoli KPI (Key performance indicator).

### Elenco di portlet

IBM Intelligent Operations Center è una soluzione basata su portlet che utilizza la tecnologia di portale per fornire strumenti e le informazioni visualizzate. Tutti i portlet inclusi in IBM Intelligent Operations Center sono elencati nelle sezioni che seguono.

#### Portlet utente

La seguente tabella elenca i portlet utente inclusi in IBM Intelligent Operations Center. La tabella elenca anche in quale pagina di esempio è disponibile ciascun portlet.

È possibile personalizzare i portlet. Per ulteriori informazioni, consultare il collegamento alla fine di questo argomento.

Tabella 37. Portlet utente in IBM Intelligent Operations Center

Portlet	Descrizione	Viste delle pagine di esempio
“Contatti” a pagina 271	Il portlet Contatti può visualizzare un elenco dei contatti organizzati per categoria. È possibile organizzare i contatti in categorie basate sulle persone con cui è necessario comunicare. Ad esempio, è possibile creare una categoria per i contatti di lavoro generali e un'altra categoria per i contatti di lavoro del progetto. Con il portlet Contatti è possibile comunicare con le persone e modificare i gruppi, i contatti o il proprio stato in linea.	<ul style="list-style-type: none"> <li>• “Vista Supervisore: Stato” a pagina 267</li> <li>• “Vista Supervisore: Operazioni” a pagina 268</li> <li>• “Vista Operatore: Operazioni” a pagina 269</li> </ul>
“Dettagli” a pagina 272	Dettagli è un portlet di elenco interattivo. Tutti gli eventi per cui è stata concessa la visualizzazione sono visibili nell'elenco di eventi e su qualsiasi portlet di mappe collegato al portlet Dettagli.	<ul style="list-style-type: none"> <li>• “Vista Supervisore: Operazioni” a pagina 268</li> <li>• “Vista Operatore: Operazioni” a pagina 269</li> <li>• “Vista Mappa ubicazioni” a pagina 270</li> </ul>
“Drill Down KPI (Key Performance Indicator)” a pagina 275	Per concentrarsi su una specifica categoria KPI nel portlet Drill Down KPI (Key Performance Indicator), fare clic sulla categoria nel portlet Stato. Questa categoria viene quindi visualizzata autonomamente nel portlet Drill Down KPI (Key Performance Indicator). È possibile utilizzare l'elenco per esaminare gli indicatori KPI sottostanti fino a quando si raggiungono i dettagli del KPI che ha causato la modifica dello stato.	<ul style="list-style-type: none"> <li>• “Vista Supervisore: Stato” a pagina 267</li> </ul>
“Mappa ubicazioni” a pagina 276	Utilizzare il portlet Mappa ubicazioni per visualizzare gli eventi contrassegnati sulla mappa ubicazioni. Una mappa ubicazioni in IBM Intelligent Operations Center è una mappa o piano con aree predefinite per l'interazione, ad esempio, i posti a sedere di un principale stadio sportivo.	<ul style="list-style-type: none"> <li>• “Vista Mappa ubicazioni” a pagina 270</li> </ul>

Tabella 37. Portlet utente in IBM Intelligent Operations Center (Continua)

Portlet	Descrizione	Viste delle pagine di esempio
"Mappa" a pagina 279	<p>Nel portlet Mappa:</p> <p>Una mappa della regione geografica con i contrassegni di risorse e di eventi.</p> <p>Un modulo filtro per la selezione di categorie di eventi da mostrare sulla mappa e nei portlet collegati al portlet Mappa.</p> <p>Un modulo filtro per la selezione di funzionalità di risorse da mostrare sulla mappa e nella scheda <b>Risorse</b> sul portlet Dettagli collegato. Per visualizzare questo modulo, selezionare prima <b>Visualizza risorse vicine</b> sul portlet Dettagli.</p>	<ul style="list-style-type: none"> <li>• "Vista Supervisore: Operazioni" a pagina 268</li> <li>• "Vista Operatore: Operazioni" a pagina 269</li> </ul>
"Attività personali" a pagina 284	<p>Un utente collegato può visualizzare le attività che gli sono state assegnate nel portlet Attività personali. Nel portlet Attività personali, le attività vengono raggruppate dalle rispettive procedure operative standard principali. Ogni procedura operativa standard corrisponde a un singolo evento.</p>	<ul style="list-style-type: none"> <li>• "Vista Supervisore: Stato" a pagina 267</li> <li>• "Vista Supervisore: Operazioni" a pagina 268</li> <li>• "Vista Operatore: Operazioni" a pagina 269</li> </ul>
"Notifiche" a pagina 287	<p>Il portlet Notifiche fornisce un elenco interattivo e dinamico di avvisi determinato dalle modifiche degli indicatori KPI e degli eventi correlati. Lo scopo di questo portlet è di evidenziare le modifiche allo stato eventi o KPI. L'elenco contiene i dettagli chiave per ciascuno degli avvisi.</p>	<ul style="list-style-type: none"> <li>• "Vista Supervisore: Stato" a pagina 267</li> <li>• "Vista Supervisore: Operazioni" a pagina 268</li> <li>• "Vista Operatore: Operazioni" a pagina 269</li> </ul>
"Report" a pagina 288	<p>Utilizzare il portlet Report per visualizzare un report di eventi come grafico. Il portlet fornisce diverse opzioni in base alle quali raggruppare gli eventi, ed è possibile scegliere gli eventi in base a una data o intervallo di date particolare. I report in questione consentono di pianificare gli eventi correnti e futuri.</p>	<ul style="list-style-type: none"> <li>• "Supervisore: Report " a pagina 270</li> <li>• "Operatore: Report" a pagina 270</li> </ul>
"Stato" a pagina 291	<p>Il portlet Stato fornisce un riepilogo di livello esecutivo dello stato degli indicatori KPI sulle organizzazioni per le quali si dispone dell'autorizzazione di visualizzazione. Utilizzare questo portlet per visualizzare modifiche aggiornate nello stato KPI, in modo che sia possibile pianificare e intraprendere eventuali azioni se necessario.</p>	<ul style="list-style-type: none"> <li>• "Vista Supervisore: Stato" a pagina 267</li> </ul>

### Attività correlate:

“Personalizzazione dei portlet” a pagina 145

In qualità di amministratore è possibile modificare le impostazioni del portlet per personalizzare un portlet.

### Portlet di gestione

La seguente tabella elenca i portlet di gestione inclusi in IBM Intelligent Operations Center. I portlet di gestione sono nella pagina Gestione.

Tabella 38. Portlet di gestione in IBM Intelligent Operations Center

Portlet	Descrizione
“Informazioni” a pagina 195	Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.
“Console di gestione” a pagina 203	Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.
“Verifica dei componenti” a pagina 210	Lo strumento Controllo di verifica del sistema esegue il test dei componenti presenti in IBM Intelligent Operations Center per verificare se sono accessibili e funzionanti.
“Riepilogo autorizzazioni utente” a pagina 80	Il portlet Riepilogo autorizzazioni utente visualizza i dettagli dell'appartenenza al gruppo e le autorizzazioni concesse agli utenti.
“KPI (Key Performance Indicators)” a pagina 168	Nel portlet KPI (Key Performance Indicators) è possibile visualizzare, modificare, copiare, creare ed eliminare KPI. È possibile anche personalizzare le gerarchie di KPI nei portlet Stato e Drill Down KPI (Key Performance Indicator).
“Gestore mappa ubicazioni” a pagina 176	Utilizzare il portlet Gestore mappa ubicazioni per personalizzare il portlet Mappa ubicazioni.
“SOP (Standard Operating Procedure)” a pagina 127	È possibile definire procedure operative standard e le attività per la gestione degli eventi inseriti in IBM Intelligent Operations Center. Utilizzare il portlet SOP (Standard Operating Procedure) per accedere alle applicazioni procedura operativa standard, matrice di selezione procedura operativa standard e designer flusso di lavoro in Tivoli Service Request Manager.
“Programmazione script di eventi” a pagina 107	Utilizzare il portlet Programmazione script di eventi per scrivere uno script e creare un elenco sequenziale di eventi da pubblicare a intervalli di tempo predefiniti.
“Publisher di esempio” a pagina 103	Il portlet Publisher di esempio è uno strumento di test automatizzato rivolto a un amministratore che gestisce o verifica la soluzione. Un amministratore può utilizzare il portlet Publisher di esempio come applicazione client per eseguire il test della pubblicazione di messaggi CAP in IBM Intelligent Operations Center. Il portlet Publisher di esempio può eliminare il requisito per la creazione manuale di un'applicazione client del test.

### Attività correlate:

“Personalizzazione dei portlet”

In qualità di amministratore è possibile modificare le impostazioni del portlet per personalizzare un portlet.

## Creazione e personalizzazione di una pagina

È possibile creare nuove pagine da includere in IBM Intelligent Operations Center e specificare quali portlet visualizzare in quelle pagine. È possibile personalizzare l'aspetto e il layout dei portlet inclusi in ogni pagina.

### Informazioni su questa attività

Utilizzare l'interfaccia utente WebSphere Portal per personalizzare le pagine e i portlet.

**Nota:** Quando si crea o si modifica il layout di una pagina, assicurarsi che i portlet funzionino correttamente e che soddisfino le seguenti regole:

- I portlet Mappa e Dettagli devono trovarsi nello stesso gruppo e sulla stessa pagina per consentire l'aggiunta di un evento dal portlet Mappa.
- I portlet Attività personali e Dettagli devono trovarsi nello stesso gruppo e nella stessa pagina per consentire la richiesta dei dettagli dell'evento dal portlet Attività personali o la richiesta dei dettagli della Procedura operativa standard dal portlet Dettagli.

### Procedura

1. Per aprire WebSphere Portal, fare clic sulla scheda **Amministrazione**.
2. In WebSphere Portal, fare clic su **Interfaccia utente del portale**.
3. Fare clic sull'opzione richiesta:
  - Per gestire le pagine o creare nuove pagine, fare clic su **Gestisci pagine**.
  - Per registrare temi e skin, impostare il tema predefinito ed impostare lo skin predefinito per ogni tema, fare clic su **Temi e skin**.
  - Per personalizzare gli elementi chiave del sito nei temi, incluso il banner, la navigazione, i tipi di carattere ed i colori, fare clic su **Personalizzazione temi**.
4. Apportare le modifiche necessarie. Per ulteriori informazioni sull'utilizzo di WebSphere Portal per personalizzare i portlet, consultare il link nella parte inferiore dell'argomento per la documentazione del prodotto WebSphere Portal.

### Informazioni correlate:



Documentazione del prodotto IBM WebSphere Portal 7

## Personalizzazione dei portlet

In qualità di amministratore è possibile modificare le impostazioni del portlet per personalizzare un portlet.

### Informazioni su questa attività

Esistono due modalità di personalizzazione, ciascuna che consente la modifica delle impostazioni del portlet per tutti gli utenti:

- L'opzione **Modifica impostazioni condivise** cambia solo l'istanza del portlet utilizzata quando si modificano le impostazioni.
- L'opzione **Configura** modifica le impostazioni globali del portlet per tutte le istanze del portlet ovunque si verifichino.

Le modalità di personalizzazione disponibili dipendono dalle autorizzazioni associate al proprio ID utente. Le impostazioni globali vengono sostituite dalle impostazioni condivise.

## Procedura

1. Collegarsi al portale delle soluzioni come amministratore.
2. Fare clic nell'angolo in alto a destra del portlet per visualizzare il menu del portlet.
3. Fare clic su **Modifica delle impostazioni condivise** o su **Configura**.
4. Immettere le impostazioni nei campi forniti.
5. Per chiudere la finestra delle impostazioni, fare clic su uno dei pulsanti:
  - **Salva** per salvare le modifiche.
  - **Annulla** per annullare le modifiche.
  - **Reimposta su valori predefiniti** per ripristinare le impostazioni globali predefinite.

## Risultati

Eventuali nuove impostazioni salvate diventano effettive la volta successiva che il portlet viene aggiornato. I valori delle impostazioni globali predefinite fornite con IBM Intelligent Operations Center vengono utilizzati per qualsiasi parametro che non è stato reimpostato.

### Impostazioni portlet Informazioni

Personalizzare il portlet Informazioni modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

#### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Informazioni. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 39. Parametri di personalizzazione del portlet Informazioni

Parametro	Descrizione	Valore predefinito
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	400
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600

#### Concetti correlati:

“Informazioni” a pagina 195

Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.

### Impostazioni portlet Console di gestione

Personalizzare il portlet Console di gestione modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

#### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Console di gestione. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 40. Parametri di personalizzazione del portlet Console di gestione

Parametro	Descrizione	Valore predefinito
-----------	-------------	--------------------

Tabella 40. Parametri di personalizzazione del portlet Console di gestione (Continua)

JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	AdministrationConsolePortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	400
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	450
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione viene visualizzato ed è Console di gestione.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

#### Concetti correlati:

“Console di gestione” a pagina 203

Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.

### Impostazioni portlet Contatti

Personalizzare il portlet Contatti modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Contatti. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 41. Parametri di personalizzazione del portlet Contatti

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	SametimeWebClientPortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	250
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione è visualizzato e visualizzato è: Contatti.



Tabella 41. Parametri di personalizzazione del portlet Contatti (Continua)

Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.
---------------------------	--	---

**Concetti correlati:**

“Contatti” a pagina 271

Utilizzare il portlet Contatti per inviare messaggi istantanei all'interno della soluzione.

**Impostazioni portlet Dettagli**

Personalizzare il portlet Dettagli modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

**I parametri di personalizzazione**

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Dettagli. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 42. Parametri di personalizzazione per il portlet Dettagli

Nome parametro	Descrizione	Valore predefinito
Colonne	Specifiche e ordine di colonne da visualizzare nell'elenco.	[{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}]
Condizioni	Ulteriori condizioni per la visualizzazione degli eventi o delle risorse, le condizioni aggiuntive non possono essere sovrascritte utilizzando la barra degli strumenti o il filtro della mappa. L'impostazione predefinita è che non vengono applicate condizioni supplementari.	[]
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	CommonEventsPortletHelp
Nascondi eventi aggiunti	Impostazione true o false per nascondere o visualizzare il pulsante <b>Aggiungi eventi</b> e l'opzione di menu a comparsa.	true

Tabella 42. Parametri di personalizzazione per il portlet *Dettagli* (Continua)

Nascondi risorse aggiunte	Impostazione true o false per nascondere o visualizzare il pulsante <b>Aggiungi risorse</b> nella scheda <b>Risorse</b> .	true
Nascondi eventi	Impostazione true o false per nascondere o visualizzare la scheda <b>Eventi e incidenti</b> .	false
Nascondi risorse	Impostazione true o false per nascondere o visualizzare la scheda <b>Risorse</b> .	false
Nascondi barra degli strumenti	Impostazione true o false per nascondere o visualizzare la barra degli strumenti nella parte superiore dell'elenco.	true
Ignora modalità annulla risorsa	True o false per confermare o ignorare il messaggio di annullamento della modalità in entrata dal portlet Mappa.	false
Ignora creazione evento	Impostazione true o false per confermare o ignorare gli eventi creati nel portlet Mappa dall'utente.	false
Ignora modifiche al filtro degli eventi	Impostazione true o false per confermare o ignorare le selezioni del filtro degli eventi effettuate nel portlet Mappa dall'utente.	false
Ignora selezione evento	Impostazione true o false per confermare o ignorare la selezione dell'evento in entrata effettuata nel portlet Mappa dall'utente.	false
Ignora attività evento	Impostazione true o false per confermare o ignorare tutte le selezioni del menu a comparsa dell'evento.	false
Ignora reimpostazione mappa	Impostazione true o false per confermare o ignorare un clic del pulsante <b>Risorse</b> nel portlet.	false
Ignora filtro risorsa modificato	Impostazione true o false per confermare o ignorare le selezioni del filtro delle risorse effettuate nel portlet Mappa dall'utente.	false
Ignora attività risorsa	Impostazione true o false per confermare o ignorare tutte le selezioni del menu a comparsa della risorsa.	false
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra i portlet Mappa, Dettagli e Mappa ubicazioni sulla stessa pagina.	default
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	350
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600

Tabella 42. Parametri di personalizzazione per il portlet Dettagli (Continua)

Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Dettagli.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

**Nota:** La spiegazione di cosa accade al titolo del portlet quando si fornisce un raggruppamento di risorse vale anche per il titolo della colonna che viene originato dallo stesso raggruppamento di risorse.

## parametro Colonne

Il valore del parametro **colonne** è un array di oggetti JSON che può essere configurato come descritto in Tabella 43.

Tabella 43. Gli oggetti all'interno del valore del parametro colonne del portlet Dettagli

Oggetto	Contiene
id	Identificativo colonna per indicare che la colonna deve essere visualizzata
width	Numero di pixel che indica la larghezza della colonna
formato	Stringa che rappresenta il formato da utilizzare per le colonne data e ora, la voce sovrascrive l'impostazione nella tabella sysprop
sortAscending	<ul style="list-style-type: none"> <li>Il valore true per utilizzare un ordine del criterio di ordinamento crescente negli elementi della colonna</li> <li>Il valore false per utilizzare un ordine del criterio di ordinamento discendente negli elementi della colonna</li> </ul>
sortPriority	<ul style="list-style-type: none"> <li>Numero che indica la priorità di ordinamento di quella colonna tra tutte le colonne, minore è il numero, più alta è la priorità</li> <li>Nessun valore, lasciare vuoto per utilizzare la priorità di ordinamento predefinita delle colonne</li> <li>Il valore -1 per disabilitare la priorità di ordinamento predefinita delle colonne</li> </ul>
titolo	Titolo di intestazione della colonna, lasciare vuoto per utilizzare il titolo di intestazione predefinita

Le colonne vengono visualizzate nel portlet nello stesso ordine indicato negli oggetti JSON che costituiscono il valore del parametro **columns**. Solo le colonne con gli identificativi della colonna specificata nel valore vengono visualizzate, tutte le altre colonne vengono nascoste. Se il valore del

parametro **columns** viene omissso, vengono visualizzate le colonne come indicato nell'impostazione predefinita mostrate nella prima riga di Tabella 42 a pagina 148.

I valori possibili per gli identificativi di colonna sono descritte in Tabella 44.

Tabella 44. Identificativi di colonna validi per il portlet Dettagli

Identificativo colonna	Descrizione
commonevents.id	UUID fornito all'evento in tabella eventi comuni
commonevents.externalEventId	Identificativo evento assegnato dal mittente dell'evento
commonevents.specification	Specifica del formato seguito dall'evento, ad esempio, CAP
commonevents.eventType	Valore non convertito per il codice specifico del sistema che indica se un evento è stato incrementato o meno: Evento o Incidente
commonevents.sent	Ora invio come specificato dal mittente dell'evento
commonevents.headline	Testo del titolo che descrive l'evento
testo commonevents.hover	Testo al passaggio del mouse che descrive l'evento
commonevents.category	Valore categoria non convertito
commonevents.certainty	Valore certezza non convertito
commonevents.severity	Valore severità non convertito
commonevents.urgency	Valore urgenza non convertito
commonevents.url	Indirizzo Web dell'URL per le informazioni aggiuntive sull'evento
commonevents.externalWorkOrderId	Identificativo ordine di lavoro associato, di solito l'ID Tivoli Service Request Manager procedura operativa standard
commonevents.areaId	Identificativo area mappa ubicazioni se l'evento è collegato ad una mappa ubicazioni
commonevents.largeIcon	Icona utilizzata per rappresentare l'evento nella mappa
commonevents.largeHiliteIcon	Icona utilizzata quando l'evento viene evidenziato nella mappa
commonevents.largeGreyIcon	Icona utilizzata quando l'evento viene disabilitato nella mappa
commonevents.smallIcon	Icona utilizzata per l'evento nell'elenco
commonevents.user1	Il valore impostato all'interno della politica Tivoli Netcool/Impact
commonevents.user2	Il valore impostato dall'utente all'interno della politica Tivoli Netcool/Impact
commonevents.user3	Il valore impostato dall'utente all'interno della politica Tivoli Netcool/Impact
commonevents.user4	Il valore impostato dall'utente all'interno della politica Tivoli Netcool/Impact
commonevents.user5	Il valore impostato dall'utente all'interno della politica Tivoli Netcool/Impact

## Parametro condizioni

Il valore del parametro **condizioni** è un array di oggetti JSON che può essere configurato come descritto in Tabella 45 a pagina 152.

Tabella 45. Gli oggetti all'interno del valore parametro condizioni del portlet Dettagli

Tipo di oggetto	Contiene
selector	Identificatore della colonna in cui viene applicato l'operatore viene
operator	Operatore SQL che viene applicato ai valori del selettore; le opzioni sono: <ul style="list-style-type: none"> <li>• <code>contains</code> quando la colonna selector contiene il valore, questa opzione è l'impostazione predefinita</li> <li>• <code>equals</code> quando la colonna selector è uguale al valore</li> <li>• <code>notEquals</code> la colonna selector non è uguale al valore</li> <li>• <code>startsWith</code> quando la colonna selector inizia con il valore</li> <li>• <code>endsWith</code> quando la colonna selector finisce con il valore</li> </ul>
values	Viene visualizzato il valore della colonna, il valore deve essere il valore chiave non convertito come specificato nella tabella precedente

**Nota:**

Il parametro **condizioni** definisce i criteri in aggiunta ai criteri forniti nel filtro del portlet Mappa. Questi criteri sovrascrivono le condizioni specificate nel filtro mappa o nella barra degli strumenti.

**Nota:** La barra degli strumenti è nascosta per impostazione predefinita.

Ad esempio, è necessaria la seguente modifica alle colonne:

- Visualizzare solo le colonne **Inviato**, **Titolo**, **Categoria**, e **URL**.
- Modificare la larghezza della colonna **Inviati** con 12.
- Modificare il formato della colonna **Inviati** con g-`MMM-yyyy HH:mm`.
- Modificare la priorità del criterio di ordinamento della colonna **Inviati** con 2 e la colonna **Categoria** con 1.

Queste modifiche vengono visualizzate quando si immette quanto segue nel campo **Colonne** e si salvano le preferenze:

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"}, {"id": "commonevents.headline"}, {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

Ad esempio, si desidera visualizzare solo gli eventi che soddisfano le seguenti condizioni:

- Una **Gravità Estrema** o **Grave**
- Un **Tipo evento Incidente**

Queste modifiche vengono visualizzate quando si immette quanto segue nel campo **Condizioni** e si salvano le preferenze:

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]}, {"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

**Concetti correlati:**

“Dettagli” a pagina 272

Utilizzare il portlet Dettagli per visualizzare, monitorare e gestire gli eventi in IBM Intelligent Operations Center.

**Impostazioni portlet Drill Down KPI (Key Performance Indicator)**

Personalizzare il portlet Drill Down KPI (Key Performance Indicator) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Drill Down KPI (Key Performance Indicator). I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 46. Parametri di personalizzazione del portlet Drill Down KPI (Key Performance Indicator)

Parametro	Descrizione	Valore predefinito
Colonne	Specifiche e ordine di colonne da visualizzare nell'elenco.	[{"sortPriority":"1", "sortAscending":"true", "id":"kpi.NAME"}]
Colori KPI personalizzati	Colori utilizzati nel portlet per indicare lo stato dei KPI, ad esempio, è possibile immettere:  {"acceptable":"#7f7f7f", "take_action":"#34333"}  I colori che si immettono qui sovrascrivono i colori forniti dalla soluzione.	{}
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	KpiDrillDownPortletHelp
Abilita filtro KPI	Impostazione di true o false per abilitare o disabilitare un filtro KPI in base alle informazioni contenute nell'impostazione del parametro <b>filtro KPI</b> .	false
Nascondi barra degli strumenti	Impostazione true o false per nascondere o visualizzare la barra degli strumenti nella parte superiore del portlet.	true
Filtro KPI	ID dei KPI da visualizzare quando <b>Abilita filtro KPI</b> è impostato su true per il portlet, ad esempio, è possibile immettere:  ["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]	[]
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra i portlet Drill Down KPI (Key Performance Indicator) e Stato sulla stessa pagina.	default
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	350
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Drill Down KPI (Key Performance Indicator).

Tabella 46. Parametri di personalizzazione del portlet Drill Down KPI (Key Performance Indicator) (Continua)

Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.
---------------------------	--	---

**Nota:** La spiegazione di cosa accade al titolo del portlet quando si fornisce un raggruppamento di risorse vale anche per il titolo della colonna che viene originato dallo stesso raggruppamento di risorse.

## Parametro colonne

Il valore del parametro **colonne** è un array di oggetti JSON che può essere configurato come descritto nella seguente tabella.

Tabella 47. Gli oggetti all'interno del valore del parametro colonne del portlet Drill Down KPI (Key Performance Indicator)

Oggetto	Contiene
sortPriority	<ul style="list-style-type: none"> <li>Numero che indica la priorità di ordinamento di quella colonna tra tutte le colonne, minore è il numero, più alta è la priorità</li> <li>Nessun valore, lasciare vuoto per utilizzare la priorità di ordinamento predefinita della colonna</li> <li>-1 per disabilitare la priorità di ordinamento predefinita della colonna</li> </ul>
sortAscending	<ul style="list-style-type: none"> <li>true per utilizzare un ordine del criterio di ordinamento crescente negli elementi della colonna</li> <li>false per utilizzare un ordine del criterio di ordinamento decrescente negli elementi della colonna</li> </ul>
id	Identificativo colonna per indicare che la colonna deve essere visualizzata

Le colonne vengono visualizzate nel portlet nello stesso ordine indicato negli oggetti JSON che costituiscono il valore del parametro **columns**. Solo le colonne con gli identificativi della colonna specificata nel valore vengono visualizzate, tutte le altre colonne vengono nascoste. Se il valore del parametro **columns** viene omesso, vengono visualizzate le colonne come indicato nell'impostazione predefinita mostrate nella prima riga di Tabella 46 a pagina 153.

I valori possibili per gli identificativi di colonna sono descritte nella tabella.

Tabella 48. Identificativi di colonna validi per il portlet Drill Down KPI (Key Performance Indicator)

Identificativo colonna	Descrizione
kpi.NAME	Nome del KPI
kpi.CURRENT.VALUE	Il valore corrente del KPI
kpi.CURRENT.STATUS	Lo stato corrente del KPI
kpi.CALCULATION.TIME	Ora in cui KPI è stato calcolato



### Concetti correlati:

“Drill Down KPI (Key Performance Indicator)” a pagina 275

Utilizzare il portlet Drill Down KPI (Key Performance Indicator) per visualizzare ulteriori informazioni su una categoria KPI, lo stato dei KPI sottostanti.

## Impostazioni portlet KPI (Key Performance Indicators)

Personalizzare il portlet KPI (Key Performance Indicators) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet KPI (Key Performance Indicators). I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 49. Parametri di personalizzazione del portlet KPI (Key Performance Indicators)

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	KpiManagerPortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	500
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: KPI (Key Performance Indicators).
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

### Concetti correlati:

“KPI (Key Performance Indicators)” a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

## Impostazioni portlet Mappa ubicazioni

Personalizzare il portlet Mappa ubicazioni modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 50. I valori del parametro di personalizzazione del portlet Mappa ubicazioni

Parametro	Descrizione	Valore predefinito
-----------	-------------	--------------------

Selezioni filtro predefinite	Categorie di eventi predefinite da visualizzare sulla mappa. Immettere uno o più nomi separati da un punto e virgola e senza spazi.	CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other
Colore di evidenziazione area predefinito	Il colore predefinito di un settore che viene evidenziato quando si passa sull'area utilizzando il cursore.	#808080
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	LocationMapPortletHelp
Selezione mappa predefinita	Nome della mappa ubicazioni da visualizzare nel portlet.	Miami SunLife Stadium
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	400
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra i portlet Mappa, Dettagli e Mappa ubicazioni sulla stessa pagina.	default
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Mappa ubicazioni.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

#### Concetti correlati:

“Mappa ubicazioni” a pagina 276

Utilizzare il portlet Mappa ubicazioni per visualizzare gli eventi contrassegnati sulla mappa ubicazioni. Una mappa ubicazioni in IBM Intelligent Operations Center è una mappa o piano con aree predefinite per l'interazione, ad esempio, i posti a sedere di un principale stadio sportivo.

### Impostazioni portlet Gestore mappa ubicazioni

Personalizzare il portlet Gestore mappa ubicazioni modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

#### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 51. I valori del parametro di personalizzazione del portlet Gestore mappa ubicazioni

Parametro	Descrizione	Valore predefinito
Colore predefinito per la nuova area selezionata	Colore predefinito di un'area che tracciata sulla mappa e selezionata.	#4AA02C
Colore predefinito per l'area selezionata salvata	Colore predefinito di un'area sulla mappa che salvata e selezionata.	#808080
Colore predefinito per la nuova area	Colore predefinito di un'area che tracciata sulla mappa.	#009900
Colore predefinito per l'area salvata	Il colore predefinito di un area salvata sulla mappa.	#808080
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	LocationMapManagerPortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	400
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Gestore mappa ubicazioni.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

#### Concetti correlati:

“Gestore mappa ubicazioni” a pagina 176

Utilizzare il portlet Gestore mappa ubicazioni per personalizzare il portlet Mappa ubicazioni.

### Impostazioni portlet Mappa

Personalizzare il portlet Mappa modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

#### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Mappa. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 52. I valori del parametro di personalizzazione

Parametro	Descrizione	Valore predefinito
-----------	-------------	--------------------

Tabella 52. I valori del parametro di personalizzazione (Continua)

Centra latitudine	Le coordinate specifiche per impostare il punto centrale della mappa. L'ubicazione corrente della mappa viene visualizzata a destra dei campi. È possibile ingrandire e ottenere una panoramica dell'associazione per la propria ubicazione richiesta, quindi tagliare e incollare i valori visualizzati nei campi corrispondenti.	25.780416
Centra longitudine		-80.203629
Livello di zoom	Livello di ingrandimento standard per la mappa. L'intervallo di livelli di zoom validi disponibili dipende dalla mappa di base. In genere, l'intervallo è compreso da 1 a salire. Il valore 1 è il livello di zoom minimo che visualizza l'ingrandimento minimo della mappa. Ad esempio, la mappa di base ArcGIS predefinita fornita con la soluzione visualizza dettagli geografici fino ad un livello di zoom massimo di 12.	11
Tipo livello base	Valore per il tipo della mappa di base.	ARC_GIS_REST
URL livello base	URL della mappa di base. L'URL deve contenere, nell'ordine corretto, i segnaposto che rappresentano le coordinate x, y e z della mappa. È possibile selezionare una mappa dal server Esri GIS o un servizio GIS pubblicamente disponibile.	<a href="http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}">http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}</a>
Feed KML o URL file	URL per visualizzare i dati KML. Immettere un URL per un'ubicazione sullo stesso server del portlet con lo stesso dominio e porta. Per assicurarsi di implementare questa condizione, immettere solo URL che iniziano con il carattere '/' o barra, in modo che il browser selezioni il domini e la porta corrente. Per più stringhe URL utilizzare un punto e virgola, senza spazi tra gli URL. Se il sito Web richiesto non è locale, utilizzare un server proxy sul server del portale per accedere al sito. <b>Nota:</b> Utilizzare questa opzione per piccole modifiche locali, ma è necessario considerare la quantità di dati coinvolti, in modo che la visualizzazione non sia ridondante o influisca le prestazioni.	Non esiste un valore predefinito fornito con la soluzione.

Tabella 52. I valori del parametro di personalizzazione (Continua)

La quantità di elementi da visualizzare	Limite per il numero di contrassegni visualizzati su una vista. Immettere il numero massimo di contrassegni che è possibile visualizzare. Se il numero di contrassegni nell'area della mappa in vista supera questo limite, nessun contrassegno viene visualizzato e viene visualizzato un messaggio di avvertenza. L'utente può quindi scegliere se caricare i contrassegni o modificare la vista.	250
Selezioni filtro predefinite	Categorie di eventi predefinite da visualizzare sulla mappa. Immettere uno o più nomi separati da un punto e virgola e senza spazi.	CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra i portlet Mappa, Dettagli e Mappa ubicazioni sulla stessa pagina.	default
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Mappa.
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	NavigatorPortletHelp
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

**Concetti correlati:**

“Mappa” a pagina 279

Utilizzare il portlet Mappa per visualizzare eventi e risorse presenti su una mappa.

**Impostazioni portlet Attività personali**

Personalizzare il portlet Attività personali modificando le impostazioni nei campi della finestra

**Impostazioni condivise.**

## I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Attività personali. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 53. Parametri di personalizzazione del portlet Attività personali

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	ActivitiesPortletHelp
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra portlet sulla stessa pagina. Ad esempio, un nome comune può configurare la comunicazione tra i portlet Attività personali e Dettagli.	default
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	200
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Attività personali.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

### Concetti correlati:

“Attività personali” a pagina 284

Il portlet Attività personali visualizza un elenco dinamico di attività di proprietà del gruppo di cui l'utente collegato all'interfaccia è membro.

## Impostazioni portlet Notifiche

Personalizzare il portlet Notifiche modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Notifiche. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 54. Parametri di personalizzazione del portlet Notifiche

Parametro	Descrizione	Valore predefinito
Colonne	Specifiche e ordine di colonne da visualizzare nell'elenco.	[{"id": "notifications.HEADLINE"}, {"id": "notifications.SENTFROM"}, {"id": "notifications.SENTTIME", "width" : "10", "format": "yyyy-MM-dd HH:mm:ss"}]
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	CityCoordinatorPortletHelp

Tabella 54. Parametri di personalizzazione del portlet Notifiche (Continua)

Nascondi barra degli strumenti	Impostazione true o false per nascondere o visualizzare la barra degli strumenti nella parte superiore del portlet.	true
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	200
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Notifiche.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

**Nota:** La spiegazione di cosa accade al titolo del portlet quando si fornisce un raggruppamento di risorse vale anche per il titolo della colonna che viene originato dallo stesso raggruppamento di risorse.

## Parametro colonne

Il valore del parametro **colonne** è un array di oggetti JSON che può essere configurato come descritto in Tabella 55.

Tabella 55. Gli oggetti all'interno del valore del parametro colonne del portlet Notifiche

Oggetto	Contiene
id	Identificativo colonna per indicare che la colonna deve essere visualizzata
width	Numero di pixel che indica la larghezza della colonna
format	Stringa che rappresenta il formato da utilizzare per le colonne data e ora, la voce sovrascrive l'impostazione nella tabella sysprop
sortAscending	<ul style="list-style-type: none"> <li>true per utilizzare un ordine del criterio di ordinamento crescente negli elementi della colonna</li> <li>false per utilizzare un ordine del criterio di ordinamento decrescente negli elementi della colonna</li> </ul>
sortPriority	<ul style="list-style-type: none"> <li>Numero che indica la priorità di ordinamento di quella colonna tra tutte le colonne, minore è il numero, più alta è la priorità</li> <li>Nessun valore, lasciare vuoto per utilizzare la priorità di ordinamento predefinita della colonna</li> <li>-1 per disabilitare la priorità di ordinamento predefinita della colonna</li> </ul>
titolo	Titolo di intestazione della colonna, lasciare vuoto per utilizzare il titolo di intestazione predefinita



Le colonne vengono visualizzate nel portlet nello stesso ordine indicato negli oggetti JSON che costituiscono il valore del parametro **columns**. Solo le colonne con gli identificativi della colonna specificata nel valore vengono visualizzate, tutte le altre colonne vengono nascoste. Se il valore del parametro **columns** viene omissso, vengono visualizzate le colonne come indicato nell'impostazione predefinita mostrate nella prima riga di Tabella 54 a pagina 160.

I valori possibili per gli identificativi di colonna sono descritte in Tabella 56.

Tabella 56. Identificativi di colonna validi per il portlet Notifiche

Identificativo colonna	Descrizione
notifications.ID	UUID specificato alla notifica nella tabella delle notifiche
notifications.CATEGORY	Valore non convertito della categoria dell'evento o del KPI correlato alla notifica
notifications.SENTFROM	Servizio che ha generato la notifica
notifications.SENTTOGROUP	Elenco di gruppi che possono accedere alla notifica
notifications.SENTTIME	Ora generata dal servizio che ha inoltrato la notifica
notifications.HEADLINE	Breve descrizione del testo della notifica
notifications.DESCRPTION	Descrizione dettagliata del testo della notifica
notifications.ALERTLINK	Elenco di avvisi CAP relativi alla notifica
notifications.KPILINK	KPI correlato alla notifica

#### Concetti correlati:

“Notifiche” a pagina 287

Utilizzare il portlet Notifiche per visualizzare i messaggi di avviso ed i relativi dettagli.

### Impostazioni portlet Report

Personalizzare il portlet Report modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

#### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 57. I valori del parametro di personalizzazione del portlet Report

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	ReportsIntegrationPortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	600
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	800
Titolo del portlet	Titolo del portlet Report.	Report personalizzato

Tabella 57. I valori del parametro di personalizzazione del portlet Report (Continua)

URL report	Specifica l'URL del report visualizzato.	http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false
Raggruppamento di risorse	Ubicazione del bundle delle risorse fornito come origine per il valore delle proprietà, ad esempio, titolo portlet. Questa ubicazione è necessaria se si desidera specificare il titolo come chiave proprietà nel bundle delle risorse fornito. Se non è specificato alcun bundle di risorse, la chiave non viene esaminata e il titolo viene visualizzato come mostrato nel campo Titolo del portlet della finestra <b>Impostazioni condivise</b> .	Non esiste alcun raggruppamento di risorse predefinito.
Mostra campo URL nella pagina	Selezionare <b>True</b> per includere il pulsante <b>URL report</b> nella pagina del portlet Report. Questo pulsante consente a tutti gli utenti, non solo agli amministratori, di creare un report personalizzato e di impostare l'URL del report. Selezionare <b>False</b> per escludere il pulsante <b>URL report</b> dalla pagina del portlet Report.	False

#### Concetti correlati:

“Report” a pagina 288

Utilizzare il portlet Report per visualizzare un report di eventi come grafico. Il portlet fornisce diverse opzioni in base alle quali raggruppare gli eventi, ed è possibile scegliere gli eventi in base a una data o intervallo di date particolare. I report in questione consentono di pianificare gli eventi correnti e futuri.

### Impostazioni portlet Publisher di esempio

Personalizzare il portlet Publisher di esempio modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

### I parametri di personalizzazione

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Publisher di esempio. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 58. Parametri di personalizzazione del portlet Publisher di esempio

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	SamplePublisherPortletHelp

Tabella 58. Parametri di personalizzazione del portlet Publisher di esempio (Continua)

Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Publisher di esempio.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.

**Concetti correlati:**

“Publisher di esempio” a pagina 103

Utilizzare il portlet Publisher di esempio per pubblicare gli eventi CAP (Common Alerting Protocol) su IBM Intelligent Operations Center.

**Impostazioni portlet SOP (Standard Operating Procedure)**

Personalizzare il portlet SOP (Standard Operating Procedure) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

**I parametri di personalizzazione**

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet SOP (Standard Operating Procedure). I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 59. Parametri di personalizzazione del portlet SOP (Standard Operating Procedure)

Parametro	Descrizione	Valore predefinito
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	SOPManagerPortletHelp
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	440

**Concetti correlati:**

“SOP (Standard Operating Procedure)” a pagina 127

È possibile definire procedure operative standard e le attività per la gestione degli eventi inseriti in IBM Intelligent Operations Center. Utilizzare il portlet SOP (Standard Operating Procedure) per accedere alle applicazioni procedura operativa standard, matrice di selezione procedura operativa standard e designer flusso di lavoro in Tivoli Service Request Manager.

**Impostazioni portlet Stato**

Personalizzare il portlet Stato modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

**I parametri di personalizzazione**

I campi della finestra **Impostazioni condivise** contengono i valori dei parametri di personalizzazione per il portlet Stato. I parametri di personalizzazione vengono descritti nella seguente tabella.

Tabella 60. Parametri di personalizzazione del portlet Stato

Parametro	Descrizione	Valore predefinito
-----------	-------------	--------------------

Tabella 60. Parametri di personalizzazione del portlet Stato (Continua)

Colori KPI personalizzati	Colori da utilizzare nel portlet per indicare lo stato dei KPI, ad esempio, è possibile immettere: {"acceptable": "#7f7f7f", "take_action": "#34333"}  I colori che si immettono qui sovrascrivono i colori forniti dalla soluzione.	{ }
JSP predefinito della guida	Nome del file della guida JSP da mostrare quando si seleziona la guida dal menu del portlet.	KpiStatusPortletHelp
Abilita filtro KPI	Impostazione di true o false per abilitare o disabilitare un filtro KPI aggiuntivo per il portlet in base alle informazioni contenute nel valore del parametro <b>filtro KPI</b> .	false
Filtro KPI	ID dei KPI da visualizzare quando 'Abilita filtro KPI' è impostato su per il portlet, ad esempio: ["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]	[ ]
Identificativo del gruppo portlet	Nome del gruppo a cui appartiene questo portlet. Un nome comune configura la comunicazione tra i portlet Drill Down KPI (Key Performance Indicator) e Stato sulla stessa pagina.	default
Altezza portlet	Numero di pixel che indica l'altezza standard del portlet.	200
Altezza massima del portlet	Numero di pixel che indica l'altezza massima del portlet.	600
Titolo del portlet	Titolo che sostituisce il titolo fornito con la soluzione.	Se non si immette un valore per questo parametro, il titolo fornito dalla soluzione e visualizzato è: Stato.
Raggruppamento di risorse	Ubicazione del raggruppamento di risorse fornito dall'utente come origine del valore delle proprietà, ad esempio, il titolo del portlet. Tale ubicazione è obbligatoria se si desidera specificare il titolo come chiave di proprietà in un raggruppamento di risorse fornito dall'utente. Se non viene specificato alcun raggruppamento di risorse, la chiave non viene ricercata ed il titolo viene visualizzato come fornito dalla soluzione.	Non esiste alcun raggruppamento di risorse predefinito.
Mostra legenda	Impostazione true o false per nascondere o visualizzare la legenda nel portlet.	true
Ordine di priorità	La proprietà KPI in base alla quale l'elenco di KPI viene ordinato. L'impostazione predefinita è ordinare in ordine alfabetico crescente in base al nome KPI. Altre opzioni sono kpi.CURRENT.VALUE, kpi.CURRENT.STATUS e kpi.CALCULATION.TIME	+kpi.NAME

#### Concetti correlati:

“Stato” a pagina 291

Utilizzare il portlet Stato per visualizzare lo stato degli indicatori KPI (key Performance Indicator) per una singola organizzazione o per più organizzazioni.

## Personalizzazione della guida del portlet

È possibile distribuire la guida alternativa per un portlet IBM Intelligent Operations Center.

## Informazioni su questa attività

Per un ausilio nell'utilizzo di ciascun portlet, fare clic nell'angolo superiore destro del portlet e selezionare **Guida** dal menu visualizzato.

Se si modifica il layout o i dati visualizzati in un portlet, è possibile che si voglia cambiare anche la visualizzazione della guida.

### Procedura

1. Creare la guida alternativa come un file JSP.
2. È possibile assegnare al file qualsiasi nome si desidera, ma è necessario utilizzare il suffisso corretto per la propria lingua. L'impostazione della lingua è basata sulla lingua del proprio browser. Utilizzare l'identificativo locale standard per la propria lingua, ad esempio:

Opzione	Descrizione
<code>_pt_BR</code>	Portoghese (Brasile)
<code>_en</code>	Inglese
<code>_fr</code>	Francese
<code>_de</code>	Tedesco
<code>_es</code>	Spagnolo

3. Utilizzare la finestra **Impostazioni condivise** del portlet per impostare il parametro **DefaultHelpJSP** con il nome file della guida alternativo. Non includere il suffisso della lingua o l'estensione file .jsp.
4. Copiare il file JSP della guida alternativa nell'ubicazione corretta: `/opt/IBM/WebSphere/wp_profile/installedApps/cell1/ioc_portal_ear.ear/portlet_war/portlet_root/jsp/html/help`. I valori per ogni portlet delle variabili `portlet_war` e `portlet_root` sono elencati in un argomento separato. Consultare il link alla fine di questo argomento per un elenco di questi valori.

**Nota:** Quando si modifica il file della guida di Riepilogo autorizzazioni utente, sostituire `ioc_portal_ear.ear` con `iss_portal_ear.ear` nel percorso fornito in questo passo.

### Operazioni successive

Fornire le traduzioni del file della guida alternativo in tutte le lingue supportate, inclusa una lingua predefinita.

**Informazioni correlate:**

 Documentazione del prodotto IBM WebSphere Portal 7

### Ubicazioni dei file della guida del portlet

Valori delle ubicazioni sono richiesti per ciascun portlet quando si sostituisce la guida del portlet predefinito con il proprio file JSP della guida alternativo.

Tabella 1 e 2 forniscono i valori per il percorso dei file della guida del portlet dell'utente e di gestione.

Tabella 61. Valori del portlet utente per l'ubicazione di un file della guida alternativo

Portlet	<code>portlet_war</code>	<code>portlet_root</code>
Dettagli	<code>icoc_ui_common_events_portlet.war</code>	<code>_icoc_ui_common_events_portlet</code>
Drill Down KPI (Key Performance Indicator)	<code>icoc_ui_kpi_drilldown_portlet.war</code>	<code>_icoc_ui_kpi_drilldown_portlet</code>
Mappa ubicazioni	<code>icoc_ui_location_map_portlet.war</code>	<code>_icoc_ui_location_map_portlet</code>

Tabella 61. Valori del portlet utente per l'ubicazione di un file della guida alternativo (Continua)

Portlet	portlet_war	portlet_root
Mappa	icoc_ui_navigator_portlet.war	_icoc_ui_navigator_portlet
Attività personali	icoc_ui_activities_portlet.war	_icoc_ui_activities_portlet
Notifiche	icoc_ui_city_coordinator_portlet.war	_icoc_ui_city_coordinator_portlet
Report	icoc_ui_reports_portlet.war	_icoc_ui_reports_portlet
Stato	icoc_ui_kpi_status_portlet.war	_icoc_ui_kpi_status_portlet

Tabella 62. Valori del portlet di amministrazione per l'ubicazione di un file della guida alternativo

Portlet	portlet_war	portlet_root
Console di gestione	icoc_ui_administration_console_portlet.war	_icoc_ui_administration_console_portlet
Programmazione script di eventi	icoc_ui_event_scripting_portlet.war	_icoc_ui_event_scripting_portlet
KPI (Key Performance Indicators)	icoc_ui_kpi_manager_portlet.war	_icoc_ui_kpi_manager_portlet
Gestore mappa ubicazioni	icoc_ui_location_map_manager_portlet.war	_icoc_ui_location_map_manager_portlet
Publisher di esempio	icoc_ui_sample_publisher_portlet.war	_icoc_ui_sample_publisher_portlet
SOP (Standard Operating Procedure)	icoc_ui_sop_manager_portlet.war	_icoc_ui_sop_manager_portlet
Riepilogo autorizzazioni utente	iss_ui_security_portlet.war	_iss_ui_security_portlet

## Personalizzazione dei KPI

In IBM Intelligent Operations Center è possibile personalizzare i modelli KPI (Key Performance Indicator) per adattarlo ai processi business.

I KPI sono progettati per fornire dati statistici che possono essere utilizzati per analizzare gli andamenti o per indicare aree problematiche. I dati KPI vengono aggiornati da eventi all'interno di IBM Intelligent Operations Center.

IBM Intelligent Operations Center fornisce una serie di KPI di esempio e gli eventi che possono essere utilizzati per aggiornare lo stato del KPI. Ci sono tre modelli KPI di esempio forniti con IBM Intelligent Operations Center basati sulla sicurezza pubblica di esempio, sul trasporto e il monitoraggio dell'acqua e sui processi business. Per ulteriori informazioni sui KPI di esempio forniti con IBM Intelligent Operations Center, seguire il link alla fine dell'argomento.

Ogni soluzione IBM Intelligent Operations Center segue un processo di creazione e integrazione del KPI per impostare i KPI richiesti per l'ambiente di business specifico. È possibile creare i propri modelli KPI con IBM WebSphere Business Monitor. Per ulteriori informazioni sulla creazione e integrazione dei KPI con IBM Intelligent Operations Center, seguire il link alla fine dell'argomento.

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI in IBM Intelligent Operations Center. Il portlet KPI (Key Performance Indicators) viene fornito per l'amministratore come una delle opzioni **Soluzione strumenti di personalizzazione**.

Utilizzando il portlet, è possibile visualizzare le proprietà KPI; creare, copiare o modificare i KPI e visualizzare o modificare le visualizzazioni gerarchiche dei modelli KPI.

Utilizzare la scheda **Definizione KPI** per definire i KPI associati a un modello KPI specifico in IBM Intelligent Operations Center:

- Visualizzare l'elenco corrente dei KPI appartenenti a un modello KPI.
- Visualizzare le proprietà di un KPI esistente.
- Aggiornare le proprietà di un KPI esistente.
- Creare un nuovo KPI per un modello KPI:
  - Aggregare il KPI calcolato utilizzando una metrica definita
  - Valore del KPI di espressione basato su altri KPI
- Eliminare un KPI.

Gli aggiornamenti vengono salvati nei modelli IBM WebSphere Business Monitor memorizzati nel database IBM Intelligent Operations Center. Gli aggiornamenti vengono riportati anche nel successivo aggiornamento dei portlet Stato e Drill Down KPI (Key Performance Indicator).

Utilizzare la scheda **Gerarchia di visualizzazione dei KPI** per aggiornare le gerarchie KPI visualizzate nei portlet Stato e Drill Down KPI (Key Performance Indicator).

- Visualizzare le gerarchie KPI esistenti.
- Visualizzare le proprietà principali di un KPI.
- Modificare la struttura ad albero per lo spostamento o la rimozione di elementi in una gerarchia KPI.
- Aggiunta di KPI predefiniti in una gerarchia.

Gli aggiornamenti vengono riportati nel successivo aggiornamento dei portlet Stato e Drill Down KPI (Key Performance Indicator).

**Nota:** Qualsiasi aggiornamento alla gerarchia di visualizzazione è indipendente dal modello KPI e la conoscenza del modello KPI è necessaria per garantire che gli aggiornamenti siano conformi alla logica del modello KPI.

#### **Concetti correlati:**

“Creazione ed integrazione dei KPI” a pagina 109

I modelli KPI (Key performance indicator) possono essere creati e modificati utilizzando un toolkit di sviluppo del monitoraggio di business e un portlet di gestione KPI.

“KPI di esempio” a pagina 121

Con IBM Intelligent Operations Center vengono forniti KPI di esempio. I KPI di esempio sono progettati per fornire una guida per l'implementazione di tipi diversi di KPI utilizzando il toolkit di sviluppo di IBM WebSphere Business Monitor. Modelli di monitoraggio di esempio vengono forniti nel campo idrico, dei trasporti e della sicurezza pubblica.

## **KPI (Key Performance Indicators)**

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

Nel portlet KPI (Key Performance Indicators) è possibile visualizzare, modificare, copiare, creare ed eliminare KPI. È possibile anche personalizzare le gerarchie di KPI nei portlet Stato e Drill Down KPI (Key Performance Indicator).

Per accedere al portlet KPI (Key Performance Indicators), nell'interfaccia di gestione WebSphere Portal fare clic su **Intelligent Operations > Strumenti di personalizzazione > KPI (Key Performance Indicator)**.

### **Visualizzazione di gerarchie KPI**

Utilizzare la scheda **Relazioni e visualizzazione** per visualizzare i modelli KPI così come vengono visualizzati nei portlet Stato e Drill Down KPI (Key Performance Indicator).



## Informazioni su questa attività

Sulla sinistra della finestra **Relazioni e visualizzazione**, vengono elencati i nodi di livello root delle gerarchie KPI che l'utente è autorizzato a visualizzare. Questi nodi rappresentano i modelli KPI così come vengono visualizzati nei portlet Stato e Drill Down KPI (Key Performance Indicator)

### Procedura

1. Espandere il nodo a livello root per visualizzare i livelli inferiori della struttura ad albero del modello che si desidera visualizzare.
2. Fare clic sul titolo del nodo di livello root per visualizzare l'anteprima dei dettagli sulla destra della finestra. Le informazioni vengono visualizzate come descritto nella seguente tabella.

Opzione	Descrizione
Nome	titolo del nodo a livello root
Tipo	tipo di nodo a livello root
ID modello	identificativo per il corrispondente modello KPI
Categoria	classificazione del modello
Icona	l'icona che rappresenta il nodo a livello root

3. Fare clic sul KPI per visualizzare l'anteprima dei dettagli sul lato destro della finestra **Relazioni e visualizzazione**.

### Modifica una gerarchia di KPI

Utilizzare la scheda **Relazioni e visualizzazione** per modificare o rimuovere un modello KPI così come è visualizzato nei portlet Stato e Drill Down KPI (Key Performance Indicator).

### Procedura

1. Sul lato sinistro della finestra **Relazioni e visualizzazione**, fare clic sul nodo del livello root e sugli elementi secondari per espandere la struttura ad albero gerarchica per il livello che si desidera.
2. È possibile spostare, aggiungere, modificare o rimuovere gli elementi esistenti come segue:
  - Per spostare gli elementi secondari all'interno di una struttura ad albero, trascinare l'elemento nella posizione richiesta. Indicatori di colore verde o rosso indicano se è consentito o meno lo spostamento.
  - Per aggiungere in una struttura ad albero dall'elenco di elementi secondari esistenti per un modello KPI, fare clic con il tasto destro del mouse sull'elemento che contiene l'elemento secondario e fare clic su **Aggiungi KPI**.
  - Per passare alla finestra **Proprietà KPI** e modificare un elemento secondario, fare clic con il tasto destro del mouse sull'elemento e fare clic su **Modifica**.
  - Per rimuovere un nodo di livello root o un elemento secondario da una struttura ad albero, fare clic con il tasto destro del mouse sull'elemento e fare clic su **Rimuovi**. La rimozione di un elemento del nodo root rimuove tutti gli elementi secondari che contiene.
3. Fare clic su **Salva** per salvare gli aggiornamenti.

**Nota:** Non è possibile qui modificare il nome di un'organizzazione proprietaria o un nodo di livello root. Se si desidera modificare un'organizzazione proprietaria, rimuoverla e sostituirla con un altro nome.

### Aggiunta di un'organizzazione proprietaria

Utilizzare la scheda **Relazioni e visualizzazione** per aggiungere un nodo di livello root da visualizzare nei portlet Stato e Drill Down KPI (Key Performance Indicator).

## Procedura

1. In alto a sinistra della finestra **Relazioni e visualizzazione**, fare clic su **Aggiungi organizzazione proprietaria**
2. Immettere un nome di visualizzazione.
3. Dall'elenco a discesa del campo **Modello**, selezionare il nodo di livello root da aggiungere.
4. Dall'elenco a discesa del campo **Categoria**, selezionare una categoria per il nodo di livello root.
5. Dall'elenco a discesa del campo **Icona**, selezionare il nome file per l'icona che rappresenta il nodo di livello root.
6. Fare clic su **OK** per aggiungere il nuovo nodo sul lato sinistro della finestra **Relazioni e visualizzazione**.
7. Fare clic su **Salva** per aggiornare la visualizzazione nei portlet Stato e Drill Down KPI (Key Performance Indicator)

## Modifica legenda KPI

Utilizzare la scheda **Relazioni e visualizzazione** per modificare la legenda KPI sul portlet Stato.

## Procedura

1. In alto a sinistra della finestra **Relazioni e visualizzazione**, fare clic su **Legenda KPI**.
2. Modificare la visualizzazione per la legenda KPI nel modo seguente:
  - Per aggiungere un intervallo, fare clic su **Aggiungi riga**.
  - Per modificare un intervallo, modificare i campi in **Nome intervallo**, **Colore**, **Icona**.
  - Per eliminare un intervallo, fare clic **Elimina**.
3. Fare clic su **OK** per aggiornare la visualizzazione nei portlet Stato e Drill Down KPI (Key Performance Indicator).

## Visualizzazione di un modello KPI

Utilizzare la scheda **Definizione KPI** per visualizzare i KPI appartenenti ai modelli KPI all'interno di IBM Intelligent Operations Center.

## Procedura

Il campo **Filtra per modello** contiene un elenco a discesa dei modelli dei processi di business che l'utente è autorizzato a visualizzare. Selezionare tutti i modelli per cui si desidera visualizzare i KPI. Le informazioni KPI vengono visualizzate come descritto nella seguente tabella.

Opzione	Descrizione
Nome KPI	Titolo del KPI. È possibile selezionare il nome KPI per visualizzare le proprietà.
Modello	Nome del modello a cui appartiene il KPI.
Creato	Metodo di creazione del KPI: <ul style="list-style-type: none"><li>• Un KPI modellato è un KPI creato a livello di modello utilizzando IBM WebSphere Business Monitor.</li><li>• Un KPI dashboard è un KPI creato utilizzando il portlet KPI (Key Performance Indicators)</li></ul>
Tipo	Tipo di KPI: <ul style="list-style-type: none"><li>• Un KPI aggregato ha un valore basato sulla metrica e sul metodo di aggregazione selezionato.</li><li>• Un KPI espressione ha un valore basato sugli altri KPI o sulla funzioni definite dall'utente utilizzando l'espressione XPath definita.</li></ul>

Opzione	Descrizione
Accesso	<p>Livello di accesso di un KPI:</p> <ul style="list-style-type: none"> <li>• Un KPI condiviso è un KPI che altri utenti hanno accesso a visualizzare.</li> <li>• Un KPI privato è un KPI che non è possibile condividere con utenti diversi dal proprietario.</li> </ul>

## Visualizzazione o modifica di un KPI

Utilizzare la scheda **Definizione KPI** per visualizzare o modificare un KPI esistente appartenente ad un modello in IBM Intelligent Operations Center.

### Procedura

1. Selezionare un KPI. In alto a sinistra della finestra **Definizione KPI**, fare clic su **Modifica**. Viene visualizzata la finestra **Proprietà KPI**.
2. Per modificare il KPI, modificare i campi nelle schede della finestra delle proprietà. Per ulteriori dettagli relativi alle modifiche di tali campi per creare un KPI aggregato o espressione, fare clic sul link alla fine di questa sezione.

**Nota:** Non è possibile qui modificare la definizione di un KPI modellato.

3. Per salvare e uscire dalla finestra **Proprietà KPI** aggiornata, fare clic su **OK**. Per salvare e continuare a modificare il KPI copiato, fare clic su **Applica**. Per uscire senza salvare, fare clic su **Annulla**.

## Copia di un KPI

Utilizzare la scheda **Definizione KPI** per effettuare una copia di un KPI esistente per un modello in IBM Intelligent Operations Center.

### Procedura

1. Selezionare un KPI. In alto a sinistra della finestra **Definizione KPI**, fare clic su **Altre azioni > Copia**. Viene visualizzata la finestra **Proprietà KPI**.
2. Immettere un nuovo nome KPI nel campo **Nome KPI**.
3. Modificare le proprietà del KPI copiato seguendo i passi 3 e 4 della procedura di modifica di un KPI.

## Creazione di un KPI

Utilizzare la scheda **Definizione KPI** per creare un KPI per un modello in IBM Intelligent Operations Center.

### Procedura

1. In alto a sinistra della finestra **Definizione KPI**, fare clic su **Crea**.
2. Fare clic su **Nuovo KPI aggregato** o **Nuovo KPI espressione**. Viene visualizzata la finestra **Proprietà KPI**.
3. Modificare le proprietà del nuovo KPI seguendo i passi 3 e 4 della procedura di modifica di un KPI.

## Operazioni successive

Per ulteriori informazioni sulla creazione dei KPI, accedere al link della documentazione di IBM Websphere Business Monitor alla fine dell'argomento.

## KPI di esempio

Viene fornito un insieme di KPI di esempio con la soluzione. I KPI in questione sono realizzati per fornire una guida alla pianificazione e all'implementazione dei diversi tipi di KPI ed essere adatti alla propria organizzazione. Sono forniti esempi in campo idrico, trasporti e sicurezza pubblica.

## Personalizzazione del portlet KPI (Key Performance Indicators)

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

### Concetti correlati:

“Stato” a pagina 291

Utilizzare il portlet Stato per visualizzare lo stato degli indicatori KPI (key Performance Indicator) per una singola organizzazione o per più organizzazioni.

“Drill Down KPI (Key Performance Indicator)” a pagina 275

Utilizzare il portlet Drill Down KPI (Key Performance Indicator) per visualizzare ulteriori informazioni su una categoria KPI, lo stato dei KPI sottostanti.

### Riferimenti correlati:

“Impostazioni portlet KPI (Key Performance Indicators)” a pagina 155

Personalizzare il portlet KPI (Key Performance Indicators) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

### Informazioni correlate:

 Centro informazioni di IBM WebSphere Business Process Management versione 7.0

## Backup prima della personalizzazione KPI

Backup e ripristino KPI che sono stati creati o modificati con IBM WebSphere Business Monitor o con il portlet KPI (Key Performance Indicators).

### Informazioni su questa attività

Prima di personalizzare i modelli KPI e modificare i KPI, si potrebbe desiderare di eseguire il backup dei modelli esistenti. La procedura contenuta in questo argomento esporta tutti i KPI dal modello specificato nel file specificato ed importa i KPI dal file specificato nel modello specificato.

### Procedura

1. Collegarsi a server delle applicazioni.
2. Passare al profilo bin directory of the IBM WebSphere Business Monitor: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin`
3. Per esportare i KPI, eseguire il comando: `./wsadmin.sh -wsadmin_classpath "../..../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../..../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../..../scripts/wbm/kpi/exportKpis.jy" "xml_file_path" model_ID model_version ALL`  
*xml\_file\_path* è il nome e il percorso del file XML in cui si stanno esportando i KPI. *model\_ID* *model\_version* sono l'ID e la versione del modello KPI da cui si stanno esportando i KPI.
4. Per importare i KPI, eseguire il comando: `./wsadmin.sh -wsadmin_classpath "../..../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../..../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../..../scripts/wbm/kpi/importKpis.jy" "xml_file_path"`  
*xml\_file\_path* è il nome e il percorso del file XML da cui si stanno importando i KPI.

### Esempio

Per esportare tutti i KPI dal modello, `icoc_sample_public_safety_monitor_model` a `/tmp/kpis.xml`, eseguire il seguente comando. Nel comando, il valore di *xml\_file\_path* è `/tmp/kpis.xml`, il valore di *model\_ID* è `icoc_sample_public_safety_monitor_model` e il valore di *model\_version* è `2011-02-18T10:49:46`.

```
./wsadmin.sh -wsadmin_classpath ".././../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:  
.././../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f ".././../scripts.wbm  
/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model  
2011-02-18T10:49:46 ALL
```

Per ulteriori informazioni, consultare il link del centro informazioni di WebSphere Business Monitor, alla fine dell'argomento.

#### Riferimenti correlati:

“Esecuzione backup dei dati” a pagina 259

Per evitare la perdita di dati importanti in IBM Intelligent Operations Center, eseguire, ad intervalli regolari, il backup di alcuni file, directory e database.

#### Informazioni correlate:



IBM Smarter Cities Software Solutions Redbooks

---

## Personalizzazione degli eventi correlati

Questa sezione illustra la correlazione eventi e descrive come modificare e creare nuove tabelle decisionali. Inoltre descrive l'applicazione delle regole.

### Correlazione di eventi e applicazione delle regole

Questo argomento fornisce una panoramica del processo di correlazione eventi e descrive brevemente l'applicazione delle regole.

La correlazione di eventi basata sull'applicazione delle regole in WebSphere Operational Decision Management consente di modificare e di estendere le regole di correlazione senza conoscenza tecnica avanzata di IBM Intelligent Operations Center or WebSphere Operational Decision Management. Tuttavia, è necessaria la conoscenza di base degli eventi CAP (Common Alerting Protocol) e di WebSphere Operational Decision Management.

Le variabili che determinano il modo in cui gli eventi sono correlati sono tre: l'evento di origine, l'evento di destinazione e la tabella decisionale.

Per ciascun evento CAP (Common Alerting Protocol) in entrata, l'applicazione delle regole viene richiamata per determinare se qualcuno degli eventi esistenti è correlato all'evento in entrata. L'evento di origine è sempre il nuovo evento in entrata e attiva la correlazione. Il processo di correlazione verifica l'evento di origine rispetto agli eventi nel database. Quando un evento viene trovato nel database che lo correla all'evento di origine, questo evento viene chiamato l'evento di destinazione. Ogni volta che viene trovata un'eventuale correlazione, il portlet Notifiche invia un avviso.

La determinazione è unidirezionale. Questo concetto è importante perché le regole che determinano la correlazione non devono essere simmetriche. Ad esempio, se l'evento A è correlato all'evento B, non significa che l'evento B è correlato ad un evento A.

L'applicazione delle regole fornisce una tabella di correlazione di esempio che soddisfa la maggior parte dei requisiti. Fare riferimento a “Personalizzazione delle impostazioni di correlazione eventi” per i diversi modi di personalizzare le regole correlate.

## Personalizzazione delle impostazioni di correlazione eventi

In questa sezione viene spiegato come personalizzare le impostazioni della correlazione eventi.

La tabella decisionale, che può essere modificata nel Decision Center, ha due tipi di colonne. Le colonne a sinistra vengono chiamate colonne decisione. Esse determinano quale colonna azione, sulla destra,

utilizzare. Le tabelle decisionali vengono contrassegnate da sinistra a destra e, secondo i valori delle differenti righe, conducono ad una colonna azione sulla destra. La colonna azione definisce ciò che viene eseguito quando viene raggiunta una riga specifica.

Il modo consigliato per espandere e modificare le impostazioni di correlazione eventi è quello di modificare una tabella decisionale esistente. I seguenti elementi descrivono come vengono formattate le tabelle decisionali:

- Sul lato sinistro della tabella decisionale (sfondo bianco) ci sono le colonne decisionali. Queste determinano quali delle righe nelle colonne delle azioni (sfondo grigio) vengono eseguite.
- L'ultima colonna azione nella tabella richiama il servizio di query e pubblicazione. Se c'è una riga di azione che non si desidera come pubblicazione e query di correlazione, disattivare la voce in questa ultima colonna.
- La colonna SQL Query impostata nelle colonne azione può sostituire i parametri della query. La sostituzione dei parametri di query è complessa e non necessaria per la maggior parte delle applicazioni. Il requisito per questa query è che vi siano tre colonne denominate nel risultato della query:
  - event\_headline - Il titolo da utilizzare nella descrizione della correlazione. Questo testo diventa la descrizione della notifica.
  - event\_external\_id - L'id esterno dell'evento, come ad esempio CAP-ID
  - event\_internal\_id - L'id interno, come CapAlertId, per essere utilizzato dal portlet Notifiche da associare ai titoli nel campo **Riferimenti agli avvisi** delle proprietà di notifica.

Questa sezione contiene i seguenti argomenti:

## **Modifica delle proprietà della decisione**

Utilizzare l'interfaccia utente di Decision Center in WebSphere Operational Decision Management per modificare le impostazioni di correlazione eventi. Questa sezione fornisce ulteriori informazioni sulla modifica delle proprietà della decisione nelle tabelle decisionali. Fornisce anche un link alla documentazione WebSphere Operational Decision Management.

## **Informazioni su questa attività**

L'interfaccia utente è ubicata sul nodo 1 dell'installazione di server portale a questo URL:  
[http://app\\_server:9084/teamserver](http://app_server:9084/teamserver). Collegarsi come waswebadmin.

La maggior parte delle modifiche apportate possono essere eseguite all'interno dell'applicazione delle regole come descritto in "Modifica della tabella decisionale" a pagina 175. Altre modifiche potrebbero coinvolgere delle modifiche a quanto segue:

- Le politiche Tivoli Netcool/Impact
- Il nodo di calcolo WebSphere Message Broker Java che trasforma i messaggi derivanti dalle politiche di impatto nel formato bean guidato del messaggio
- XOM (Executable Object Model) di query e BOM (Business Object Model)

Per ulteriori informazioni ed istruzioni sulla modifica di XOM e BOM, per informazioni sul nodo broker del messaggio ed informazioni sul centro decisionale, fare riferimento ai centri informazione di WebSphere Operational Decision Management e WebSphere Message Broker utilizzando i link di seguito indicati.

## Informazioni correlate:

 Centro informazioni di IBM WebSphere Operational Decision Management

 Documentazione di WebSphere Message Broker

## Modifica della tabella decisionale

Questo argomento fornisce una breve spiegazione della tabella decisionale e fornisce i passaggi per modificare le proprietà della stessa.

Nell'applicazione della regola IBM Intelligent Operations Center WebSphere Operational Decision Management, esiste una tabella definita della correlazione di base che utilizza la categoria ed il tipo dell'evento per determinare quale riga di azione eseguire.

Al momento, le righe di azione sono identiche ma possono essere modificate per essere adattate alle proprie esigenze. Ad esempio, è possibile definire che gli eventi incendio vengano trattati in modo diverso da altri eventi e correlarli solo con acqua e altri eventi incendio. Per modificare i valori in modo da adattarli alle proprie esigenze, attivare la cella della colonna Categorie per la riga e immettere "incendi, acqua" nella cella. Se si vuole la regola per distinguere tra Eventi e Incidenti, aggiungere una riga a questa colonna decisionale e la colonna delle azioni.

Per modificare il raggio della ricerca di eventi correlati, modificare il valore **Imposta il raggio di ricerca**. Il valore intero immesso viene interpretato come metri dal centro dell'evento di origine. Pertanto, se si immette 2000, si correla solo con gli eventi che sono a meno di 2000 metri di distanza dall'evento di origine.

## Modifica delle proprietà della tabella decisionale

### Procedura

1. Collegarsi a [http://app\\_server:9084/teamserver](http://app_server:9084/teamserver) come rtsadmin.
2. Andare nel proprio browser.
3. Fare clic su **capCorrelationRules**.
4. Fare clic su **simpleCorrelationPolicy**.
5. Fare clic su **Modifica**. Viene visualizzata la pagina delle proprietà.
6. Fare clic su **Avanti** nella pagina delle proprietà.
7. Modificare la tabella. Per esempi di colonne da aggiungere alla tabella decisionale, consultare il modello fornito nella cartella dei modelli.
8. Quando si termina di apportare modifiche alla tabella, fare clic su **Fine**.

## Operazioni successive

Esportare l'applicazione delle regole dal centro decisionale utilizzando il relativo collegamento riportato di seguito.

### Attività correlate:

“Distribuzione della serie di regole modificate nel flusso IBM Intelligent Operations Center”

Utilizzare questo argomento per distribuire la serie di regole modificate sul server di esecuzione della regola.

## Distribuzione della serie di regole modificate nel flusso IBM Intelligent Operations Center

Utilizzare questo argomento per distribuire la serie di regole modificate sul server di esecuzione della regola.



## Informazioni su questa attività

Quando si modifica una qualunque proprietà o elemento nella tabella decisionale, bisogna distribuire l'insieme di regole modificate nel flusso in IBM Intelligent Operations Center. Dopo aver distribuito la serie di regole modificate sul server di esecuzione della regola, le regole di correlazione funzionano in modo diverso in base alle modifiche. Il server di esecuzione regola controlla le correlazioni possibili per gli eventi in entrata.

Per distribuire la serie di regole modificate, completare la seguente procedura.

### Procedura

- Esportare l'applicazione delle regole dal centro decisionale:
  - Andare su `app_server:9084/teamservice/`.
  - Collegarsi come `rtsadmin`.
  - Navigare su **Progetto > Genera RuleSet**.
  - Fare clic su **Avanti**, non selezionare nulla e scaricare il file RuleApp jar.
- Importare l'applicazione delle regole nel server di esecuzione della regola:
  - Andare su `app_server:9083/res`.
  - Fare clic sulla scheda Esplora.
  - Fare clic su **icoc\_wodm\_correlation\_ruleApp > Aggiungi Ruleset**.
  - Denominare la serie di regole e prendere nota del percorso della nuova serie di regole:  
`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`.  
Dove
    - `yourChosenName` è il nome scelto per la serie di regole
    - `version` è la versione della serie di regole
- Impostare il nuovo percorso della serie di regole nella politica di impatto:
  - Andare su `event_server:9080/nci/login_main.jsp`.
  - Dal menu a discesa sulla sinistra, selezionare IBM Intelligent Operations Center.
  - Fare clic su **Politiche** e selezionare la politica **IOC\_Event\_Correlation**.
  - Modificare il valore del campo: **JMSProps.ilog\_rules\_bres\_mdb\_rulesetPath** nel nuovo percorso:  
`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`.  
Dove
    - `yourChosenName` è il nome scelto per la serie di regole
    - `version` è la versione della serie di regole
  - Fare clic su **Salva**.

#### Attività correlate:

“Modifica delle proprietà della tabella decisionale” a pagina 175

---

## Gestore mappa ubicazioni

Utilizzare il portlet Gestore mappa ubicazioni per personalizzare il portlet Mappa ubicazioni.

È possibile personalizzare i seguenti aspetti del portlet Mappa ubicazioni:

- Nome classificazione da visualizzare sul menu alla sinistra del portlet.
- La mappa che deve essere visualizzata nel portlet.
- Aree all'interno di una mappa.

Le aree all'interno di una mappa sono identificate da un codice identificativo area. Qualsiasi evento con un codice identificativo area viene visualizzato in tutte le mappe ubicazioni con tale area definita.

Esiste anche la possibilità di fornire un identificativo principale dell'area. È possibile utilizzare l'identificativo principale per creare una gerarchia dell'area. Ad esempio, creare delle aree per rappresentare i posti a sedere al primo piano di uno stadio sportivo. Ogni posto a sedere viene definito nella mappa ubicazioni di dettaglio del primo piano dello stadio. Inoltre, assegnare a ciascun posto a sedere un identificativo principale per indicare che è al primo piano dello stadio. Un evento con un identificativo area per uno dei posti a sedere viene visualizzato nella mappa di dettaglio dei posti a sedere del primo piano. Questo evento viene visualizzato anche nella mappa generale dello stadio perché il primo piano in questa mappa ha lo stesso identificativo area utilizzato come identificativo principale per i posti a sedere.

Per accedere al portlet Gestore mappa ubicazioni, nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > Gestore mappa ubicazioni**.

## Aggiunta di una classificazione al menu mappa

Utilizzare la scheda **Classificazioni** per aggiungere una classificazione da visualizzare nel menu mappa del portlet Mappa ubicazioni

### Procedura

1. Immettere un nome nel campo **Nome classificazione**. È possibile aggiungere una descrizione.
2. Per aggiungere la classificazione al portlet, fare clic su **Inoltre**.

### Risultati

La nuova classificazione viene visualizzata nel portlet Mappa ubicazioni quando si aggiorna la pagina del portlet.

## Aggiunta di una mappa al portlet

Utilizzare la scheda **Mappe ubicazioni** per aggiungere una mappa ubicazioni da visualizzare nel portlet Mappa ubicazioni.

### Procedura

1. Immettere un nome nel campo **Nome classificazione**. È possibile effettuare una scelta dall'elenco a discesa.
2. Immettere un nome della mappa ubicazioni nel campo **Nome mappa**. Si ha la possibilità di aggiungere una descrizione della mappa.
3. Immettere un URL per la mappa ubicazioni nel campo **Immagine**.
4. Per aggiungere la mappa al menu, fare clic su **Inoltre**.

### Risultati

La mappa viene visualizzata nel menu del portlet Mappa ubicazioni quando si aggiorna la pagina del portlet. È possibile selezionare e visualizzare la mappa.

## Aggiunta o modifica delle aree in un mappa ubicazioni

Utilizzare la scheda **Aree** per creare nuove aree, modificare aree o rimuovere aree per la visualizzazione nella mappa ubicazioni sul portlet Mappa ubicazioni.

### Procedura

1. Immettere un nome mappa nel campo **Nome mappa**. È possibile effettuare una scelta dall'elenco a discesa delle mappe.

2. Per tracciare una nuova area nella mappa, fare clic sul simbolo di poligono nell'angolo in alto a destra della casella. Fare clic sulla posizione richiesta nella mappa e quindi fare clic su ogni angolo per disegnare un poligono. Fare doppio clic per terminare il poligono. Per impostazione predefinita le nuove aree vengono visualizzate in colore verde.
3. Per immettere i dettagli per un'area, fare clic sul simbolo della mano nell'angolo in alto a destra della casella. Fare clic su un'area da aggiornare.
4. Immettere un nome della mappa area nel campo **Nome area**. È possibile aggiungere una descrizione.
5. Immettere un identificativo area nel campo **Identificativo area**. L'utente ha la possibilità di aggiungere un identificativo area principale.
6. Per aggiornare un'area nella mappa, fare clic su **Aggiorna area**. Per rimuovere un'area dalla mappa, fare clic su **Rimuovi area**.
7. Per aggiungere le modifiche alla mappa, fare clic su **Inoltra**.

## Risultati

Le modifiche vengono visualizzate nel portlet Mappa ubicazioni quando si aggiorna la pagina del portlet.

## Personalizzazione del portlet Gestore mappa ubicazioni

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

### Concetti correlati:

“Mappa ubicazioni” a pagina 276

Utilizzare il portlet Mappa ubicazioni per visualizzare gli eventi contrassegnati sulla mappa ubicazioni. Una mappa ubicazioni in IBM Intelligent Operations Center è una mappa o piano con aree predefinite per l'interazione, ad esempio, i posti a sedere di un principale stadio sportivo.

### Riferimenti correlati:

“Impostazioni portlet Gestore mappa ubicazioni” a pagina 156

Personalizzare il portlet Gestore mappa ubicazioni modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

---

## Specifica dei dati di configurazione del sistema

La tabella delle proprietà del sistema IBM Intelligent Operations Center memorizza i dati di configurazione IBM Intelligent Operations Center.

Le seguenti proprietà sono proprietà di sistema utilizzate da IBM Intelligent Operations Center.

*Tabella 63. Valori di sistema utilizzati da IBM Intelligent Operations Center*

Area di autenticazione	Oggetto	Nome	Tipo	Valore
Sistema	*	ActivityCollectionRefreshInterval	Numero intero	La frequenza di aggiornamento di raccolta sul server espressa in secondi. Il valore predefinito è 300 (5 minuti). Questa proprietà influisce sulla velocità di servizio UI di aggiornamento per le attività.

Tabella 63. Valori di sistema utilizzati da IBM Intelligent Operations Center (Continua)

Area di autenticazione	Oggetto	Nome	Tipo	Valore
Sistema	*	ActivityProviderEJBNDIName	Stringa	Il nome bind JNDI dell'interfaccia remota del provider dell'attività. Tramite questa interfaccia, è possibile distribuire il proprio provider attività da utilizzare con il proprio processo o sistema di gestione del flusso di lavoro. Il provider attività è un EJB che implementa l'interfaccia attività in iss_common.jar.
Sistema	*	AppMonitorPort	Stringa	La porta web utilizzata da Tivoli Monitoring.
Sistema	*	ApplicationServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da server delle applicazioni.
Sistema	*	CollectionRefreshInterval	Numero intero	La frequenza di aggiornamento di raccolta sul server espressa in secondi. Il valore predefinito è di 15 secondi. Questa proprietà influisce sulla velocità di servizio UI di aggiornamento per eventi e notifiche.
Sistema	*	DatabaseServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da server di dati.
Sistema	*	DateFormat	Stringa	Il formato utilizzato quando IBM Intelligent Operations Center visualizza la data. Il valore predefinito è yyyy-MM-dd. Può essere specificato qualsiasi modello data Java <code>java.text.SimpleDateFormat</code> .
Sistema	*	DateTimeFormat	Stringa	Il formato utilizzato quando IBM Intelligent Operations Center visualizza la data e l'ora. Il valore predefinito è yyyy-MM-dd HH:mm:ss. Può essere specificato qualsiasi modello data e ora Java <code>java.text.SimpleDateFormat</code> valido.
Sistema	*	DisableTSRMSync	Booleano	Specifica se la sincronizzazione Tivoli Service Request Manager è disabilitata. Il valore predefinito è di false. Impostare su true se una distribuzione non contiene l'installazione di Tivoli Service Request Manager.
Sistema	*	EventContainerDeleteEvent	Stringa	<p>Specifica se un evento viene eliminato dal database Object Server di Tivoli Netcool/OMNIBus. L'eliminazione viene implementata dalla politica Tivoli Netcool/Impact quando il database IBM Intelligent Operations Center viene aggiornato con un evento. Il valore predefinito è true.</p> <p>Se il valore è true, l'evento viene eliminato dal database Object Server.</p> <p>Se il valore è false, l'evento non viene eliminato dal database Object Server.</p>

Tabella 63. Valori di sistema utilizzati da IBM Intelligent Operations Center (Continua)

Area di autenticazione	Oggetto	Nome	Tipo	Valore
Sistema	*	EventRouterPollDelay	Numero intero	Il ritardo espresso in millisecondi tra gli intervalli di polling UI. Il ritardo è il numero di millisecondi prima del successivo intervallo di polling. Il valore predefinito è 0.
Sistema	*	EventRouterPollErrorDelay	Numero intero	Il ritardo in millisecondi tra gli intervalli di polling UI dopo che si è verificato un errore. Il ritardo è il numero di millisecondi dopo un errore e prima del successivo intervallo di polling. Il valore predefinito è 5000.
Sistema	*	EventRouterTimeout	Numero intero	L'intervallo di polling UI in secondi. L'intervallo di polling è l'intervallo di tempo in cui eseguire il polling degli eventi prima del timeout. Il valore predefinito è 20.
Sistema	*	EventServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da server eventi.
Sistema	*	MgmtServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da server di gestione.
Sistema	*	ModelManagerServerEJBPort	Stringa	La porta EJB utilizzata da servizi di modelli semantici.
Sistema	*	ModelManagerServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da servizi di modelli semantici.
Sistema	*	MonitorServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da IBM WebSphere Business Monitor.
Sistema	*	MonitorServerWebPort	Stringa	La porta web utilizzata dal Gateway dei servizi REST di IBM WebSphere Business Monitor.
Sistema	*	MonitorServerSecurityEnabled	Booleano	Specifica se la connessione a IBM WebSphere Business Monitor utilizza SSL per una connessione HTTP protetta. Il valore predefinito è true.  Se il valore è true, la connessione utilizza SSL.  Se il valore è false, la connessione non utilizza SSL.
Sistema	*	PortalServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da WebSphere Portal Server.
Sistema	*	PortalServerWebPort	Stringa	La porta web utilizzata da WebSphere Portal Server.
Sistema	*	RegExpEmail	Sistema	L'espressione regolare utilizzata per convalidare un indirizzo di posta elettronica. Il valore predefinito è .+.
Sistema	*	RegExpTelephone	Sistema	L'espressione regolare utilizzata per convalidare un numero di telefono. Il valore predefinito è .+.

Tabella 63. Valori di sistema utilizzati da IBM Intelligent Operations Center (Continua)

Area di autenticazione	Oggetto	Nome	Tipo	Valore
Sistema	*	SecurityUserPrefix	Stringa	Il prefisso dell'ID utente utilizzato per associare l'utente al nome distinto LDAP. Il valore predefinito è uid.
Sistema	*	SecurityUserSuffix	Stringa	Il suffisso ID utente utilizzato per associare l'utente a un nome distinto LDAP o un nome distinto locale. Il valore predefinito, utilizzato durante l'esecuzione di un portale con sicurezza LDAP, è ou=users,ou=SWG,o=IBM,c=US. Impostare il valore su o=defaultWIMFileBasedRealm durante l'esecuzione di un portale locale senza la sicurezza LDAP.
Sistema	*	TdsPort	Stringa	La porta web utilizzata da Tivoli Directory Server Web Administration Tool
Sistema	*	TimeFormat	Stringa	Il formato utilizzato quando IBM Intelligent Operations Center visualizza la data e l'ora. Il valore predefinito è HH:mm:ss. Può essere specificato qualsiasi modello data Java <code>java.text.SimpleDateFormat</code> .
Sistema	*	TSRMDirectServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da Tivoli Service Request Manager.
Sistema	*	TSRMDirectServerWebPort	Stringa	La porta web utilizzata da Tivoli Service Request Manager.
Sistema	*	TSRMServerActivityUri	Stringa	L'attività e l'URI dell'applicazione attività utilizzati da Tivoli Service Request Manager. Il valore predefinito è <code>/tsrm/maximo/ui/maximo?event=loadapp&amp;value=Activity&amp;uniqueid={0}</code> . Il valore ID attività viene sostituito per {0}.
Sistema	*	TSRMServerResourceAddUri		L'URI della risorsa di aggiunta utilizzato da Tivoli Service Request Manager. Il valore predefinito è <code>/tsrm/maximo/ui/maximo?event=loadapp&amp;value=plusires&amp;additional=event=INSERT</code> . Il valore ID risorsa esterna viene sostituito per {0}.
Sistema	*	TSRMServerResourceDeleteUri		L'URI della risorsa di eliminazione utilizzato da Tivoli Service Request Manager. Il valore predefinito è <code>/tsrm/maximo/ui/maximo?event=loadapp&amp;value=plusires&amp;additional=event=useqbe&amp;additional=eventvalue=LOCATION={0}</code> . Il valore ID risorsa esterna viene sostituito per {0}.
Sistema	*	TSRMServerResourcePropertiesUri		L'URI delle proprietà della risorsa utilizzato da Tivoli Service Request Manager. Il valore predefinito è <code>/tsrm/maximo/ui/maximo?event=loadapp&amp;value=plusires&amp;additional=event=useqbe&amp;additional=eventvalue=LOCATION={0}</code> . Il valore ID risorsa esterna viene sostituito per {0}.

Tabella 63. Valori di sistema utilizzati da IBM Intelligent Operations Center (Continua)

Area di autenticazione	Oggetto	Nome	Tipo	Valore
Sistema	*	TSRMServerResourceUpdateUri		L'URI della risorsa di aggiornamento utilizzato da Tivoli Service Request Manager. Il valore predefinito è /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0}. Il valore ID risorsa esterna viene sostituito per {0}.
Sistema	*	TSRMServerSecurityEnabled	Booleano	Specifica se la connessione HTTP a Tivoli Service Request Manager serve per utilizzare SSL. Il valore predefinito è false.  Se il valore è true, la connessione utilizza SSL  Se il valore è false, la connessione non utilizza SSL.
Sistema	*	TSRMServerWorkflowUri	Stringa	L'URI del flusso di lavoro utilizzato da Tivoli Service Request Manager. Il valore predefinito è /maximo/ui/?event=loadapp&value=sr&additional=event=useqbe&additional=eventvalue=TICKETID={0}. Il valore di ID incidente viene sostituito per {0}.
Sistema	*	UseDBModelReader	Booleano	Specifica se il modello del database KPI viene letto da un file RDF. Il valore predefinito è true.  Se il valore è true, il modello di KPI non viene letto da un file RDF.  Se il valore è false, il modello di KPI viene letto da un file RDF.
Sistema	*	WebSEALServerHostname	Stringa	Il nome host o l'indirizzo IP utilizzato da Tivoli Access Manager WebSEAL.

Le seguenti proprietà possono essere modificate per configurare il modo in cui vengono elaborati i KPI.

Tabella 64. Proprietà che influenzano l'elaborazione KPI

Area di autenticazione	Oggetto	Nome	Tipo	Valore
KPI	*	CacheKpis	Booleano	Specifica se i KPI richiamati da IBM WebSphere Business Monitor vengono memorizzate nella cache. Il valore predefinito è true.  Se il valore è true, i KPI vengono memorizzati nella cache per il riutilizzo. La frequenza con cui la cache viene aggiornata è specificata da KpiCacheRefreshInterval.  Se il valore è false, i KPI vengono richiamati sempre da IBM WebSphere Business Monitor quando IBM Intelligent Operations Center richiede informazioni KPI.



Tabella 64. Proprietà che influenzano l'elaborazione KPI (Continua)

Area di autenticazione	Oggetto	Nome	Tipo	Valore
KPI	*	KpiCacheRefreshInterval	Numero intero	Specifica la frequenza con cui viene aggiornata la cache KPI. L'intervallo viene specificato in secondi. Il valore predefinito è 300 (5 minuti). KpiCacheRefreshInterval viene ignorato se CacheKpis viene specificato come false.
KPI	*	KpiSentToGroup	Stringa	Specifica i gruppi che ricevono notifiche KPI. Separare i nomi di gruppo con un punto e virgola (;). Il valore predefinito è CityWideExecutive;CityWideSupervisor.
KPI	*	PreLoadKpis	Booleano	<p>Specifica se i KPI vengono richiamati da IBM WebSphere Business Monitor quando viene avviato IBM Intelligent Operations Center. Il valore predefinito è true.</p> <p>Se true, tutti i KPI vengono richiamati da IBM WebSphere Business Monitor quando viene avviato IBM Intelligent Operations Center. I KPI vengono memorizzati nella cache per essere riutilizzati. KpiCacheRefreshInterval specifica la frequenza con cui viene aggiornata la cache.</p> <p>Se il valore è false, i KPI vengono richiamati da IBM WebSphere Business Monitor solo quando IBM Intelligent Operations Center richiede informazioni KPI.</p> <p><b>Nota:</b> Se PreLoadKpis è true, allora si suppone che CacheKpis sia true indipendentemente dal valore specificato.</p>

## Aggiornamento della tabella delle proprietà del sistema

Per modificare i dati di configurazione IBM Intelligent Operations Center di sistema, aggiornare la tabella delle proprietà di sistema.

### Informazioni su questa attività

Utilizzare un client VNC per collegarsi al server del database server di dati ed aprire una finestra comandi. Nella seguente procedura, immettere i comandi nella finestra dei comandi.

### Procedura

- Collegarsi a server di dati come root
- Per aprire DB2<sup>®</sup> Control Center, disattivare temporaneamente il controllo di accesso e immettere i comandi:
 

```
xhost +
su - db2inst1
db2cc
```
- Nel DB2 Control Center, aprire la tabella delle proprietà di sistema:
  - Per aprire DB2 Control Center, immettere il seguente comando: - db2cc
  - In DB2 Control Center, fare clic su **Tutti i database > IOCDB > Tabelle > SYSPROP.**
  - Fare clic con il tasto destro sulla tabella **SYSPROP** poi fare clic su **Apri.**
  - Modificare il campo richiesto e fare clic su **Commit**
  - Chiudere la tabella.
- Chiudere DB2 Control Center.
- Per tornare all'utente root, immettere il comando: **esci.**
- Per attivare di nuovo il controllo accessi, immettere il comando: **xhost -**

**Nota:** Per implementare le modifiche apportate, è necessario riavviare il server del portale. È possibile riavviare il server del portale con lo script IOCCControl. Per informazioni relative all'avvio dei servizi, consultare il collegamento alla fine di questo argomento.

#### Attività correlate:

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

---

## Configurazione di IBM Cognos Business Intelligence per la creazione di report

IBM Intelligent Operations Center fornisce un sottosistema di creazione report che utilizza IBM Cognos Business Intelligence per creare e gestire i report. IBM Intelligent Operations Center viene fornito con una pagina di report che può visualizzare fino a sei report. È anche possibile creare una pagina di report manualmente e personalizzare il layout del portlet.

Il sottosistema di creazione report è installato su server delle applicazioni ed utilizza modello di dati analitici.

### Creazione di un portlet Report

Utilizzare le informazioni presenti in questo argomento per creare una pagina del portlet Report copiando un portlet esistente utilizzando la console di IBM Intelligent Operations Center.

#### Informazioni su questa attività

Per copiare un portlet esistente ed impostare le proprietà per creare una nuova pagina report, completare i passi di seguito riportati.

#### Procedura

1. Collegarsi a IBM Intelligent Operations Center come amministratore.
2. Navigare su **Amministrazione > Gestione portlet > Portlet**.
3. Nel campo **Ricerca**, immettere Report e fare clic su **Ricerca**. Viene visualizzata la finestra del portlet report.
4. Accanto al portlet che si desidera copiare, fare clic sull'icona **Copia portlet**. Viene visualizzata la finestra della copia del portlet.
5. Per il nome del nuovo portlet, immettere CognosReport.
6. Fare clic su **OK**. Nella finestra Gestione portlet, viene visualizzato il nuovo portlet.
7. Navigare su **Amministrazione > Interfaccia utente del portale > Gestione pagine**.
8. Fare clic su **Root del contenuto > Intera città** e fare clic sulla scheda **Nuova pagina**. Viene visualizzata la pagina Proprietà pagina.
9. Immettere le seguenti proprietà per la nuova pagina del report:
  - a. Nel campo **Titolo**, immettere un titolo per la pagina del report. Un titolo di esempio è Operatore: Report.
  - b. Nel campo **Nome univoco**, immettere un nome che identifichi in modo specifico questa pagina del report. Un esempio di nome univoco è com.ibm.iss.ioc.citywide.OperatorReports.
  - c. Nel campo **Nome URL amico**, immettere report.
  - d. Nel campo **Tema**, accettare il valore predefinito **Eredita tema principale**.
  - e. Nel campo **Stile tema**, accettare il valore predefinito **Eredita politica del tema principale**.
  - f. In **Aggregazione- Modalità di rendering**, selezionare **Eredita modalità di rendering principale**.
  - g. Fare clic su **OK**.

La pagina del nuovo report viene aggiunta all'elenco delle pagine del portlet.

## Modifica del layout del portlet Report

Utilizzare queste operazioni per formattare il layout del portlet Report

### Informazioni su questa attività

Per selezionare il layout della pagina del portlet Report utilizzando la console IBM Intelligent Operations Center, completare le seguenti operazioni.

### Procedura

1. Accedere a IBM Intelligent Operations Center come amministratore.
2. Andare a **Amministrazione > Interfaccia utente portale > Gestisci pagine** .
3. Accanto alla pagina che si desidera modificare, fare clic sull'icona **Modifica layout pagina**. Viene visualizzata la pagina Modifica layout pagina.
4. Selezionare l'icona di layout che ha pagine affiancate con una riga al di sotto delle pagine. Questa icona è la quinta icona a partire da sinistra.
5. Nel frame in cui si desidera aggiungere il portlet, fare clic su **Aggiungi portlet**.
6. Cercare e selezionare la casella di spunta **CognosPortlet** e fare clic su **OK** per aggiungere il portlet al layout di pagina. Viene visualizzato un messaggio che conferma che il portlet è stato aggiunto.
7. Ripetere i passi 5 e 6 per aggiungere altri portlet. È possibile aggiungere fino a sei portlet.
8. Fare clic su **Eseguito**.

### Operazioni successive

È possibile modificare le impostazioni condivise per ciascun portlet. Nell'angolo superiore destro del portlet che si desidera modificare, fare clic sulla freccia e selezionare **Modifica impostazioni condivise** dal menu. Per ulteriori informazioni, consultare "Personalizzazione di un portlet per la visualizzazione di report".

## Personalizzazione di un portlet per la visualizzazione di report

Utilizzare le informazioni presenti in questo argomento per personalizzare un portlet IBM Intelligent Operations Center in modo che vengano visualizzati report IBM Cognos Business Intelligence.

### Procedura

1. Collegarsi al portale delle soluzioni come amministratore.
2. Selezionare la vista e il portlet che si desidera personalizzare per visualizzare i report.
3. Passare al menu di visualizzazione del portlet nell'angolo in alto a destra del portlet.
4. Fare clic su **Modifica impostazioni condivise**.
5. Immettere le impostazioni nei campi forniti.
  - a. Specifica un titolo per il report.
  - b. Immettere l'**URL** per il report. Individuare l'URL richiesto come descritto nell'argomento "Individuazione degli URL del report" a pagina 186.  
  
Esempio: CAP\_events\_by\_type\_status\_and\_date:  
`http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_mode1%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_date%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=true`
  - c. Impostare il portale **Larghezza** su *600*.
  - d. Impostare il portale **Larghezza** su *600*.

- e. Fare clic su **Salva**.
- f. Sul menu di visualizzazione del portlet, fare clic su **Indietro** per tornare alla vista principale del portlet.

## Risultati

Il portlet dei report viene aggiornato, visualizzando il report selezionato di recente.

## Individuazione degli URL del report

Questo argomento fornisce i passi per trovare l'URL di un report.

### Procedura

1. Accedere a IBM Cognos Connection.
2. Navigare su **Cartelle pubbliche > ioc\_model > report**.
3. Selezionare un report e fare clic sull'icona **Imposta proprietà**.
4. Nella scheda **Generale**, fare clic su **Visualizza il percorso di ricerca, ID e URL** per visualizzare l'URL del report.
5. Dalla sezione **URL azione predefinita**, copiare l'URL ed incollarlo nel portlet come richiesto.

## Come lavorare con il modello di dati

IBM Intelligent Operations Center fornisce due modelli di dati che vengono utilizzati durante la generazione di report. Un metamodello definisce la lingua e i processi da cui formare un modello.

I report in IBM Intelligent Operations Center vengono costruiti su due modelli di dati.

- Modello dati Schema comune
- Modello dati Schema CAP (Common Alerting Protocol)

Entrambi i modelli di dati IBM Intelligent Operations Center sono organizzati come livelli. Per gli autori di report, la vista o il livello di presentazione è reso disponibile e comprende i seguenti spazi nomi:

### Business

Contiene i dizionari, i filtri e i dati.

### Dimensionale

Contiene le dimensioni di eventi per i report e l'analisi.

### Query personalizzata

Contiene argomenti di interrogazioni che è possibile utilizzare per creare query personalizzate per report relazionali.

## Generazione di report di modelli di dati di schemi comuni

Questo argomento descrive in che modo generare i report di modelli di dati di schemi comuni. Tali report consentono ai gestori e ai supervisori di monitorare gli eventi correnti, agire agli eventi che si verificano e pianificare eventi futuri.

## Informazioni su questa attività

Mediante l'utilizzo della console IBM Intelligent Operations Center, completare le seguenti operazioni per generare i report di modelli di dati di schemi comuni. Consultare i link di riferimento alla fine di questo argomento per una descrizione delle opzioni per la generazione di un report.

## Procedura

1. Nella scheda Amministrazione della console IBM Intelligent Operations Center, fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**. Viene visualizzata la pagina Console di gestione.
2. In Server delle applicazioni, fare clic su **Gestione report**. Viene visualizzata la pagina IBM Cognos Connection.
3. Fare clic su **ioc common model**. Vengono visualizzate le cartelle pubbliche Cognos.
4. Fare clic su **Report**.
5. Selezionare il tipo di report che si desidera generare:
  - Per generare un report del grafico a torta, fare clic su **Grafici a torta**. Vengono visualizzati i report dei grafici a torta di schemi comuni.
  - Per generare un report di grafici tabella, fare clic su **Grafici tabella**. Vengono visualizzati i report dei grafici tabella di schemi comuni.
6. Selezionare il report che si desidera generare.

### Opzioni del grafico a torta:

Questo argomento fornisce le opzioni che possono essere selezionate per i report dei grafici a torta comuni.

Per accedere ai report dei grafici a torta dalla pagina di IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_common\_model > report > Grafici a torta**.

Tabella 65. Opzioni del grafico a torta per i report di modelli di dati di schemi comuni

Report	Descrizione
Evento per categoria	Visualizza gli eventi in base alla categoria eventi. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Evento per certezza	Visualizza gli eventi in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Evento per data inviata	Questo report mostra gli eventi che sono stati inviati in una data particolare.
Evento per tipo di evento	Visualizza gli eventi in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Evento per titolo	Visualizza gli eventi mediante la descrizione immessa per l'evento quando tale evento è stato creato. Pertanto, il titolo è effettivamente la descrizione dell'evento.
Evento per gravità	Visualizza gli eventi in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Evento per specifica	Visualizza gli eventi per specifica. Ad esempio, un evento può essere un evento CAP (Common Alerting Protocol) o non CAP (Common Alerting Protocol). Quindi, questo grafico mostra la percentuale di eventi CAP (Common Alerting Protocol) e non CAP (Common Alerting Protocol).
Evento per urgenza	Visualizza gli eventi in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Evento per URL	Visualizza gli eventi mediante l'URL immesso per l'evento quando tale evento è stato creato.

## Opzioni di grafici tabella:

Questo argomento descrive le informazioni che possono essere generate per i report di grafici tabella comuni.

Per accedere ai report dei grafici tabella dalla pagina di IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_common\_model > report > Grafici tabella**.

L'unica opzione del grafico tabella per report di modelli di dati di schemi comuni è Elenco eventi. Tale opzione fornisce un elenco completo di eventi con informazioni dettagliate per ciascun evento. Alcuni esempi di informazioni sull'elenco eventi sono descritti di seguito.

*Tabella 66. Informazioni sull'elenco eventi per grafici tabella comuni*

Campo report	Descrizione
ID	Identifica il report
ID evento esterno	L'ID evento generato quando l'evento è stato creato.
Specifica	Specifica se l'evento è un evento CAP (Common Alerting Protocol) o non CAP (Common Alerting Protocol).
Tipo evento	Visualizza gli eventi in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Inviato	La data e l'ora in cui l'evento è stato inviato.
Titolo	La descrizione dell'evento.
Categoria	Visualizza gli eventi in base alla categoria eventi. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Certezza	Visualizza gli eventi in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Gravità	Visualizza gli eventi in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Urgenza	Visualizza gli eventi in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Url	L'URL associato al report.

## Generazione di report di modelli di dati di schemi CAP (Common Alerting Protocol)

Questo argomento descrive in che modo generare i report di modelli di dati di schemi CAP (Common Alerting Protocol). Tali report consentono ai gestori e ai supervisori di monitorare gli eventi correnti, agire agli eventi che si verificano e pianificare eventi futuri.

### Informazioni su questa attività

Mediante l'utilizzo della console IBM Intelligent Operations Center, completare le seguenti operazioni per generare i report di modelli di dati di schemi CAP (Common Alerting Protocol). Consultare i link di riferimento alla fine di questo argomento per una descrizione delle opzioni per la generazione di un report.

## Procedura

1. Nella scheda Amministrazione della console IBM Intelligent Operations Center, fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**. Viene visualizzata la pagina Console di gestione.
2. In Server delle applicazioni, fare clic su **Gestione report**. Viene visualizzata la pagina IBM Cognos Connection.
3. Fare clic su **ioc cap model**. Vengono visualizzate le cartelle pubbliche Cognos.
4. Fare clic su **Report**.
5. Selezionare il tipo di report che si desidera generare:
  - Per generare un report di modello di dati riportato in questa pagina, selezionare il report.
  - Per generare un report del grafico a torta, fare clic su **Grafici a torta**. Vengono visualizzati i report dei grafici a torta di schemi comuni. Selezionare il report dall'elenco.
  - Per generare un report definito dall'utente, fare clic su **Report definiti dall'utente**. Viene visualizzata la pagina Report personalizzato Cognos. Completare i campi per il report personalizzato e fare clic su **Aggiorna**.

## Opzioni dei report di modelli di dati:

Questo argomento descrive le opzioni che possono essere selezionate per la generazione di un report CAP (Common Alerting Protocol).

Per accedere a queste opzioni del report dalla pagina IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_cap\_model > report**.

Tabella 67. Opzioni per informazioni sui report CAP (Common Alerting Protocol)

Report	Descrizione
Eventi CAP (Common Alerting Protocol) per tipo, stato e data	Questo report mostra gli eventi CAP (Common Alerting Protocol) per tipo, stato e data dell'evento. Ad esempio, il tipo di evento potrebbe essere un incidente e lo stato urgente. La data potrebbe essere quella odierna.
Metriche KPI di eventi CAP (Common Alerting Protocol) per data	Questo report mostra gli eventi CAP (Common Alerting Protocol) basati sulle metriche KPI per una particolare data o intervallo di date.
Metriche KPI di eventi CAP (Common Alerting Protocol) per reparto	Questo report mostra gli eventi CAP (Common Alerting Protocol) basati sulle metriche KPI per un particolare dipartimento o area. Ad esempio, il report potrebbe mostrare le metriche KPI relative al dipartimento idrico oppure a una particolare area di un città.
Dettagli completi di CAP (Common Alerting Protocol)	Questo report mostra i dettagli completi relativi ad eventi CAP (Common Alerting Protocol). Ad esempio, i dettagli includono l'ID CAP (Common Alerting Protocol), il mittente, la data e l'ora di invio, lo stato, il tipo di messaggio, l'origine ed altro.
Eventi IBM Intelligent Operations Center per gravità in qualunque momento	Questo report elenca tutti gli eventi IBM Intelligent Operations Center in base alla loro gravità. Ad esempio, gli eventi possono essere estremi.
Eventi IBM Intelligent Operations Center per gravità in corso	Questo report elenca tutti gli eventi IBM Intelligent Operations Center che si sono attualmente verificati per gravità. Ad esempio, la gravità in corso potrebbe essere identificata dalle cattive condizioni meteorologiche.



## Opzioni del grafico a torta:

Questo argomento descrive le opzioni disponibili per la generazione di report di grafici a torta CAP (Common Alerting Protocol).

Per accedere ai report dei grafici a torta dalla pagina di IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_cap\_model > report > Grafici a torta**.

Tabella 68. Opzioni per informazioni sui report dei grafici a torta CAP (Common Alerting Protocol)

Report	Descrizione
Cap per categoria	Visualizza CAP (Common Alerting Protocol) in base a una particolare categoria. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Cap per certezza	Visualizza gli eventi CAP (Common Alerting Protocol) in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Cap per data inviata	Visualizza gli eventi CAP (Common Alerting Protocol) inviati in una data particolare.
Cap per tipo di evento	Visualizza gli eventi CAP (Common Alerting Protocol) in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Cap per codice di gestione	Visualizza gli eventi CAP (Common Alerting Protocol) in base al codice di gestione. Ad esempio, il codice di gestione potrebbe essere "evento".
Cap per tipo di messaggio	Visualizza gli eventi CAP (Common Alerting Protocol) in base ai tipi di messaggi, ad esempio aggiornamenti e avvisi.
Cap per ambito	Visualizza gli eventi CAP (Common Alerting Protocol) in base all'ambito. Ad esempio, un evento per ambito potrebbe essere "pubblico."
Cap per mittente	Visualizza gli eventi CAP (Common Alerting Protocol) in base al nome del mittente.
Cap per gravità	Visualizza gli eventi CAP (Common Alerting Protocol) in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Cap per origine	Visualizza CAP (Common Alerting Protocol) in base a una particolare origine. Ad esempio, l'origine potrebbe essere il trasporto.
Cap per stato	Visualizza gli eventi CAP (Common Alerting Protocol) in base allo stato. I livelli di stato sono: <ul style="list-style-type: none"><li>• Accettabile</li><li>• Attenzione</li><li>• Esegui azione</li></ul>
Cap per urgenza	Visualizza gli eventi CAP (Common Alerting Protocol) in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Notifica per categoria	Visualizza i messaggi di avviso in formato CAP (Common Alerting Protocol) in base a una particolare categoria. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.

Tabella 68. Opzioni per informazioni sui report dei grafici a torta CAP (Common Alerting Protocol) (Continua)

Report	Descrizione
Notifica per tipo	Visualizza le notifiche in formato CAP (Common Alerting Protocol) in base al tipo. Ad esempio, il tipo potrebbe essere identificato da aggiornamenti e avvisi.

### Opzioni dei report di eventi definiti dall'utente:

Questo argomento descrive le opzioni disponibili per la generazione di report definiti dall'utente CAP (Common Alerting Protocol) di eventi.

Per accedere ai report definiti dall'utente dalla pagina di IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_cap\_model > report > Report definiti dall'utente > Eventi**.

Tabella 69. Opzioni di eventi CAP (Common Alerting Protocol)

Report	Descrizione
Eventi per categoria in qualunque momento	Visualizza tutti gli eventi per categoria indipendentemente dalla data. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Eventi per certezza in qualunque momento	Visualizza tutti gli eventi per certezza indipendentemente dalla data. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Eventi per tipo di evento in qualunque momento	Visualizza tutti gli eventi per tipo di evento indipendentemente dalla data. Ad esempio, gli eventi potrebbero essere l'arrivo di un tornado o un incidente stradale che si è verificato in qualsiasi data.
Eventi per gravità in qualunque momento	Visualizza tutti gli eventi per gravità indipendentemente dalla data. Ad esempio, vengono visualizzati gli eventi estremi o gravi per qualsiasi data.
Eventi per urgenza in qualunque momento	Visualizza tutti gli eventi per urgenza indipendentemente dalla data. Ad esempio, gli eventi potrebbero verificarsi ed essere descritti come "immediati."

### Opzioni del report personalizzato definito dall'utente:

Questo argomento descrive le opzioni disponibili per la generazione di report personalizzati definiti dall'utente CAP (Common Alerting Protocol).

È possibile creare un report personalizzato per eventi utilizzando il portlet Report. Innanzitutto, selezionare il modo in cui si desidera raggruppare gli eventi. Ad esempio, per visualizzare tutti gli eventi di una particolare categoria, selezionare **Categoria** nel campo **Raggruppa per**. Quindi, nei campi **Selezione dati**, scegliere i dati specifici per le informazioni che si desidera visualizzare. È possibile inoltre indicare una data o un intervallo di date per gli eventi presenti nel report. Fare clic su **Aggiorna** e il grafico cambia per riflettere le informazioni richieste.

Per richiamare l'URL per il nuovo report, fare clic su **URL per questo report**.

Per accedere ai report personalizzati definiti dall'utente dalla pagina di IBM Cognos Connection, fare clic su **Cartelle pubbliche > ioc\_cap\_model > report > Report definiti dall'utente > Report definito dall'utente**.

Tabella 70. Opzioni personalizzate definite dall'utente CAP (Common Alerting Protocol)

Report	Descrizione
Raggruppa per	Selezionare l'opzione per cui si desidera raggruppare gli eventi.
Gravità	Visualizza gli eventi in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Certezza	Visualizza gli eventi in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Urgenza	Visualizza gli eventi in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Categoria eventi	Visualizza gli eventi in base alla categoria eventi. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Tipo evento	Visualizza gli eventi in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Dalla data	Immettere la data per cui si stanno visualizzando gli eventi. Per un intervallo di date, immettere la data di inizio.
Alla data	Immettere la data fino alla quale si stanno visualizzando gli eventi.

## Configurazione di report di modelli di dati di schemi comuni

Utilizzare questo argomento per impostare le proprietà generali e specifiche per i report di modelli di dati di schemi comuni.

### Prima di iniziare

È necessario disporre dell'accesso di amministratore per eseguire questa procedura.

### Informazioni su questa attività

Utilizzare la console IBM Intelligent Operations Center per configurare questi report.

### Procedura

1. Nella scheda Amministrazione della console IBM Intelligent Operations Center, fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**. Viene visualizzata la pagina Console di gestione.
2. In Server delle applicazioni, fare clic su **Gestione report**. Viene visualizzata la pagina IBM Cognos Connection.
3. Selezionare la casella di spunta **ioc common model**, quindi fare clic su **Altro**. Viene visualizzata la pagina Azioni disponibili.
4. Fare clic su **Imposta proprietà**. Viene visualizzata la pagina Proprietà generali.
5. Selezionare i valori per le proprietà generali del report.
6. Nella scheda Autorizzazioni, selezionare le autorizzazioni per i report di modelli di dati di schemi comuni.
7. Nella scheda Funzionalità, selezionare le funzionalità per i report.
8. Fare clic su **OK**.

## Configurazione dei report di modelli di dati dello schema CAP (Common Alerting Protocol)

Utilizzare questo argomento per impostare le proprietà generali, le autorizzazioni e per assegnare le funzionalità ai tipi di utenti per i report di modelli di dati dello schema CAP (Common Alerting Protocol).

### Prima di iniziare

È necessario disporre dell'accesso di amministratore per eseguire questa procedura.

### Informazioni su questa attività

Utilizzare la console IBM Intelligent Operations Center per configurare questi report.

### Procedura

1. Nella scheda Amministrazione della console IBM Intelligent Operations Center, fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**. Viene visualizzata la pagina Console di gestione.
2. In Server delle applicazioni, fare clic su **Gestione report**. Viene visualizzata la pagina IBM Cognos Connection.
3. Selezionare la casella di spunta **ioc cap model**, quindi fare clic su **Altro**. Viene visualizzata la pagina Azioni disponibili.
4. Fare clic su **Imposta proprietà**. Viene visualizzata la pagina Proprietà generali.
5. Selezionare i valori per le proprietà generali del report.
6. Nella scheda Autorizzazioni, selezionare le autorizzazioni per i report di modelli di dati dello schema CAP (Common Alerting Protocol).
7. Nella scheda Funzionalità, selezionare le funzionalità per gli utenti dei report.
8. Fare clic su **OK**.

### Ulteriori opzioni di report

Questo argomento descrive le opzioni di report aggiuntive per i report CAP (Common Alerting Protocol) e per quelli comuni.

Per accedere a queste opzioni, fare clic su **Altro** alla destra del link di un particolare report.

Tabella 71. Ulteriori opzioni disponibili per ciascun report

Opzione	Descrizione
Imposta proprietà	Impostare le proprietà generali per il report scelto.
Visualizza versione di output del report	Scegliere la versione di output da visualizzare facendo clic su un collegamento ipertestuale del formato.
Visualizza autorizzazioni personali	Consente di visualizzare le autorizzazioni di accesso associate a questa voce.
Esegui con opzioni	Selezionare la modalità di esecuzione e ricezione del report. Gli esempi includono HTML e PDF.
Apri con Report Studio	Visualizza il report in un altro browser utilizzando Report Studio.
Apri con Business Insight Advanced	Visualizza il report in un altro browser utilizzando IBM Cognos Business Insight Advanced.
Nuova pianificazione	Pianifica un report in base a vari criteri.
Sposta	Sposta un report in una posizione differente.
Copia	Copia un report da una posizione a un'altra.

Tabella 71. Ulteriori opzioni disponibili per ciascun report (Continua)

<b>Opzione</b>	<b>Descrizione</b>
Crea un collegamento alla voce	Crea un collegamento rapido sul desktop per accedere al report.
Crea una vista report del report	Crea una vista sul proprio desktop per questo report archiviato in una directory locale.
Elimina	Elimina un report visualizzato.

---

## Capitolo 6. Gestione della soluzione

Negli argomenti di questa sezione viene descritto come eseguire le attività di gestione per IBM Intelligent Operations Center.

---

### Informazioni

Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.

Per avviare il portlet Informazioni, nell'interfaccia di gestione WebSphere Portal, fare clic su **Intelligent Operations > Informazioni**.

Il portlet Informazioni fornisce le seguenti informazioni:

- L'ubicazione di tutti i prodotti e componenti software installati
- Il nome e la versione dei prodotti installati
- Il nome e la versione dei componenti installati
- I dettagli di eventuali correzioni applicate

I componenti identificati sono componenti o parti di un prodotto, ad esempio:

- Una parte di un prodotto che dispone di un flusso di servizio o di manutenzione dedicata
- Una parte di un prodotto installabile facoltativamente
- Parti di un prodotto condivise da più prodotti

**Nota:** Le informazioni visualizzate per ciascuna correzione dipendono dal completamento del passo appropriato nelle istruzioni di installazione fornite con quella correzione.

### Personalizzazione del portlet Informazioni

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

#### Attività correlate:

“Verifica dell'installazione” a pagina 52

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

#### Riferimenti correlati:

“Impostazioni portlet Informazioni” a pagina 146

Personalizzare il portlet Informazioni modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

---

### Controllo dei servizi

I servizi IBM Intelligent Operations Center in esecuzione sul server IBM Intelligent Operations Center possono essere controllati e interrogati.

## Avvio dei servizi

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

### Informazioni su questa attività

Il comando **IOControl.sh** deve essere eseguito come utente `ibmadmin`. Se non si è collegati come `ibmadmin`, eseguire il comando `su - ibmadmin` per passare all'utente `ibmadmin`.

**Attenzione:** L'avvio dei singoli servizi deve essere eseguito solo da amministratori esperti di IBM Intelligent Operations Center. Se i servizi non vengono eseguiti in base all'ordine richiesto, potrebbero verificarsi errori imprevedibili.

### Procedura

In server di gestione eseguire il seguente comando per avviare tutti i servizi di IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start all password
```

dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

I servizi vengono avviati nell'ordine richiesto. Tali servizi prerequisiti vengono avviati prima dei servizi dipendenti. Ad esempio, i servizi di database e directory vengono avviati per primi.

Per avviare solo un servizio, eseguire il seguente comando.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start service_ID password
```

dove *service\_ID* è un ID elencato in **Opzioni di destinazione in IOControl** della guida e dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

### Risultati

I servizi IBM Intelligent Operations Center richiesti sono stati avviati.

### Operazioni successive

Dopo aver eseguito il comando **IOControl.sh**, controllare i log nella directory `/opt/IBM/ISP/mgmt/logs`. I file di log contengono i risultati del comando **IOControl.sh**.



### Attività correlate:

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Query dello stato dei servizi” a pagina 202

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

“Come ottenere supporto per Strumento di controllo della piattaforma” a pagina 203

Le informazioni sono disponibili sulle opzioni di azione e destinazione per Strumento di controllo della piattaforma.

“Verifica dell'installazione” a pagina 52

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

“Installazione di Strumento di controllo della piattaforma” a pagina 49

Lo Strumento di controllo della piattaforma viene utilizzato per gestire l'ambiente del server IBM Intelligent Operations Center. Lo strumento è installato separatamente dal prodotto.

“Installazione dello strumento Controllo di verifica del sistema” a pagina 50

Lo strumento Controllo di verifica del sistema viene utilizzato per verificare lo stato operativo dei componenti in IBM Intelligent Operations Center. Lo strumento viene installato separatamente dal prodotto.

### Ordine di avvio obbligatorio

I servizi IBM Intelligent Operations Center services devono essere avviati in base a un ordine specifico.

Strumento di controllo della piattaforma viene utilizzato per avviare i servizi IBM Intelligent Operations Center. Mentre è preferibile che l'opzione Strumento di controllo della piattaforma **avvia tutti** venga utilizzata per avviare tutti i servizi, potrebbero esserci dei casi in cui devono essere avviati i singoli servizi.

Alcuni servizi hanno dipendenze su altri servizi, pertanto i servizi devono essere avviati in base a un ordine specifico.

In generale, i servizi devono essere avviati in tre gruppi:

#### Gruppo 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt

#### Gruppo 2

ihs, appdmgr, st

#### Gruppo 3

tutti i servizi rimanenti

Avviare prima i servizi nel gruppo 1, quindi avviare il gruppo 2 e infine gruppo 3. I servizi all'interno di ciascun gruppo possono essere avviati in qualsiasi ordine.

Tabella 72. Dipendenze dell'ordine di avvio del servizio IBM Intelligent Operations Center

Servizio	Descrizione	I servizi che devono essere avviati prima che questo servizio venga avviato
db24po	DB2 Enterprise Server Edition per WebSphere Portal Server	Nessuno
db24wbm	DB2 Enterprise Server Edition per WebSphere Business Modeler	Nessuno
db24sol	DB2 Enterprise Server Edition per IBM Intelligent Operations Center	Nessuno

Tabella 72. Dipendenze dell'ordine di avvio del servizio IBM Intelligent Operations Center (Continua)

Servizio	Descrizione	I servizi che devono essere avviati prima che questo servizio venga avviato
db24ana	DB2 Enterprise Server Edition per Cognos	Nessuno
db24mgmt	DB2 Enterprise Server Edition per i servizi Tivoli Enterprise Portal	Nessuno
db24tsrm	DB2 Enterprise Server per Tivoli Service Request Manager	Nessuno
db24sms	DB2 Enterprise Server per servizi di modelli semantici	Nessuno
tds	Tivoli Directory Server	Nessuno
tdspxyapp	Tivoli Directory Server Proxy (server delle applicazioni)	tds
tdspxyevt	Tivoli Directory Server Proxy (server eventi)	tds
tdspxymgt	Tivoli Directory Server Proxy (server di gestione)	tds
tdsappsrv	Tivoli Directory Server Application Server	Nessuno
tamps	Tivoli Access Manager Policy Server	tamas
tamas	Tivoli Access Manager Authorization Server	tds
tamwpm	Tivoli Access Manager Web Portal Manager	Nessuno
tamweb	Tivoli Access Manager WebSEAL	tamas
tems	Tivoli Monitoring Enterprise Monitoring Server	Nessuno
teps	Tivoli Monitoring Enterprise Portal Server	tems, db24mgmt
tim	Tivoli Identity Manager	tds
appdmgr	WebSphere Application Server Network Deployment	Nessuno
cplex	WebSphere Application Server per CPLEX	db24sms
ihs	HTTP Server for Runtime (server delle applicazioni)	Nessuno
ihs evt	HTTP Server for Runtime (server eventi)	ihs
ihs mgt	HTTP Server for Runtime (server di gestione)	ihs
ncob	Tivoli Netcool/OMNIBus	Nessuno
nci	Tivoli Netcool/Impact	ncob
wbm	IBM WebSphere Business Monitor	db24wbm
st	Lotus Sametime	Nessuno
stpxy	Lotus Sametime Proxy Application Server	st
wpe	WebSphere Portal Extend	tdspxyapp, db24po, appdmgr
wmb	WebSphere Message Broker	Nessuno
cognos	IBM Cognos Business Intelligence	db24ana, appdmgr
tsrm	Tivoli Service Request Manager	appdmgr, db24tsrm
wodm	WebSphere Operations Decision Manager	appdmgr
wodm dc	WebSphere Operations Decision Manager (Decision Center)	Nessuno
smsclt	Servizi di modelli semantici (Client Services)	appdmgr
smsdaaq	Servizi di modelli semantici (Data Services)	appdmgr
smsmdl	Servizi di modelli semantici (Model Services)	appdmgr
smsgmt	Servizi di modelli semantici (Management Services)	appdmgr
smsrtc	Servizi di modelli semantici (RTC Services)	appdmgr
iocxml	Probe IBM Intelligent Operations Center XML	db24so1

## Avvio e arresto del probe Tivoli Netcool/OMNIBus

Avviare il probe Tivoli Netcool/OMNIBus dopo che tutti i server IBM Intelligent Operations Center sono stati avviati.

### Informazioni su questa attività

Il probe fa parte dello script `IOCControl`. Il probe viene avviato e arrestato quando si desidera avviare ed arrestare Tivoli Netcool/OMNIBus. Il probe Tivoli Netcool/OMNIBus è collegato a Tivoli Netcool/OMNIBus nello script. Utilizzare la seguente procedura per arrestare, avviare e verificare lo stato del probe.

### Procedura

1. Per arrestare il probe, da server di gestione, eseguire:  
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ncob password`
2. Per avviare il probe, da server di gestione, eseguire:  
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ncob password`
3. Per verificare lo stato del probe:
  - In server di gestione, eseguire il comando:  
`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start iocxml password`
  - In server eventi, eseguire il comando:  
`tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`

### Arresto dei servizi

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

### Informazioni su questa attività

Il comando `IOCControl.sh` deve essere eseguito come utente `ibmadmin`. Se non si è collegati come `ibmadmin`, eseguire il comando `su - ibmadmin` per passare all'utente `ibmadmin`.

**Attenzione:** L'arresto dei singoli servizi deve essere eseguito solo da amministratori esperti di IBM Intelligent Operations Center. Se i servizi non vengono arrestati in base all'ordine richiesto, potrebbero verificarsi errori imprevedibili.

### Procedura

In server di gestione eseguire il seguente comando per arrestare tutti i servizi di IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop all password
```

dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

Per arrestare solo un servizio, eseguire il seguente comando.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop service_ID password
```

dove *service\_ID* è un ID elencato in **Opzioni di destinazione** in `IOCControl` della guida e dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

## Risultati

I servizi IBM Intelligent Operations Center richiesti vengono arrestati.

## Operazioni successive

Dopo aver eseguito il comando **IOControl.sh**, controllare i log nella directory `/opt/IBM/ISP/mgmt/logs`. I file di log contengono i risultati del comando **IOControl.sh**.

### Attività correlate:

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Query dello stato dei servizi” a pagina 202

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

“Come ottenere supporto per Strumento di controllo della piattaforma” a pagina 203

Le informazioni sono disponibili sulle opzioni di azione e destinazione per Strumento di controllo della piattaforma.

“Verifica dell'installazione” a pagina 52

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

“Installazione di Strumento di controllo della piattaforma” a pagina 49

Lo Strumento di controllo della piattaforma viene utilizzato per gestire l'ambiente del server IBM Intelligent Operations Center. Lo strumento è installato separatamente dal prodotto.

“Installazione dello strumento Controllo di verifica del sistema” a pagina 50

Lo strumento Controllo di verifica del sistema viene utilizzato per verificare lo stato operativo dei componenti in IBM Intelligent Operations Center. Lo strumento viene installato separatamente dal prodotto.

## Ordine di arresto obbligatorio

I servizi IBM Intelligent Operations Center devono essere arrestati in base a un ordine specifico.

Strumento di controllo della piattaforma viene utilizzato per arrestare i servizi IBM Intelligent Operations Center. Mentre è preferibile che l'opzione Strumento di controllo della piattaforma **arresta tutti** venga utilizzata per arrestare tutti i servizi, potrebbero esserci dei casi in cui devono essere arrestati i singoli servizi.

Alcuni servizi hanno dipendenze su altri servizi, pertanto i servizi devono essere arrestati in base a un ordine specifico.

In generale, i servizi devono essere arrestati in tre gruppi:

### Gruppo 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt

### Gruppo 2

ihs, appdmgr, st

### Gruppo 3

tutti i servizi rimanenti

Arrestare prima i servizi nel gruppo 3, quindi arrestare il gruppo 2 e infine gruppo 1. I servizi all'interno di ciascun gruppo possono essere arrestati in qualsiasi ordine.

Tabella 73. Dipendenze dell'ordine di arresto del servizio IBM Intelligent Operations Center

Servizio	Descrizione	I servizi che devono essere arrestati prima che questo servizio venga arrestato
db24po	DB2 Enterprise Server Edition per WebSphere Portal Server	wpe
db24wbm	DB2 Enterprise Server Edition per WebSphere Business Modeler	wbm
db24sol	DB2 Enterprise Server Edition per IBM Intelligent Operations Center	iocxml
db24ana	DB2 Enterprise Server Edition per Cognos	cognos
db24mgmt	DB2 Enterprise Server Edition per i servizi Tivoli Enterprise Portal	teps
db24tsrm	DB2 Enterprise Server per Tivoli Service Request Manager	tsrm
db24sms	DB2 Enterprise Server per servizi di modelli semantici	cplex
tds	Tivoli Directory Server	tdsprxyapp, tdspxyevt, tdspxygmt, tamas, tim
tdspxyapp	Tivoli Directory Server Proxy (server delle applicazioni)	wpe
tdspxyevt	Tivoli Directory Server Proxy (server eventi)	Nessuno
tdspxygmt	Tivoli Directory Server Proxy (server di gestione)	Nessuno
tdsappsrv	Tivoli Directory Server Application Server	Nessuno
tamps	Tivoli Access Manager Policy Server	Nessuno
tamas	Tivoli Access Manager Authorization Server	tamps
tamwpm	Tivoli Access Manager Web Portal Manager	Nessuno
tamweb	Tivoli Access Manager WebSEAL	Nessuno
tems	Tivoli Monitoring Enterprise Monitoring Server	teps
teps	Tivoli Monitoring Enterprise Portal Server	Nessuno
tim	Tivoli Identity Manager	Nessuno
appdmgr	WebSphere Application Server Network Deployment	wpe, cognos, tsrm, wodm, smsclt, smsdaq, smsmdl, smsrtc, smsgmt
cplex	WebSphere Application Server per CPLEX	Nessuno
ihs	HTTP Server for Runtime (server delle applicazioni)	ihsevt, ihsmgt
ihsevt	HTTP Server for Runtime (server eventi)	Nessuno
ihsmgt	HTTP Server for Runtime (server di gestione)	Nessuno
ncob	Tivoli Netcool/OMNIBus	nci
nci	Tivoli Netcool/Impact	Nessuno
wbm	IBM WebSphere Business Monitor	Nessuno
st	Lotus Sametime	stpxy
stpxy	Lotus Sametime Proxy Application Server	Nessuno
wpe	WebSphere Portal Extend	Nessuno
wmb	WebSphere Message Broker	Nessuno
cognos	IBM Cognos Business Intelligence	Nessuno
tsrm	Tivoli Service Request Manager	Nessuno
wodm	WebSphere Operations Decision Manager	Nessuno

Tabella 73. Dipendenze dell'ordine di arresto del servizio IBM Intelligent Operations Center (Continua)

Servizio	Descrizione	I servizi che devono essere arrestati prima che questo servizio venga arrestato
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Nessuno
smsclt	Servizi di modelli semantici (Client Services)	Nessuno
smsdaq	Servizi di modelli semantici (Data Services)	Nessuno
smsmdl	Servizi di modelli semantici (Model Services)	Nessuno
smsgmt	Servizi di modelli semantici (Management Services)	Nessuno
smsrtc	Servizi di modelli semantici (RTC Services)	Nessuno
iocxml	Probe IBM Intelligent Operations Center XML	Nessuno

## Query dello stato dei servizi

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

### Informazioni su questa attività

Il comando **IOControl.sh** deve essere eseguito come utente `ibmadmin`. Se non si è collegati come `ibmadmin`, eseguire il comando **su - ibmadmin** per passare all'utente `ibmadmin`.

### Procedura

In server di gestione, eseguire il seguente comando per eseguire la query dello stato di tutti i servizi IBM Intelligent Operations Center.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password
```

dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

Per controllare solo un servizio, eseguire il seguente comando.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status service_ID password
```

dove *service\_ID* è un ID elencato in **Opzioni di destinazione** in **IOControl** della guida e dove *password* è la password per Strumento di controllo della piattaforma definito quando Strumento di controllo della piattaforma è stato installato.

### Risultati

I servizi che vengono avviati mostreranno **[on]**. I servizi che non vengono avviati mostreranno **[off]**.

### Operazioni successive

Dopo aver eseguito il comando **IOControl.sh**, controllare i log nella directory `/opt/IBM/ISP/mgmt/logs`. I file di log contengono i risultati del comando **IOControl.sh**.

### Attività correlate:

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Come ottenere supporto per Strumento di controllo della piattaforma”

Le informazioni sono disponibili sulle opzioni di azione e destinazione per Strumento di controllo della piattaforma.

“Installazione di Strumento di controllo della piattaforma” a pagina 49

Lo Strumento di controllo della piattaforma viene utilizzato per gestire l'ambiente del server IBM Intelligent Operations Center. Lo strumento è installato separatamente dal prodotto.

## Come ottenere supporto per Strumento di controllo della piattaforma

Le informazioni sono disponibili sulle opzioni di azione e destinazione per Strumento di controllo della piattaforma.

### Informazioni su questa attività

Il comando **IOControl.sh** deve essere eseguito come utente `ibmadmin`. Se non si è collegati come `ibmadmin`, eseguire il comando `su - ibmadmin` per passare all'utente `ibmadmin`.

### Procedura

In server di gestione eseguire uno dei seguenti comandi per visualizzare le opzioni per il comando **IOControl**.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh help
```

```
o
```

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh
```

### Risultati

Vengono visualizzate le opzioni per il comando **IOControl**.

### Attività correlate:

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Query dello stato dei servizi” a pagina 202

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

---

## Console di gestione

Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.

Per accedere al portlet Console di gestione, nell'interfaccia di WebSphere Portal Administration, fare clic su **Intelligent Operations > Strumenti di gestione > Console di gestione**.



Per ciascun servizio, i link presenti nel portlet Console di gestione indirizzano l'utente sulla console di gestione o alle informazioni su come accedere alla gestione.

**Nota:** Se si utilizza Microsoft Internet Explorer versione 8.0, si potrebbe riscontrare un problema con il link di gestione del report. Il messaggio è: Impossibile trovare la risorsa richiesta. La soluzione è modificare l'URL nel campo indirizzo del browser aggiungendo, /cognos, tra il nome host e /ServletGateway.

## Server delle applicazioni

Tabella 74. Amministrazione sul server delle applicazioni

Console	Amministrazione
Server delle applicazioni	Per gestire diversi i servizi forniti da IBM Intelligent Operations Center, utilizzare il link alla console basata sul Web per WebSphere Application Server. È possibile controllare i server, gestire le risorse e i provider del servizio, modificare l'host e altre impostazioni dell'ambiente.
Amministrazione report	Per configurare i report, utilizzare il link alla console basata sul Web per IBM Cognos Connection. È possibile creare nuovi report o modificare quelli esistenti. È possibile inoltre configurare le origini dati, impostare le cartelle pubbliche e private, definire le autorizzazioni e la distribuzione e pianificare l'esecuzione automatica dei report.

## Server di data

Tabella 75. Amministrazione sul server di dati

Console	Amministrazione
Database	Per ricevere dettagli su come gestire il database con DB2 Enterprise Server Edition, utilizzare il link al centro informazioni. È possibile eseguire le attività con la GUI del centro di controllo del database o dalla riga comandi.

## Server eventi

Tabella 76. Amministrazione sul server eventi

Console	Amministrazione
Contatti	Per visualizzare le impostazioni correnti nel database names.nsf, utilizzare il link per la console basata sul Web del server Lotus Domino. names.nsf viene utilizzato per configurare Lotus Domino Server. Le modifiche alla configurazione possono essere apportate con Domino Administration Client.
Gestione dei contatti	Per avere dettagli su come scaricare e impostare Domino Administration Client per la gestione dei contatti Lotus Domino, utilizzare il link al centro informazioni.
Gestione eventi	Per amministrare la gestione degli eventi con la GUI del server di oggetti, utilizzare il link alla console basata sul Web per Tivoli Netcool/OMNIBus.

Tabella 76. Amministrazione sul server eventi (Continua)

Console	Amministrazione
Elaborazione eventi e miglioramenti	Per gestire l'elaborazione degli eventi, utilizzare il link alla console basata sul Web per Tivoli Netcool/Impact. Ad esempio, è possibile controllare le connessioni al database, le connessioni all'origine dati, l'avvio del processo eventi, lo stato della politica e i log.
Server di messaggistica istantanea	Per gestire la messaggistica istantanea, utilizzare il link alla console basata sul Web per Lotus Sametime Community Server.
Bus di messaggistica	Per avere dettagli su come controllare lo stato dei messaggi con WebSphere Message Broker, utilizzare il link al centro informazioni.
Amministrazione Procedura operativa Standard	Per definire le risorse e procedure operative standard, utilizzare il link alla console basata sul Web per Tivoli Service Request Manager Start Center. È possibile definire le attività e risorse disponibili per la gestione degli eventi in IBM Intelligent Operations Center.
server delle applicazioni Procedura operativa Standard	Per la gestione, utilizzare il link alla console basata sul Web per WebSphere Application Server che utilizza Tivoli Service Request Manager.

## Server di gestione

Tabella 77. Amministrazione sul server di gestione

Console	Amministrazione
Monitoraggio applicazioni	Per gestire il monitoraggio dell'applicazione, utilizzare il link alla console basata sul Web per Tivoli Monitoring. È possibile utilizzare questa console per verifiche sullo stato di integrità del sistema.
Server delle applicazioni per la gestione	Per gestire le applicazioni integrate, utilizzare il link alla console basata sul Web per WebSphere Application Server. Questa gestione include l'amministrazione della sicurezza con Tivoli Access Manager e WebSEAL.
Database	Per ricevere dettagli su come gestire il database con DB2 Enterprise Server Edition, utilizzare il link al centro informazioni. È possibile eseguire le attività con la GUI del centro di controllo del database o dalla riga comandi.
Directory	Per gestire la directory dell'utente, utilizzare il link alla console basata su Web per Tivoli Directory Server. Per ricevere dettagli su come gestire la console basata su web Tivoli Directory Server, utilizzare il link al centro informazioni.

## Personalizzazione del portlet Console di gestione

È possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

### Riferimenti correlati:

“Impostazioni portlet Console di gestione” a pagina 146

Personalizzare il portlet Console di gestione modificando le impostazioni nei campi della finestra

### Impostazioni condivise.

### Informazioni correlate:

 Centro informazioni IBM Lotus Domino e Notes

 Centro informazioni IBM DB2 Database

 IBM Tivoli Directory Server Information Center

## Gestione dei servizi

Il portlet Console di gestione fornisce i collegamenti alle ubicazioni in cui è possibile gestire i servizi forniti dalla soluzione o trovare informazioni più dettagliate sulla gestione dei servizi.

### Server delle applicazioni

#### Servizio del server delle applicazioni

È possibile eseguire un'ampia varietà di attività di gestione dell'applicazione su una comune console basata sul Web, Integrated Solutions Console:

- Verificare lo stato del server.
- Avviare e arrestare server e cluster.
- Distribuire le applicazioni o le patch.
- Gestire l'elenco di portlet disponibili.
- Monitorare i servizi.
- Gestire le politiche di servizio dell'applicazione.
- Gestire i provider del servizio, compresi i provider del servizio REST.
- Gestire le risorse.
- Gestire la sicurezza delle applicazioni.
- Gestire gli host virtuali e altre impostazioni dell'ambiente.
- Eseguire l'amministrazione del sistema.
- Gestire l'integrazione dei servizi.
- Amministrare il server HTTP.
- Gestire la registrazione e la traccia.

Per ulteriori informazioni sul servizio applicazione, consultare la guida in linea per Integrated Solutions Console oppure consultare il link del centro informazioni WebSphere Application Server alla fine della sezione server delle applicazioni.

#### Servizio Gestione report

Per tutte le attività associate alla fornitura di report all'interno di IBM Intelligent Operations Center, è possibile utilizzare la console basata sul Web della gestione report:

- Impostazione delle origini dati.
- Creare, modificare ed eliminare report.
- Gestire l'accesso ai report.
- Pianificare i report.
- Configurare la distribuzione dei report.

Per ulteriori informazioni sul servizio amministrazione di report, consultare il link del centro informazioni IBM Cognos Business Intelligence, alla fine della sezione server delle applicazioni.

#### Informazioni correlate:



Centro informazioni WebSphere Application Server Versione 7.0



Centro informazioni IBM Cognos Business Intelligence

## Server di dati

### Servizio database

È possibile gestire i database IBM Intelligent Operations Center mediante le istanze del servizio database sul sistema server di dati. Un'istanza del servizio database è un processo separato, indipendente che viene eseguito su un server. Un'istanza può ospitare più database. Ogni istanza possiede un nome *nome istanza*. Le seguenti istanze risiedono nel server di dati:

Tabella 78. Le istanze di database che risiedono in server di dati

Istanza	Utilizzato da
dsrdbm01	directory servizio
db2inst1	riservato alle soluzioni
db2inst2	server portale
db2inst3	amministrazione di report
db2inst4	regole di business e servizio monitoraggio di business
db2inst5	servizi modello semantico
db2inst6	servizio amministrazione della procedura operativa standard
db2inst7	servizio di gestione identità
db2inst8	riservati alle applicazioni

Per gestire un'istanza da una finestra di terminale:

1. Collegarsi come utente *nome-istanza*.
2. Eseguire il comando **db2** per immettere la modalità di comando.
3. Immettere **?** per visualizzare un elenco di comandi disponibili. Molti comandi richiedono una connessione attiva ad un database.
  - Per visualizzare i database disponibili per un'istanza, eseguire il comando **list database directory**.
  - Per connettersi a un database, eseguire il comando **connect to database\_name**.
4. Per disconnettersi dal database e terminare la modalità di comando richiesto, eseguire il comando **terminate**.

Per ulteriori informazioni sul servizio database, consultare il link del centro informazioni DB2 Database alla fine della sezione server di dati.

## Informazioni correlate:

 Centro informazioni IBM DB2 Database

## Server eventi

### Contatti, amministrazione dei contatti e servizi messaggistica istantanea

È possibile gestire contatti, amministrazione dei contatti, i servizi messaggistica istantanea mediante:

- Console Lotus Domino Server per visualizzare i contatti correnti.
- Lotus Domino Administration Client per configurare SSO (single sign-on), amministrare il server di messaggistica istantanea e Lotus Sametime Client.
- Lotus Sametime Community Server per registrare e verificare la disponibilità del server di messaggistica istantanea.

**Nota:** Contatti visualizzati nella console di Lotus Domino Server da applicare solo al portlet Contatti e non sono uguali agli utenti IBM Intelligent Operations Center.

Per ulteriori informazioni sui servizi contatti, amministrazione dei contatti e messaggistica istantanea, consultare il link del centro informazioni Lotus Domino e Notes, alla fine della sezione server eventi.

## Servizio per la gestione eventi

È possibile gestire la cattura e archiviazione di eventi in IBM Intelligent Operations Center mediante del GUI il server di oggetti Tivoli Netcool/OMNIBus.

1. Aprire una sessione di terminale abilitata al sistema X Windows.
2. Collegarsi come root al server.
3. Passare alla directory `/opt/IBM/netcool/omnibus`.
4. Per aprire l'applicazione GUI, eseguire il comando: `bin/nco_config`

Per ulteriori informazioni sul servizio gestione eventi, consultare il link del centro informazioni Tivoli Netcool/Impact alla fine della sezione server eventi.

## Elaborazione eventi e miglioramenti del servizio

È possibile gestire l'elaborazione degli eventi attraverso la console basata sul Web per Tivoli Netcool/Impact:

- Verificare le connessioni all'origine dati e database.
- Verificare che EventProcessor sia in esecuzione.
- Verificare la registrazione per le politiche esistenti ed aggiornare il livello di log.
- Aggiornare le politiche esistenti o creare nuove politiche.

Per ulteriori informazioni sul servizio elaborazione e miglioramento eventi, consultare il link del centro informazioni Tivoli Netcool/Impact alla fine della sezione server eventi.

## Bus di messaggistica

I tre metodi principali per la gestione del servizio Bus di messaggistica sono:

- Riga comandi
- Explorer: un'applicazione di gestione basata su Eclipse
- Toolkit: un'applicazione basata su Eclipse che consente sia lo sviluppo dell'applicazione che amministrativo

È possibile gestire i flussi di comunicazione, definire test, trasformazioni, integrazioni e la registrazione, con lo strumento di sviluppo della GUI.

WebSphere Message Broker Toolkit viene fornito con IBM Intelligent Operations Center. Per informazioni sull'installazione e l'utilizzo del toolkit, consultare il link del centro informazioni WebSphere Message Broker alla fine della sezione server eventi

Per configurare l'ambiente della riga comandi ed eseguire la query delle istanze del WebSphere Message Broker:

- Collegarsi al server come utente mqm.
- Passare alla directory /opt/IBM/mqsi/8.0.0.0.
- Per configurare l'ambiente, eseguire il comando `source bin/mqsiprofile`.
- Per eseguire la query delle istanze WebSphere Message Broker, eseguire il comando: `bin/mqsilist`.

Per ulteriori informazioni sul servizio bus messaggio, consultare il link del centro informazioni WebSphere Message Broker alla fine della sezione server eventi.

### **Servizio di gestione procedura operativa standard**

È possibile definire risorse e attività per la gestione degli eventi mediante la console basata sul Web amministrata dalla procedura operativa standard, centro di avvio Tivoli Service Request Manager.

Per ulteriori informazioni sul servizio amministrato dalla procedura operativa standard, consultare il link del centro informazioni Tivoli Service Request Manager, alla fine della sezione server eventi.

### **Servizio applicazioni procedura operativa standard**

È possibile gestire le applicazioni associate alle risorse e alle attività tramite la console basata sul Web per WebSphere Application Server, che serve Tivoli Service Request Manager.



Per ulteriori informazioni sul servizio dell'applicazione procedura operativa standard, consultare la guida in linea oppure consultare il link del centro informazioni WebSphere Application Server Versione 7.0 alla fine della sezione server delle applicazioni.

#### **Concetti correlati:**

“Configurazione di Tivoli Service Request Manager” a pagina 123

Nell'interfaccia utente Tivoli Service Request Manager, è possibile gestire procedure operative standard, flussi di lavoro e le risorse.

#### **Informazioni correlate:**

-  Centro informazioni IBM Lotus Domino e Notes
-  Centro informazioni di IBM Tivoli Netcool/Impact
-  IBM WebSphere Message Broker Information Center
-  IBM Tivoli Service Request Manager Information Center

### **Server di gestione Servizio monitoraggio applicazioni**

È possibile gestire il monitoraggio applicazioni attraverso la console basata sul Web per Tivoli Monitoring. Scaricare l'applicazione ed eseguirla per controllare lo stato dei server e visualizzare tutti gli agent di monitoraggio in esecuzione. Per effettuare l'accesso, immettere l'ID utente e la password. L'ID utente predefinito è sysadmin e la password della topologia immessa durante l'installazione.

Per ulteriori informazioni sul servizio monitoraggio applicazioni, consultare il link Tivoli Enterprise Portal - User's Guide, alla fine dell'argomento.

## Server delle applicazioni per il servizio di gestione

È possibile gestire le giunzioni per Tivoli Access Manager WebSEAL sulla comune console basata sul Web, Integrated Solutions Console.

Per ulteriori informazioni su questo servizio, consultare la guida in linea oppure consultare il link del centro informazioni WebSphere Application Server Versione 7.0 alla fine della sezione server delle applicazioni.

## Servizio database

C'è una sola istanza del servizio database, db2inst2, ospitato sul server di gestione. È possibile utilizzare questa istanza per la gestione del sistema e la memorizzazione dei dati specifici per Tivoli Access Manager.

Per informazioni dettagliate sul servizio database, consultare il link del centro informazioni IBM DB2 Database alla fine della sezione server di dati.

## Servizio directory

Gestire la directory degli utenti attraverso la console basata sul Web per Tivoli Directory Server, è possibile visualizzare, aggiungere o modificare gli utenti in LDAP.

Per ulteriori informazioni dettagliate sul servizio directory, consultare il link del centro informazioni Tivoli Directory Server, alla fine dell'argomento.

### Informazioni correlate:



IBM Tivoli Monitoring, Tivoli Enterprise Portal user's guide



IBM Tivoli Directory Server Information Center

---

## Verifica dei componenti

Lo strumento Controllo di verifica del sistema esegue il test dei componenti presenti in IBM Intelligent Operations Center per verificare se sono accessibili e funzionanti.

## Come utilizzare lo strumento Controllo di verifica del sistema

Lo strumento Controllo di verifica del sistema viene utilizzato per determinare lo stato operativo di servizi compreso il sistema IBM Intelligent Operations Center.

## Informazioni su questa attività

Lo strumento Controllo di verifica del sistema verifica le funzionalità di sistema.




Per dettagli sui singoli test e sulla risoluzione dei problemi nel caso in cui il test abbia esito negativo, fare clic su **Guida** per il test.

**Proprietà** fornisce ulteriori informazioni relative al test da utilizzare quando viene contattato il supporto software IBM.

## Procedura

1. Collegarsi a IBM Intelligent Operations Center come utente con autorizzazione di amministratore.
2. Fare clic su **Intelligent Operations > Strumenti di gestione > Controllo di verifica del sistema**.
3. Selezionare il test o più test da eseguire effettuando quanto segue:
  - Fare clic su un test specifico da eseguire.
  - Fare clic su **Esegui tutti i test** per verificare le funzionalità di tutte le selezioni.

## Risultati

L'icona  verrà visualizzata quando un test è completato con esito positivo. L'icona  verrà visualizzata quando un test ha esito negativo. Se un test ha esito negativo, attenersi alle istruzioni per la determinazione del problema del test per risolvere gli errori. È possibile accedere a queste istruzioni facendo clic sull'icona  o sulla **Guida**.

Se è stato eseguito un test specifico, i risultati di esecuzione del test vengono visualizzati nella parte inferiore del portlet insieme all'ora di esecuzione del test. Se è stata selezionata l'opzione **Esegui tutti i test**, queste informazioni non vengono visualizzate.

## Operazioni successive

Lo strumento può essere reimpostato e tutti i risultati cancellati, facendo clic su **Reimposta**.

### Attività correlate:

“Verifica dell'installazione” a pagina 52

Dopo l'installazione di IBM Intelligent Operations Center, accertarsi che il prodotto sia stato correttamente installato.

“Installazione dello strumento Controllo di verifica del sistema” a pagina 50

Lo strumento Controllo di verifica del sistema viene utilizzato per verificare lo stato operativo dei componenti in IBM Intelligent Operations Center. Lo strumento viene installato separatamente dal prodotto.

## Test di Controllo di verifica del sistema

IBM Intelligent Operations Center fornisce svariati test Controllo di verifica del sistema che possono essere utilizzati per determinare lo stato operativo di diversi servizi e componenti di IBM Intelligent Operations Center.

I test sono raggruppati in modo logico per funzione. Ad esempio, collaborazione e monitoraggio.

### Test di Gestione account (Tivoli Identity Manager API)

Il test di Gestione account (Tivoli Identity Manager API) verifica l'accesso all'API di Tivoli Identity Manager accedendo alla porta IIOP.

### Risorse

Il test di Gestione account (Tivoli Identity Manager API) utilizza la seguente risorsa:

- Tivoli Identity Manager Server (su server di gestione).

### Determinazione del problema

Se il test di Gestione account (Tivoli Identity Manager API) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.



## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server di gestione. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di gestione da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. Nel server di gestione, esaminare i log di Tivoli Identity Manager riportati di seguito:
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
    - Tutti i file di log presenti nelle sottodirectory V6 della directory `/var/idsldap/`.
3. Accertarsi che i file system sui sistemi server delle applicazioni e server di gestione non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il server Tivoli Identity Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server di gestione, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare il l'agent del nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "timServer1". Il server sembra arrestato.`, avviare `timServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "timServer1" è AVVIATO.`. Se è stato necessario avviare `timServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server timserver aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `timServer1`

Arrestare i server in questo ordine:

- a. `timServer1`
- b. `agentnodo`

Il server `timServer1` viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server di gestione: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.


5. Verificare che il server Tivoli Identity Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:

- a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://MANAGEMENT_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `MANAGEMENT_SERVER_HOST` è il nome host per server di gestione.

- b. Visualizzare lo stato del server `timServer1` facendo clic su **Server > Tipi di server > WebSphere Application Server**.

L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.

L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `timServer1`

Arrestare i server in questo ordine:

- a. `timServer1`
- b. `agentnodo`

Per arrestare il server `timServer1`, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server di gestione: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

6. Verificare che sia possibile accedere alla console di Tivoli Identity Manager dal sistema WebSphere Portal su server delle applicazioni utilizzando il seguente URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. dove `MANAGEMENT_SERVER_HOST` è il nome host per server di gestione. Collegarsi con l'ID utente `itim manager`.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Gestione account (Tivoli Identity Manager Console)

Il test Gestione account (Tivoli Identity Manager Console) determina se è possibile accedere a Tivoli Identity Manager accedendo all'URL di gestione Tivoli Identity Manager.

## Risorse

Il test di Gestione account (Tivoli Identity Manager Console) utilizza la seguente risorsa:

- Tivoli Identity Manager Server (su server di gestione)

## Determinazione del problema

Se il test di Gestione account (Tivoli Identity Manager Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server di gestione. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di gestione da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. Nel server di gestione, esaminare i log di Tivoli Identity Manager riportati di seguito:
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
    - Tutti i file di log presenti nelle sottodirectory V6 della directory `/var/idsldap/`.
3. Accertarsi che i file system sui sistemi server delle applicazioni e server di gestione non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il server Tivoli Identity Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server di gestione, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent del nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "timServer1". Il server sembra arrestato.`, avviare `timServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "timServer1" è AVVIATO.`. Se è stato necessario avviare `timServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server timserver aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `timServer1`

Arrestare i server in questo ordine:

- a. timServer1
- b. agentnodo

Il server timServer1 viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.


L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server di gestione: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Verificare che il server Tivoli Identity Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:

- a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://MANAGEMENT_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `MANAGEMENT_SERVER_HOST` è il nome host per server di gestione.
- b. Visualizzare lo stato del server timServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.

L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.

L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. timServer1

Arrestare i server in questo ordine:

- a. timServer1
- b. agentnodo

Per arrestare il server timServer1, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server di gestione: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

6. Verificare che sia possibile accedere alla console di Tivoli Identity Manager dal sistema WebSphere Portal su server delle applicazioni utilizzando il seguente URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. dove `MANAGEMENT_SERVER_HOST` è il nome host per server di gestione. Collegarsi con l'ID utente `itim manager`.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Gestione account (Assemblaggio elenco Tivoli Directory Integrator)

Il test di Gestione account (Assemblaggio elenco Tivoli Directory Integrator) determina se sono disponibili le risorse di Tivoli Directory Integrator List Assembly. Per fare ciò, il comando **tdisrvctl**, che gestisce in remoto le configurazioni, le linee di assemblaggio e altre funzioni, viene eseguito su server di gestione, mentre il test ricerca la restituzione del codice "--- AssemblyLines ---".

### Risorse

Il test di Gestione account (Assemblaggio elenco Tivoli Directory Integrator) utilizza le seguenti risorse:

- Tivoli Directory Server (su server di dati)
- Tivoli Directory Integrator (su server di gestione)

### Determinazione del problema

Se il test di Gestione account (Assemblaggio elenco Tivoli Directory Integrator) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server di dati. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di dati da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system sui sistemi server di dati e server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che Tivoli Directory Integrator Server sia in esecuzione.

- a. Collegarsi a una sessione di terminale su server di gestione come `ibmadmin`.
- b. Eseguire il comando **ps -ef | grep ibmdisrv**. I risultati saranno simili a quanto riportato di seguito:

```
ibmadmin      11411      1  0 Sep06 pts/1    00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timso1 -c ITIM_RMI.xml -d
ibmadmin      32080 19149  0 23:17 pts/1    00:00:00 grep ibmdisrv
```

In questo esempio viene mostrato che il daemon di Tivoli Directory Integrator Server, `ibmdisrv`, è in esecuzione.

5. Avviare Tivoli Directory Integrator Server, `ibmdisrv`, nel caso non sia in esecuzione.
  - a. Collegarsi a una sessione di terminale su server di gestione come `root`.
  - b. Eseguire `/etc/init.d/ITIMAd start`.
6. Verificare che il server Tivoli Directory Server LDAP sia in esecuzione.
  - a. Collegarsi a una sessione di terminale su server di dati come `root`.
  - b. Eseguire il comando **ps -ef | grep ibmslapd**. I risultati saranno simili a quanto riportato di seguito:

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
```

L'esempio mostra che il daemon Tivoli Directory Server, `ibmslapd`, è in esecuzione.

- c. Eseguire il comando **ps -ef | grep ibmdiradm**. I risultati saranno simili a quanto riportato di seguito:

```
root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Questo esempio mostra che il daemon Tivoli Directory Server, `ibmdiradm`, è in esecuzione.

7. Se il daemon Tivoli Directory Server, `ibmslapd`, non è in esecuzione, effettuare le operazioni riportate di seguito.

- a. Come utente *root* di Linux, eseguire `/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01` per avviare Directory Server
8. Se il daemon Tivoli Directory Administration Server, *ibmdiradm*, non è in esecuzione, effettuare le operazioni riportate di seguito.
  - a. Da una sessione di terminale su server di dati, eseguire `su - dsrdbm01`.
  - b. Eseguire `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t` per avviare server delle applicazioni.
9. Se il daemon Tivoli Directory Server, *ibmslapd*, è in esecuzione, effettuare le operazioni riportate di seguito.
 

**Nota:** eseguire questa operazione anche se Tivoli Directory Server è stato avviato nel passo precedente.

  - a. Collegarsi a una sessione di terminale su server di dati come *dsrdbm01*.
  - b. Eseguire `idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*`, dove *ADMIN\_PASSWORD* è la password account dell'amministratore root LDAP. Verranno visualizzati gli oggetti utente LDAP esistenti.
10. Verificare che Tivoli Directory Server Web Administration Tool sia in esecuzione. Tivoli Directory Server Web Administration Tool viene utilizzato per arrestare e avviare l'istanza LDAP, per aggiungere utenti o account e per visualizzare i file di log.
  - a. Collegarsi a una sessione di terminale su server di gestione come *ibmadmin*.
  - b. Eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD` sul server di gestione dove *WAS\_ADMIN\_PASSWORD* è la password dell'amministratore di WebSphere Application Server. Se lo strumento è in esecuzione, verrà restituito un messaggio simile a quello riportato di seguito.  
 ADMU0508I: il server delle applicazioni "tdsServer" è AVVIATO  
 Se viene restituito il seguente messaggio, è necessario avviare il server *tdsServer*.  
 ADMU0509I: impossibile raggiungere il server delle applicazioni "tdsServer". Il server sembra essere arrestato.
  - c. Avviare il server *tdsServer* eseguendo il comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer`. Verrà avviato il server *tdsServer* e verrà visualizzato un messaggio simile a quello riportato di seguito.  
 ADMU3000I: server *tdsServer* aperto per e-business; id processo 26654
11. Accedere a Tivoli Directory Server Web Administration Tool all'indirizzo: `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` dove *MANAGEMENT\_SERVER\_HOST* è il nome host di server di gestione.
12. Collegarsi con l'account di amministratore root LDAP, *cn=root* e la password appropriata. Il nome del server LDAP deve essere `DATABASE_DIRECTORY_SERVER_HOST:389`, dove *DATABASE\_DIRECTORY\_SERVER\_HOST* è il nome host di server di dati.
13. Fare clic su **Gestione server > Start/stop/reset server**. Verrà visualizzato lo stato del server LDAP. Questa pagina può anche essere utilizzata per avviare, arrestare o reimpostare il server LDAP.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Gestione account (Tivoli Directory Server)

Il test di Gestione account (Tivoli Directory Server) determina se Tivoli Directory Server è disponibile inviando una richiesta HTTP al server.

## Risorse

Il test di Gestione account (Tivoli Directory Server) utilizza la seguente risorsa:

- Tivoli Directory Server (su server di dati)



## Determinazione del problema

Se il test di **Tivoli Directory Server HTTP** ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
2. Accertarsi che i file system su server di dati non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Verificare che il server Tivoli Directory Server LDAP sia in esecuzione.
  - a. Collegarsi a una sessione di terminale su server di dati come **root**.
  - b. Eseguire il comando **ps -ef | grep ibmslapd**. I risultati saranno simili a quanto riportato di seguito:

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149    0 23:17 pts/1    00:00:00 grep ibmslapd
```

L'esempio mostra che il daemon Tivoli Directory Server, **ibmslapd**, è in esecuzione.
  - c. Eseguire il comando **ps -ef | grep ibmdiradm**. I risultati saranno simili a quanto riportato di seguito:

```
root      4394 14038    0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

Questo esempio mostra che il daemon Tivoli Directory Server, **ibmdiradm**, è in esecuzione.
4. Se il daemon Tivoli Directory Server, **ibmslapd**, non è in esecuzione, effettuare le operazioni riportate di seguito.
  - a. Come utente **root** di Linux, eseguire **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** per avviare Directory Server
5. Se il daemon Tivoli Directory Administration Server, **ibmdiradm**, non è in esecuzione, effettuare le operazioni riportate di seguito.
  - a. Da una sessione di terminale su server di dati, eseguire **su - dsrdbm01**.
  - b. Eseguire **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** per avviare server delle applicazioni.
6. Se il daemon Tivoli Directory Server, **ibmslapd**, è in esecuzione, effettuare le operazioni riportate di seguito.

**Nota:** eseguire questa operazione anche se Tivoli Directory Server è stato avviato nel passo precedente.

  - a. Collegarsi a una sessione di terminale su server di dati come **dsrdbm01**.
  - b. Eseguire **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\***, dove **ADMIN\_PASSWORD** è la password account dell'amministratore root LDAP. Verranno visualizzati gli oggetti utente LDAP esistenti.
7. Verificare che Tivoli Directory Server Web Administration Tool sia in esecuzione. Tivoli Directory Server Web Administration Tool viene utilizzato per arrestare e avviare l'istanza LDAP, per aggiungere utenti o account e per visualizzare i file di log.
  - a. Collegarsi a una sessione di terminale su server di gestione come **ibmadmin**.
  - b. Eseguire il comando **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PASSWORD** sul server di gestione dove **WAS\_ADMIN\_PASSWORD** è la password dell'amministratore di WebSphere Application Server. Se lo strumento è in esecuzione, verrà restituito un messaggio simile a quello riportato di seguito.

```
ADMU0508I: il server delle applicazioni "tdsServer" è AVVIATO
```

Se viene restituito il seguente messaggio, è necessario avviare il server **tdsServer**.

ADMU0509I: impossibile raggiungere il server delle applicazioni "tdsServer". Il server sembra essere arrestato.

- c. Avviare il server tdsServer eseguendo il comando `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer`. Verrà avviato il server tdsServer e verrà visualizzato un messaggio simile a quello riportato di seguito.

ADMU3000I: server tdsServer aperto per e-business; id processo 26654

8. Accedere a Tivoli Directory Server Web Administration Tool all'indirizzo: `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` dove `MANAGEMENT_SERVER_HOST` è il nome host di server di gestione.
9. Collegarsi con l'account di amministratore root LDAP, `cn=root` e la password appropriata. Il nome del server LDAP deve essere `DATABASE_DIRECTORY_SERVER_HOST:389`, dove `DATABASE_DIRECTORY_SERVER_HOST` è il nome host di server di dati.
10. Fare clic su **Gestione server > Start/stop/reset server**. Verrà visualizzato lo stato del server LDAP. Questa pagina può anche essere utilizzata per avviare, arrestare o reimpostare il server LDAP.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Analytics (Cognos Gateway Console)

Il test di Analytics (Cognos Gateway Console) determina se è possibile accedere a Cognos, su server delle applicazioni, dall'URL Cognos Servlet Gateway e Cognos Administration Portal.

## Risorse

Il test di Analytics (Cognos Gateway Console) utilizza la seguente risorsa:

- Cognos (sul sistema server delle applicazioni).

## Determinazione del problema

Se il test di Analytics (Cognos Gateway Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedure

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. In server delle applicazioni, esaminare i log di Cognos riportati di seguito:
    - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemErr.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log`
    - Tutti file di log presenti nella directory `/opt/IBM/cognos/c10_64/logs/`.
2. Accertarsi che i file system sul sistema server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando `df -h`.
3. Accertarsi che i server Cognos Dispatcher e Cognos Gateway siano avviati. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `cgnsadm` (utente Cognos).
  - b. In una finestra comandi, eseguire: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere Application Server.



- c. Se viene visualizzato un messaggio simile al seguente: ADMU0509I: impossibile raggiungere il server delle applicazioni "nodeagent". Il server sembra arrestato., avviare nodeagent utilizzando il seguente comando: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: ADMU0508I: il server delle applicazioni "nodeagent" è AVVIATO. . Se è stato necessario avviare nodeagent, verrà visualizzato un messaggio simile al seguente: ADMU3000I: server nodeagent aperto per e-business; id processo 26654.
- d. Se viene visualizzato un messaggio simile al seguente: ADMU0509I: impossibile raggiungere il server delle applicazioni "CognosX\_Displ". Il server sembra arrestato. , avviare CognosX\_Displ utilizzando il seguente comando: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX\_Displ. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: ADMU0508I: il server delle applicazioni "CognosX\_Displ" è AVVIATO . Se è stato necessario avviare CognosX\_Displ, verrà visualizzato un messaggio simile al seguente: ADMU3000I: server CognosX\_Displ aperto per e-business; id processo 26654.
- e. Se viene visualizzato un messaggio simile al seguente: ADMU0509I: impossibile raggiungere il server delle applicazioni "CognosX\_GW1". Il server sembra arrestato. , avviare CognosX\_GW1 utilizzando il seguente comando: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX\_GW1. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: ADMU0508I: il server delle applicazioni "CognosX\_GW1" è AVVIATO . Se è stato necessario avviare CognosX\_GW1, verrà visualizzato un messaggio simile al seguente: ADMU3000I: server CognosX\_GW1 aperto per e-business; id processo 26676.

**Important:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. nodeagent
- b. CognosX\_Displ
- c. CognosX\_GW1

Arrestare i server in questo ordine:

- a. CognosX\_GW1
- b. CognosX\_Displ
- c. nodeagent

Il server CognosX\_GW1 viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul sistema server delle applicazioni: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX\_GW1 -username waswebadmin -password WAS\_ADMIN\_PWD, dove WAS\_ADMIN\_PWD è la password dell'amministratore WebSphere.

Il server CognosX\_Displ viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul sistema server delle applicazioni: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX\_Displ -wasadmin admin -password WAS\_ADMIN\_PWD, dove WAS\_ADMIN\_PWD è la password dell'amministratore WebSphere.


Il comando nodeagent viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul sistema server delle applicazioni: /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD, dove WAS\_ADMIN\_PWD è la password dell'amministratore WebSphere.

4. Accertarsi che i server Cognos Dispatcher e Cognos Gateway siano avviati. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:

- a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.
- b. Visualizzare lo stato dei server CognosX-Disp1 e CognosX\_GW1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.

L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.

L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` in una finestra comandi.

**Important:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. nodeagent
- b. CognosX\_Displ
- c. CognosX\_GW1

Arrestare i server in questo ordine:

- a. CognosX\_GW1
- b. CognosX\_Displ
- c. nodeagent

Per arrestare i server CognosX\_GW1 e CognosX\_Displ, selezionarli e fare clic su **Arresta**.

Il comando nodeagent viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul sistema server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere.

5. Accertarsi che sia possibile accedere a Cognos Administration Portal dal sistema WebSphere Portal, su server delle applicazioni, utilizzando il seguente URL: `http://APPLICATION_SERVER_HOST:9081/ServletGateway/servlet/Gateway`, dove `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

## What to do next

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Server delle applicazioni (Servizio Web di WebSphere Application Server)

Il test di Server delle applicazioni (Servizio Web di WebSphere Application Server) verifica l'accesso al servizio Web di WebSphere Application Server accedendo al servizio Web DrpGeoSvcs.

## Risorse

Il test di Server delle applicazioni (Servizio Web di WebSphere Application Server) utilizza la seguente risorsa:

- WebSphere Application Server (su server delle applicazioni).

## Determinazione del problema

Se il test di Server delle applicazioni (Servizio Web di WebSphere Application Server) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di configurazione di WebSphere UDDI Registry riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log
2. Verificare che il file system su server delle applicazioni non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando `df -h`.
3. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
    - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "cpudServer1". Sembra arrestato.` avviare cpudServer1 utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "cpudServer1" è AVVIATO.`. Se è stato necessario avviare cpudServer1, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server cpudServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:




- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Il server cpudServer1 viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per il server delle applicazioni.
  - b. Visualizzare lo stato del server cpudServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Per arrestare il server cpudServer, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Verificare che sia possibile accedere alla console utente UDDI di WebSphere.
  - a. Su server delle applicazioni, accedere a `https://APPLICATION_SERVER_HOST:9080/uddigui/`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Regole di business (WebSphere Operational Decision Manager JRules Console)

Il test di Regole di business (WebSphere Operational Decision Manager JRules Console) verifica l'accesso a WebSphere Operational Decision Management JRules accedendo alla console Rule Execution Server.

## Risorse

Il test di Regole di business (WebSphere Operational Decision Manager JRules Console) utilizza la seguente risorsa:

- WebSphere Operational Decision Management JRules (su server delle applicazioni).

## Determinazione del problema

Se il test di Regole di business (WebSphere Operational Decision Manager JRules Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di configurazione di WebSphere Operational Decision Management riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
2. Verificare che il file system su server delle applicazioni non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che Rule Execution Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "wodmServer1". Sembra arrestato.`, avviare `wodmServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "wodmServer1" è AVVIATO.`. Se è stato necessario avviare `wodmServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server wodmServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `wodmServer1`




Arrestare i server in questo ordine:

- a. `wodmServer1`
- b. `agentnodo`

Il server `wodmServer1` viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.



L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Accertarsi che Rule Execution Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.
  - b. Visualizzare lo stato del server `wodmProfile` facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `wodmServer1`

Arrestare i server in questo ordine:

- a. `wodmServer1`
- b. `agentnodo`

Per arrestare il server `wodmProfile`, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere a Rule Execution Server Console da server delle applicazioni all'indirizzo `http://APPLICATION_SERVER_HOST:9083/res`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni. Collegarsi utilizzando l'ID utente `resAdmin1`.
6. In Rule Execution Server Console aprire la console Diagnostics. Fare clic su **Run Diagnostics**. Verrà visualizzato un report con l'esecuzione dei test. Fare clic su **Expand All** per visualizzare i dettagli di ciascun test.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Regole di business (WebSphere Operational Decision Manager JRules Rule)

Regole di business (WebSphere Operational Decision Manager JRules Rule) esegue il test dell'accesso al motore di regole JRules di WebSphere Operational Decision Management contattando la regola di business `cardTransactionRuleApp` installata su Rules Execution Server e verificando l'output.

## Risorse

Il test di Regole di business (WebSphere Operational Decision Manager JRules Rule) utilizza la seguente risorsa:

- WebSphere Operational Decision Management JRules (su server delle applicazioni).

## Determinazione del problema

Se il test di Regole di business (WebSphere Operational Decision Manager JRules Rule) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di configurazione di WebSphere Operational Decision Management riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
2. Verificare che il file system su server delle applicazioni non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che Rule Execution Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "wodmServer1". Sembra arrestato.`, avviare `wodmServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "wodmServer1" è AVVIATO.`. Se è stato necessario avviare `wodmServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server wodmServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `wodmServer1`




Arrestare i server in questo ordine:

- a. `wodmServer1`
- b. `agentnodo`



Il server wodmServer1 viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Accertarsi che Rule Execution Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.
  - b. Visualizzare lo stato del server wodmProfile facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. wodmServer1

Arrestare i server in questo ordine:

- a. wodmServer1
- b. agentnodo

Per arrestare il server wodmProfile, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere a Rule Execution Server Console da server delle applicazioni all'indirizzo `http://APPLICATION_SERVER_HOST:9083/res`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni. Collegarsi utilizzando l'ID utente `resAdmin1`.
6. In Rule Execution Server Console aprire la console Diagnostics. Fare clic su **Run Diagnostics**. Verrà visualizzato un report con l'esecuzione dei test. Fare clic su **Expand All** per visualizzare i dettagli di ciascun test.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Collaboration (Lotus Domino Console)

Il test di Collaboration (Lotus Domino Console) determina se Domino Directory è accessibile tramite il suo URL.

### Risorse

Il test di Collaboration (Lotus Domino Console) utilizza la seguente risorsa:

- Domino Server (on the server eventi).

### Determinazione del problema

Se il test di Collaboration (Lotus Domino Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. Nel server eventi, esaminare i log di Lotus Domino riportati di seguito:
    - /local/notesdata/console.out
    - /local/notesdata/log.nsf
    - Tutti i file di log presenti nella directory /local/notesdata/IBM\_TECHNICAL\_SUPPORT/.
2. Verificare che i file system sul sistema server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Verificare che i componenti del processo Lotus Domino siano in esecuzione.
  - a. Accedere alla console di Lotus Domino Directory all'indirizzo `http://EVENT_SERVER_HOST:84/names.nsf` dove `EVENT_SERVER_HOST` è il nome host di server eventi. Accedere utilizzando il nome utente e la password dell'amministratore Domino.
  - b. Se non è possibile accedere alla console, su server eventi, eseguire il comando `ps -ef | grep notes` per determinare se i processi Lotus Domino sono in esecuzione. I processi Lotus Domino sono:
    - server
    - event
    - update
    - replica
    - router
    - adminp
    - calconn
    - sched
    - http
    - rnmgr
    - staddin
4. Se una parte dei processi è in esecuzione, arrestare tali processi prima di riavviare tutti i processi.
  - a. Su server eventi, collegarsi come utente notes.
  - b. Passare alla directory /local/notesdata.
  - c. Eseguire il comando `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` per arrestare tutti i processi Lotus Domino in esecuzione.
  - d. Controllare che tutti i processi siano stati arrestati eseguendo il comando `ps -ef | grep notes`.
  - e. Se alcuni processi Lotus Domino sono ancora in esecuzione, arrestarli utilizzando il comando `kill -9 pid` dove `pid` è l'identificativo del processo Lotus Domino.
5. Se i processi Lotus Domino non sono in esecuzione, avviare i componenti Lotus Domino Server.
  - a. Su server eventi, collegarsi come utente notes.

- b. Passare alla directory `/local/notesdata`.
- c. Eseguire il comando `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` per avviare tutti i componenti Lotus Domino Server.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Collaboration (Lotus Sametime Console)

Il test di Collaboration (Lotus Sametime Console) determina se Sametime Console è accessibile tramite il relativo URL.

## Risorse

Il test di Collaboration (Lotus Sametime Console) utilizza la seguente risorsa:

- Sametime Server (su server eventi).

## Determinazione del problema

Se il test di Collaboration (Lotus Sametime Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Raccogliere ed esaminare i file di log e di configurazione di Sametime Community Server.
  - a. Collegarsi a server eventi come utente *notes*.
  - b. Passare alla directory `/local/notesdata`.
  - c. Eseguire il comando `sh stdiagzip.sh`. Questo comando eseguirà la raccolta di tutti i file di log pertinenti e li scriverà nella directory `/local/notesdata/`.
  - d. Revisionare i file di log presenti nella directory `/local/notesdata/`.
2. Verificare che i file system sul sistema server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando `df -h`.
3. Accertarsi che i componenti del processo Sametime siano in esecuzione.
  - a. Accedere alla home page Sametime all'indirizzo `http://EVENT_SERVER_HOST:84/stcenter.nsf` dove `EVENT_SERVER_HOST` è in nome host di server eventi. Accedere utilizzando il nome utente e la password dell'amministratore Domino.
  - b. Sulla home page di Sametime, fare clic su **Administer the server**.
  - c. Sulla pagina Server - Overview, assicurarsi che tutti i servizi Sametime siano in esecuzione.
4. Se una parte dei processi è in esecuzione, arrestare tali processi prima di riavviare tutti i processi.
  - a. Su server eventi, collegarsi come utente *notes*.
  - b. Passare alla directory `/local/notesdata`.
  - c. Eseguire il comando `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` per arrestare tutti i processi Sametime in esecuzione.
  - d. Controllare che tutti i processi siano stati arrestati eseguendo il comando `ps -ef | grep notes`.
  - e. Se alcuni processi sono ancora in esecuzione, arrestarli utilizzando il comando `kill -9 pid`, dove `pid` è l'identificativo del processo Lotus Domino.
5. Se i processi Sametime non sono in esecuzione, avviare i componenti del server Lotus Sametime.
  - a. Su server eventi, collegarsi come utente *notes*.
  - b. Passare alla directory `/local/notesdata`.
  - c. Eseguire il comando `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` per avviare tutti i componenti Lotus Sametime Server.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Collaboration (Lotus Sametime Proxy)

Il test di Collaboration (Lotus Sametime Proxy) determina se è possibile accedere all'applicazione Lotus Sametime Proxy Web dall'URL dell'applicazione Lotus Sametime Proxy Web.

## Risorse

Il test di Collaboration (Lotus Sametime Proxy) utilizza la seguente risorsa:

- Sametime Proxy (su server delle applicazioni).

## Determinazione del problema

Se il test di Collaboration (Lotus Sametime Proxy) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di Sametime Proxy Server riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemErr.log
2. Verificare che i file system sul sistema server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che Sametime Proxy Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi, eseguire: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "nodeagent". Il server sembra arrestato.`, avviare `nodeagent` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "nodeagent" è AVVIATO.` . Se è stato necessario avviare `nodeagent`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server nodeagent aperto per e-business; id processo 26654.`
  - d. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "STProxyServer1". Il server sembra arrestato.` , avviare `STProxyServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/startServer.sh STProxyServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "STProxyServer1" è AVVIATO.` . Se è stato necessario avviare `STProxyServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server STProxyServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:




- a. nodeagent
- b. STProxyServer1

Arrestare i server in questo ordine:

- a. STProxyServer1
- b. nodeagent

Il server STProxyServer1 viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere.

Il comando nodeagent viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere.

4. Accertarsi che Sametime Proxy Server sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.
  - b. Visualizzare lo stato del server STProxyServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. nodeagent
- b. STProxyServer1

Arrestare i server in questo ordine:

- a. STProxyServer1
- b. nodeagent

Per arrestare il server STProxyServer1, selezionare il server e fare clic su **Arresta**.

Il comando nodeagent viene arrestato eseguendo il comando riportato di seguito in una finestra comandi sul server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere.

5. Accertarsi che sia possibile accedere a Sametime Proxy Console dal sistema WebSphere Portal, su server delle applicazioni, utilizzando il seguente URL: `http://APPLICATION_SERVER_HOST:9085/stwebclient/popup.jsp`, dove `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Database (DB2)

Il test di Database (DB2) determina se è possibile accedere alla connessione JDBC tra l'applicazione Web e server di dati. Viene stabilita una connessione JDBC tipo 4 e immessa una query SQL dinamica per il conteggio del numero di tabelle presenti nel database.

## Risorse

Il test di Database (DB2) utilizza le seguenti risorse:

- Definizione UddiDataSource contenente la connessione per il database UDDIDB (su server delle applicazioni).
- Database UDDIDB (istanza db2inst4 su server di dati).

## Determinazione del problema

Se il test di Database (DB2) non è in grado di accedere a server di dati, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni (dove il test è stato avviato) e server di dati (dove risiede il database). Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di dati da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system sul sistema server di dati non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Accertarsi che i database utilizzati da server di dati siano avviati.
  - a. Su server di dati, eseguire il comando riportato di seguito da una finestra comandi come db2inst4:

```
ps -ef | grep db2 | grep db2inst4
```

I processi DB2, compresi i seguenti, devono essere eseguiti come utente dell'istanza db2inst4:

```
db2sysc
db2vend
db2acd
```

5. Se i processi DB2 non sono in esecuzione, avviarli eseguendo `db2start` dalla finestra comandi come utente db2inst4:
6. Controllare i log DB2 per errori associati all'istanza database utilizzata per questo test. I log si trovano su server di dati nella directory `/datahome/db2inst4/sqllib/db2dump`.
7. Controllare la presenza nel file `db2diag.log` di errori emessi durante l'avvio del database utilizzato per questo test.
8. Verificare la connessione alle risorse del contenitore Web DataSource utilizzando la console di gestione WebSphere Application Server.
  - a. Su server delle applicazioni, accedere alla console di gestione WebSphere Application Server all'indirizzo: `https://APPLICATION_SERVER_HOST:9043/ibm/console`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni.



- b. Fare clic su **Risorse** > **JDBC** > **Origini dati**.
- c. Controllare l'origine dati UddiDataSource facendo clic su **Verifica connessione** per eseguire il test della connessione all'origine dati.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Database (DB2 Instance - *istanza*)

Database (DB2 Instance - *istanza*) verifica lo stato del gestore DB2 dell'istanza DB2 su server di dati eseguendo lo script **db2status**.

## Risorse

Il test di Database (DB2 Instance - *istanza*) utilizza la seguente risorsa:

- L'*istanza* DB2 (su server di dati)

## Determinazione del problema

Se il test di Database (DB2 Instance - *istanza*) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni (dove il test è stato avviato) e server di dati (dove risiede il database). Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di dati da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che il file system sul sistema server di dati non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Accertarsi che i database utilizzati da server di dati siano avviati.
  - a. Su server di dati, eseguire il comando riportato di seguito da una finestra comandi in qualità di utente *istanza*, dove *istanza* è il nome dell'istanza DB2 indicata nel nome del test:

```
db2 get snapshot for dbm | grep status
```

Se il gestore database è avviato per *l'istanza*, viene visualizzato il seguente messaggio: Database manager status = Active.

5. Se i processi DB2 non sono in esecuzione, avviarli eseguendo **su - istanza** dalla finestra comandi (se l'esecuzione avviene come utente root). In caso contrario, eseguire **db2start** per avviare il gestore database.
6. Controllare i log DB2 per errori associati all'istanza database utilizzata per questo test. I log si trovano su server di dati nella directory `/datahome/istanza/sql1lib/db2dump`.
7. Controllare la presenza nel file `db2diag.log` di errori emessi durante l'avvio del database utilizzato per questo test.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.



## Test di Directory (UDDI V3 e UDDI V3 HTTPS)

Il test di Directory (UDDI V3 e UDDI V3 HTTPS) determina se è possibile accedere a WebSphere UDDI Registry utilizzando l'URL HTTP e HTTPS di WebSphere UDDI Registry.

### Risorse

Il test di Directory (UDDI V3 e UDDI V3 HTTPS) utilizza la seguente risorsa:

- WebSphere Application Server (su server delle applicazioni).

### Determinazione del problema

Se il test di Directory (UDDI V3 e UDDI V3 HTTPS) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di configurazione di WebSphere UDDI Registry riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log
2. Verificare che i file system sul sistema server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
    - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "cpudServer1". Sembra arrestato.`, avviare cpudServer1 utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "cpudServer1" è AVVIATO.`. Se è stato necessario avviare cpudServer1, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server cpudServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:




- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Il server cpudServer1 viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per il server delle applicazioni.
  - b. Visualizzare lo stato del server cpudServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Per arrestare il server cpudServer, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere alla console utente di WebSphere UDDI Registry dal sistema WebSphere Portal, su server delle applicazioni, utilizzando il seguente URL: `http://APPLICATION_SERVER_HOST:9080/uddigui/`, dove `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Diagnostica interna (Echo REST remoto)

Il test di Diagnostica interna (Echo REST remoto) verifica l'accesso a Remote Responder accedendo all'URL. Si tratta di una verifica diagnostica di Controllo di verifica del sistema e controlla i link tra i moduli Controllo di verifica del sistema.

### Risorse

Diagnostica interna (Echo REST remoto) utilizza le seguenti risorse:

- WebSphere Application Server (su server delle applicazioni).

### Determinazione del problema

Se il test di Diagnostica interna (Echo REST remoto) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server delle applicazioni, esaminare i log di configurazione di WebSphere UDDI Registry riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log
2. Verificare che il file system su server delle applicazioni non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come **ibmadmin**.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "cpudServer1". Sembra arrestato.`, avviare cpudServer1 utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "cpudServer1" è AVVIATO.`. Se è stato necessario avviare cpudServer1, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server cpudServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:




- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Il server cpudServer1 viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Accertarsi che il server cpudServer1 sia avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per il server delle applicazioni.
  - b. Visualizzare lo stato del server cpudServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.
    - L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.
    - L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.
    - L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. cpudServer1

Arrestare i server in questo ordine:

- a. cpudServer1
- b. agentnodo

Per arrestare il server cpudServer, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Verificare che sia possibile accedere alla console utente UDDI di WebSphere.
  - a. Su server delle applicazioni, accedere a `https://APPLICATION_SERVER_HOST:9080/uddigui/`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Broker)

Il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Broker) esegue una verifica delle funzioni di pubblicazione e di sottoscrizione di WebSphere Message Broker. Il test pubblica un messaggio sull'argomento con il nome JNDI elencato nelle proprietà come `jms/TopCatWmbPub`. WebSphere Message Broker riceve il messaggio e quindi pubblica un messaggio di ritorno sull'argomento `IOP.CAT.PUB`. Il test ha esito positivo se viene ricevuto il messaggio di risposta. Il test ha esito negativo se si verifica un errore o se il messaggio di risposta non viene ricevuto entro il periodo di timeout specificato nel file delle proprietà.

### Risorse

Il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Broker) utilizza le seguenti risorse:

- WebSphere Portal Server (su server delle applicazioni).
- WebSphere Message Queue (su server eventi).
- WebSphere Message Broker (su server eventi).

### Determinazione del problema

Se il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Broker) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server eventi. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve da e verso ciascun server. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system su server eventi e server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il gestore code WebSphere Message Queue e il broker WebSphere Message Broker siano in esecuzione.
  - a. Su server eventi, collegarsi come amministratore di WebSphere Message Queue. Ad esempio, `mqm`.
  - b. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`QMNAME(IOC.MB.QM) STATUS(Running)`
  - c. Se viene restituito uno stato diverso da `Running`, avviare il gestore code WebSphere Message Queue mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
  - d. Su server eventi, collegarsi come amministratore di WebSphere Message Broker. Ad esempio, `mqm`.
  - e. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`BIP1284I: broker 'IOC_BROKER' su gestore code 'IOC.MB.QM' in esecuzione.`
  - f. Se viene restituito uno stato diverso da `Running`, avviare il broker WebSphere Message Broker mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC\_BROKER**.
5. Controllare i file di log per errori. I file di log si trovano su server eventi nella directory `/var/log/messages`. Individuare i messaggi con il prefisso 'BIP'. Inoltre, ricercare i nomi delle code e la data e ora di esecuzione del test.

6. Se il broker o i gestori code non sembrano avviati, il loro avvio è possibile anche avviando server eventi ed eseguendo gli script di avvio del sistema.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Queue)

Il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Queue) esegue una verifica delle funzioni di pubblicazione e di sottoscrizione di WebSphere Message Queue. Il test crea un argomento specificato nelle proprietà. Quindi, il test pubblica un messaggio sull'argomento e tenta immediatamente di leggere il messaggio pubblicato. Il test ha esito positivo se è possibile leggere il messaggio inviato. Il test ha esito negativo se si verifica un errore o se il messaggio non può essere letto entro 15 secondi (15000 millisecondi).

## Risorse

Il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Queue) utilizza le seguenti risorse:

- WebSphere Portal Server (su server delle applicazioni).
- WebSphere Message Queue (su server eventi).

## Determinazione del problema

Se il test di Messaging (argomento Pubblica/Sottoscrivi di WebSphere Message Queue) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server eventi. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve da e verso ciascun server. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system sui server non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il gestore code WebSphere Message Queue sia in esecuzione.
  - a. Su server eventi, collegarsi come amministratore di WebSphere Message Queue. Ad esempio, `mqm`.
  - b. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`QMNAME(IOC.MB.QM) STATUS(Running)`
  - c. Se viene restituito uno stato diverso da `Running`, avviare il gestore code WebSphere Message Queue mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
5. Controllare i file di log per errori. I file di log si trovano su server eventi nella directory `/var/log/messages`. Individuare i messaggi con il prefisso 'BIP'. Inoltre, ricercare i nomi delle code e la data e ora di esecuzione del test.
6. Se il gestore code non sembra avviato, il relativo avvio è possibile anche avviando server eventi ed eseguendo gli script di avvio del sistema.



## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

### Test di Messaging (verifica installazione di WebSphere Message Broker/Queue)

Il test di Messaging (verifica installazione di WebSphere Message Broker/Queue) determina se è possibile accedere a WebSphere Message Queue and Message Broker. Ciò viene effettuato eseguendo il comando WebSphere Message Broker **mqsilist** sul sistema su cui è in esecuzione WebSphere Message Broker.

### Risorse

Messaging (verifica installazione di WebSphere Message Broker/Queue) utilizza le seguenti risorse:

- WebSphere Portal Server (su server delle applicazioni).
- WebSphere Message Queue and Message Broker (su server eventi).

### Determinazione del problema

Se il test di Messaging (verifica installazione di WebSphere Message Broker/Queue) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Controllare che vi sia una connettività di rete tra il sistema WebSphere Portal system (su server delle applicazioni) ed il sistema WebSphere Message Broker (su server eventi). Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server eventi da server delle applicazioni e viceversa. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system sui sistemi server delle applicazioni e server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il gestore code WebSphere Message Queue e il broker WebSphere Message Broker siano in esecuzione.
  - a. Su server eventi, collegarsi come amministratore di WebSphere Message Queue. Ad esempio, `mqm`.
  - b. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`QMNAME(IOC.MB.QM) STATUS(Running)`
  - c. Se viene restituito uno stato diverso da `Running`, avviare il gestore code WebSphere Message Queue mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
  - d. Su server eventi, collegarsi come amministratore di WebSphere Message Broker. Ad esempio, `mqm`.
  - e. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`BIP1284I: broker 'IOC_BROKER' su gestore code 'IOC.MB.QM' in esecuzione.`
  - f. Se viene restituito uno stato diverso da `Running`, avviare il broker WebSphere Message Broker mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC\_BROKER**.
5. Controllare i file di log per errori. I file di log si trovano su server eventi nella directory `/var/log/messages`. Individuare i messaggi con il prefisso 'BIP'. Inoltre, ricercare i nomi delle code e la data e ora di esecuzione del test.
6. Se il broker o i gestori code non sembrano avviati, il loro avvio è possibile anche avviando server eventi ed eseguendo gli script di avvio del sistema.



## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Messaging (coda WebSphere Message Broker/Queue)

Il test di Messaging (coda WebSphere Message Broker/Queue) esegue una verifica di WebSphere Message Queue inserendo un messaggio in una coda.

## Risorse

Il test di Messaging (coda WebSphere Message Broker/Queue) utilizza le seguenti risorse:

- WebSphere Portal Server (su server delle applicazioni).
- WebSphere Message Queue (su server eventi).
- WebSphere Message Broker (su server eventi).

## Determinazione del problema

Se il test di Messaging (coda WebSphere Message Broker/Queue) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server eventi. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve da e verso ciascun server. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system sui sistemi server delle applicazioni e server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Verificare che il gestore code WebSphere Message Queue e il broker WebSphere Message Broker siano in esecuzione.
  - a. Su server eventi, collegarsi come amministratore di WebSphere Message Queue. Ad esempio, `mqm`.
  - b. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`QMNAME(IOC.MB.QM) STATUS(Running)`
  - c. Se viene restituito uno stato diverso da `Running`, avviare il gestore code WebSphere Message Queue mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
  - d. Su server eventi, collegarsi come amministratore di WebSphere Message Broker. Ad esempio, `mqm`.
  - e. In una finestra comandi, eseguire **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. Viene visualizzato un messaggio simile a quello riportato di seguito:  
`BIP1284I: broker 'IOC_BROKER' su gestore code 'IOC.MB.QM' in esecuzione.`
  - f. Se viene restituito uno stato diverso da `Running`, avviare il broker WebSphere Message Broker mediante il seguente comando: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsi start IOC\_BROKER**.
5. Controllare i file di log per errori. I file di log si trovano su server eventi nella directory `/var/log/messages`. Individuare i messaggi con il prefisso 'BIP'. Inoltre, ricercare i nomi delle code e la data e ora di esecuzione del test.
6. Se il broker o i gestori code non sembrano avviati, il loro avvio è possibile anche avviando server eventi ed eseguendo gli script di avvio del sistema.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Monitoring (Netcool Impact Console)

Il test Monitoring (Netcool Impact Console) determina se Netcool Impact Console è in esecuzione ed è accessibile dall'URL di Netcool Impact Console.

## Risorse

Il test di Monitoring (Netcool Impact Console) utilizza la seguente risorsa:

- Netcool Impact Server (su server eventi)

## Determinazione del problema

Se il test di Monitoring (Netcool Impact Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server eventi, esaminare i log di Netcool Impact riportati di seguito:
    - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log
    - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
2. Verificare che i file system sul sistema server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che il server server1 sia avviato.
  - a. Sul sistema server eventi, collegarsi come wasadmin.
  - b. In una finestra comandi, eseguire: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password WAS\_ADMIN\_PWD, dove WAS\_ADMIN\_PWD è la password dell'amministratore WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente ADMU0509I: impossibile raggiungere il server "server1". Il server sembra arrestato. , avviare il server server1, che avvierà anche Netcool Impact Console Server, utilizzando il seguente comando: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: ADMU0508I: il server delle applicazioni "server1" è AVVIATO. Se è stato necessario avviare il server server1, verrà visualizzato un messaggio: ADMU3000I: Server server1 aperto per e-business; l'id processo è 26654.  
Il server server1 viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server eventi: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password WAS\_ADMIN\_PWD dove WAS\_ADMIN\_PWD è la password dell'amministratore WebSphere.
4. Accertarsi che sia possibile accedere a Netcool Impact Console da server eventi: http://EVENT\_SERVER\_HOST:9080/nci, dove EVENT\_SERVER\_HOST è il nome host di server eventi.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Monitoring (Netcool Omnibus)

Il test di Monitoring (Netcool Omnibus) determina se Netcool Omnibus è disponibile. Ciò viene effettuato eseguendo il comando **nco\_pa\_status -server NCO\_PA**.

### Risorse

Il test di Monitoring (Netcool Omnibus) utilizza la seguente risorsa:

- Netcool Omnibus Server (su server eventi)

### Determinazione del problema

Se il test di Monitoring (Netcool Omnibus) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server eventi. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server eventi da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Controllare che l'agent e i servizi del server Process Control siano in esecuzione.
  - a. Da una finestra comandi su server eventi, eseguire il comando **\$NCHOME/omnibus/bin/nco\_pa\_status -server NCO\_PA** come utente *netcool* Linux.
  - b. Se i servizi non sono avviati o in esecuzione, avviare il server eseguendo il comando **/etc/init.d/nco start** su server eventi come utente *root* Linux.
  - c. Se l'agent del processo non è in esecuzione, avviarlo eseguendo il comando **\$NCHOME/omnibus/bin/nco\_pad** su server eventi come utente *netcool* Linux.
3. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. In server eventi esaminare tutti i file di log che iniziano con NCO nelle seguenti directory:
    - `/opt/IBM/netcool/log`
    - `/opt/IBM/netcool/omnibus/log`
4. Verificare che i file system sul sistema server eventi non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
5. Accertarsi che sia possibile accedere al portlet Netcool Omnibus da server delle applicazioni: `http://EVENT_SERVER_HOST:9060/ibm/console`, dove `EVENT_SERVER_HOST` è il nome host di server eventi.

### Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Monitoring (Tivoli Composite Application Manager Agents - server)

Il test di Monitoring (Tivoli Composite Application Manager Agents - *server*) verifica se gli agent Tivoli Composite Application Manager sono in esecuzione eseguendo il comando **cinfo**.

### Risorse

Il test di Monitoring (Tivoli Composite Application Manager Agents - *server*) utilizza le seguenti risorse:

- Tivoli Composite Application Manager
  - Agent di Tivoli Composite Application Manager (su server delle applicazioni)

- Agent di Tivoli Composite Application Manager (su server eventi)
- Agent di Tivoli Composite Application Manager (su server di dati)
- Agent di Tivoli Composite Application Manager (su server di gestione)

## Determinazione del problema

Se il test di Monitoring (Tivoli Composite Application Manager Agents - *server*) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

### Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni, server di gestione, server eventi, e server di dati. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di gestione, server eventi e server di dati da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Accertarsi che i file system su server delle applicazioni, server di gestione, server eventi e server di dati non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Ripetere questa procedura su server delle applicazioni, server di gestione, server eventi e server di dati per accertarsi che i componenti di Tivoli Monitoring siano in esecuzione.
  - a. Collegarsi a una sessione di terminale sul server come root.
  - b. Eseguire il comando `/opt/IBM/ITM/bin/cinfo -r`. Verranno visualizzati risultati simili a quelli riportati di seguito. Gli agent differiranno sui diversi server. Gli agent devono avere uno stato di esecuzione (running).
 

```
***** Sun May 13 02:13:26 EDT 2012 *****
User: root Groups: root bin daemon sys adm disk wheel idldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
*****
Host      Prod   PID   Owner  Start  ID     ..Status
baapp2   lz     31042 root   May09  None  ...running
baapp2   ht     18755 root   May09  None  ...running
baapp2   yn     4190  root   02:11  None  ...running
```
  - c. Avviare eventuali agent Tivoli Composite Application Manager che non sono in esecuzione.
    - 1) Collegarsi a una sessione di terminale sul server come root.
    - 2) Eseguire `/opt/IBM/ITM/bin/itmcmd agent start PRODUCT_CODE` dove `PRODUCT_CODE` è il valore PID per un agent rilevato nei risultati del comando `/opt/IBM/ITM/bin/cinfo -o`.
5. Rivedere i file di log per le eccezioni.
  - a. Nel server di gestione, esaminare i log di Tivoli Enterprise Monitoring Server e Tivoli Enterprise Portal Server riportati di seguito:
    - Tivoli Enterprise Monitoring Server: `/opt/IBM/ITM/logs/*_CODICE_PRODOTTO_{nnnnnn}.log`
    - Tivoli Enterprise Portal Server: `/opt/IBM/ITM/logs/*_CODICE_PRODOTTO_{nnnnnn}.log`
 dove `CODICE_PRODOTTO` è il PID restituito dal comando `/opt/IBM/ITM/bin/cinfo -o`.

### Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

### Test di Monitoring (Tivoli Enterprise Monitoring Server)

Il test Monitoring (Tivoli Enterprise Monitoring Server) determina se Tivoli Enterprise Monitoring Server in esecuzione su server di gestione è disponibile. Una query che richiede lo stato del componente viene

inviata al server SOAP di Tivoli Monitoring Web Services. La query contiene un ID utente e una password non validi per il sistema. La risposta deve indicare che è stato utilizzato un ID o una password non valida. L'errore indica che Tivoli Enterprise Monitoring Server sta funzionando correttamente.

## Risorse

Il test di Monitoring (Tivoli Enterprise Monitoring Server) utilizza le seguenti risorse:

- Tivoli Enterprise Monitoring System (su server di gestione)
  - Tivoli Monitoring Web Services SOAP Server
  - Tivoli Enterprise Portal Server
  - Tivoli Enterprise Portal Server - Database DB2

## Determinazione del problema

Se il test di Monitoring (Tivoli Enterprise Monitoring Server) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Controllare che vi sia una connettività di rete tra server delle applicazioni e server di gestione. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server di gestione da server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. Su server di gestione, esaminare i seguenti file di log server di gestione:
    - Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log`
    - Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log`
    - Log incorporati di WebSphere Application Server:
      - Log di errori: `/opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
      - Log di output: `/opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`
      - Log di avvio: `/opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`
3. Accertarsi che i file system su server di gestione non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Accertarsi che i componenti Tivoli Monitoring siano in esecuzione su server di gestione.
  - a. Collegarsi a una sessione di terminale su server di gestione come root.
  - b. Eseguire il comando **`/opt/IBM/ITM/bin/cinfo -r`**.
5. Accertarsi che i database dei componenti Tivoli siano operativi.
  - a. Collegarsi a una sessione di terminale su server di gestione come `db2inst1`.
  - b. Eseguire il comando **`ps -ef | grep db2inst1`**.
  - c. Accertarsi che i processi DB2 siano in esecuzione. Essi includono `db2sysc`, `db2vend` e `db2acd`.
  - d. Se i processi DB2 non sono in esecuzione, eseguire il comando **`$> db2start`**.
  - e. Controllare i file di log DB2 su server di dati per eventuali errori di database relativi all'avvio di database utilizzati dai componenti Tivoli. I file di log si trovano nella directory `/datahome/db2inst1/sqllib/db2dump` su server di dati.
6. Nei risultati, verificare che Tivoli Enterprise Monitoring Server sia in esecuzione ricercando una voce per `ms`. Se la voce non è riportata, Tivoli Enterprise Monitoring Server non è in esecuzione.

7. Se Tivoli Enterprise Monitoring Server non è in esecuzione, avviare il server.
  - a. Collegarsi a una sessione di terminale su server di gestione come root.
  - b. Eseguire il comando `/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS`.
8. Nei risultati della procedura 4 a pagina 245, accertarsi che Tivoli Enterprise Portal Server sia in esecuzione ricercando una voce per cq. Se la voce non è riportata, Tivoli Enterprise Portal Server non è in esecuzione.
9. Se Tivoli Enterprise Portal Server non è in esecuzione, avviare il server.
  - a. Collegarsi a una sessione di terminale su server di gestione come root.
  - b. Eseguire il comando `/opt/IBM/ITM/bin/itmcmd agent start cq`.
10. Nei risultati della procedura 4 a pagina 245, accertarsi che altri componenti secondari validi siano in esecuzione.

Tabella 79. Componenti di Tivoli Monitoring

Componente	Descrizione
kf	Eclipse Help Server
cq	Tivoli Enterprise Portal Server
lz	Monitoring Agent for Linux OS
ms	Tivoli Enterprise Monitoring Server
yn	IBM Tivoli Composite Application Manager Agent for WebSphere Applications

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Monitoring (WebSphere Business Monitor Business Space Console)

Il test di Monitoring (WebSphere Business Monitor Business Space Console) determina se è possibile accedere a WebSphere Business Monitor Business Space utilizzando l'URL HTTP di WebSphere Business Monitor Business Space.

## Risorse

Il test di Monitoring (WebSphere Business Monitor Business Space Console) utilizza la seguente risorsa:

- WebSphere Application Server (su server delle applicazioni).

## Determinazione del problema

Se il test di Monitoring (WebSphere Business Monitor Business Space Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. Nel server delle applicazioni, esaminare i log di WebSphere Business Monitor riportati di seguito:
    - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. Verificare che i file system sul sistema server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando `df -h`.



3. Verificare che il server WebSphere Business Monitor sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "WBM_DE.AppTarget.WBMNode1.0". Sembra arrestato.` avviare `WBM_DE.AppTarget.WBMNode1.0` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "WBM_DE.AppTarget.WBMNode1.0" è AVVIATO.`. Se è stato necessario avviare `WBM_DE.AppTarget.WBMNode1.0`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server WBM_DE.AppTarget.WBMNode1.0 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:


- a. `agentnodo`
- b. `WBM_DE.AppTarget.WBMNode1.0`

Arrestare i server in questo ordine:

- a. `WBM_DE.AppTarget.WBMNode1.0`
- b. `agentnodo`


Il server `WBM_DE.AppTarget.WBMNode1.0` viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Verificare che il server WebSphere Business Monitor sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.
  - b. Visualizzare lo stato del server `WBM_DE.AppTarget.WBMNode1.0` facendo clic su **Server > Tipi di server > WebSphere Application Server**.  
L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.



L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. WBM\_DE.AppTarget.WBMNode1.0

Arrestare i server in questo ordine:

- a. WBM\_DE.AppTarget.WBMNode1.0
- b. agentnodo

Per arrestare il server WBM\_DE.AppTarget.WBMNode1.0, selezionarlo e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere a WebSphere Business Monitor Business Space dal sistema WebSphere Portal, su server delle applicazioni, utilizzando il seguente URL: `http://APPLICATION_SERVER_HOST:9084/BusinessSpace`, dove `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Monitoring (WebSphere Business Monitor Mobile Device Console)

Il test Monitoring (WebSphere Business Monitor Mobile Device Console) determina se è possibile accedere a WebSphere Business Monitor Mobile utilizzando l'URL HTTP di WebSphere Business Monitor Mobile.

## Risorse

Il test di Monitoring (WebSphere Business Monitor Mobile Device Console) utilizza la seguente risorsa:

- WebSphere Application Server (su server delle applicazioni).

## Determinazione del problema

Se il test di Monitoring (WebSphere Business Monitor Mobile Device Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. Nel server delle applicazioni, esaminare i log di WebSphere Business Monitor riportati di seguito:
    - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`

- /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM\_DE.AppTarget.WBMNode1.0/SystemErr.log
2. Verificare che i file system sul sistema server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
  3. Verificare che il server WebSphere Business Monitor sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
    - a. Sul sistema server delle applicazioni, collegarsi come `ibmadmin`.
    - b. In una finestra comandi eseguire `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
    - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
    - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "WBM_DE.AppTarget.WBMNode1.0". Sembra arrestato.` avviare `WBM_DE.AppTarget.WBMNode1.0` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "WBM_DE.AppTarget.WBMNode1.0" è AVVIATO.`. Se è stato necessario avviare `WBM_DE.AppTarget.WBMNode1.0`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server WBM_DE.AppTarget.WBMNode1.0 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `WBM_DE.AppTarget.WBMNode1.0`

Arrestare i server in questo ordine:

- a. `WBM_DE.AppTarget.WBMNode1.0`
- b. `agentnodo`

Il server `WBM_DE.AppTarget.WBMNode1.0` viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.


L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Verificare che il server WebSphere Business Monitor sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://APPLICATION_SERVER_HOST:9060/admin` utilizzando la password e l'ID admin di gestione di WebSphere Application Server. `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

- b. Visualizzare lo stato del server WBM\_DE.AppTarget.WBMNode1.0 facendo clic su **Server > Tipi di server > WebSphere Application Server**.

L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.

L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. WBM\_DE.AppTarget.WBMNode1.0

Arrestare i server in questo ordine:

- a. WBM\_DE.AppTarget.WBMNode1.0
- b. agentnodo

Per arrestare il server WBM\_DE.AppTarget.WBMNode1.0, selezionarlo e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server delle applicazioni: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere a WebSphere Business Monitor Mobile dal sistema WebSphere Portal, su server delle applicazioni, utilizzando il seguente URL: `http://APPLICATION_SERVER_HOST:9084/mobile`, dove `APPLICATION_SERVER_HOST` è il nome host per server delle applicazioni.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Policy (Tivoli Service Request Manager Maximo Console)

Il test Policy (Tivoli Service Request Manager Maximo Console) determina se è possibile accedere a Tivoli Service Request Manager Maximo utilizzando la pagina del centro di avvio Tivoli Service Request Manager Maximo Start Center.

## Risorse

Il test di Policy (Tivoli Service Request Manager Maximo Console) utilizza la seguente risorsa:

- Tivoli Service Request Manager Maximo (su server eventi).

## Determinazione del problema

Se il test di Policy (Tivoli Service Request Manager Maximo Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`

- b. Nel server eventi, esaminare i log di Tivoli Service Request Manager riportati di seguito:
  - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log
  - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log
2. Accertarsi che i file system sui sistemi server eventi e server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Verificare che il server Tivoli Service Request Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito sono riportate le procedure manuali:
  - a. Sul sistema server eventi, collegarsi come `ibmadmin`.
  - b. In una finestra comandi eseguire: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere "agentnodo" del server delle applicazioni. Il server sembra arrestato.`, avviare l'agent nodo utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: "agentnodo" del server delle applicazioni è AVVIATO.`. Se è stato necessario avviare l'agent del nodo, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: agent nodo server aperto per e-business; id processo 26654.`
  - a. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "MXServer1". Sembra arrestato.` avviare `MXServer1` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "MXServer1" è AVVIATO.`. Se è stato necessario avviare `MXServer1`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server MXServer1 aperto per e-business; id processo 26654.`

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. `agentnodo`
- b. `MXServer1`

Arrestare i server in questo ordine:

- a. `MXServer1`
- b. `agentnodo`

Il server `MXServer1` viene arrestato eseguendo il comando riportato di seguito in una finestra comandi su server eventi: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.


L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server eventi: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

4. Verificare che il server Tivoli Service Request Manager sia stato avviato. La verifica può essere effettuata utilizzando la console di gestione di WebSphere Application Server o mediante le procedure manuali. Di seguito è riportata la procedura utilizzando la console di gestione di WebSphere Application Server:
  - a. Accedere alla console di gestione di WebSphere Application Server all'indirizzo `http://EVENT_SERVER_HOST:9061/admin` utilizzando la password e l'ID `admin` di gestione di WebSphere Application Server. `EVENT_SERVER_HOST` è il nome host per server eventi.

- b. Visualizzare lo stato del server MXServer1 facendo clic su **Server > Tipi di server > WebSphere Application Server**.

L'icona  indica che il server è avviato. Se richiesto, selezionare il server e fare clic su **Riavvia** per riavviare il server.

L'icona  indica che il server è arrestato. Selezionare il server e fare clic su **Avvia** per avviare il server.

L'icona  indica che lo stato del server non è disponibile. L'agent del nodo potrebbe non essere in esecuzione. Per avviare l'agent del nodo, eseguire il comando `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` in una finestra comandi.

**Importante:** I server devono essere avviati e arrestati in un ordine specifico.

Avviare i server in questo ordine:

- a. agentnodo
- b. MXServer1

Arrestare i server in questo ordine:

- a. MXServer1
- b. agentnodo

Per arrestare il server MXServer1, selezionare il server e fare clic su **Arresta**.

L'agent del nodo viene arrestato digitando il seguente comando in una finestra comandi su server eventi: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` dove `WAS_ADMIN_PWD` è la password dell'amministratore di WebSphere.

5. Accertarsi che sia possibile accedere alla pagina del centro di avvio Tivoli Service Request Manager Maximo Start Center dal sistema WebSphere Portal, su server eventi, utilizzando il seguente URL: `http://EVENT_SERVER_HOST:31015/maximo/ui/login`, dove `EVENT_SERVER_HOST` è il nome host per server eventi. L'ID utente è maxadmin.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Security (Tivoli Access Manager)

Il test di Security (Tivoli Access Manager) determina se Tivoli Access Manager è in esecuzione inviando un comando `pd_start` da server di gestione e verificando i risultati.

## Risorse

Il test di Security (Tivoli Access Manager) utilizza la seguente risorsa:

- Tivoli Access Manager incluso i server di autorizzazione e della politica (su server di gestione)

## Determinazione del problema

Se il test di Security (Tivoli Access Manager) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Informazioni su questa attività

Nei passi riportati di seguito, `pdmgrd` è Tivoli Access Manager Authorization Server, `pdmgrproxyd` è Policy Proxy Server e `webseald-default` è Tivoli Access Manager WebSEAL Server.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. Nel server di gestione, esaminare i log di Tivoli Access Manager riportati di seguito:
    - /var/PolicyDirector/log/msg\_\_pdmgrd\_utf8.log
    - /var/PolicyDirector/log/msg\_\_pdacld\_utf8.log
  - b. Nel server delle applicazioni, esaminare i log di Tivoli Access Manager riportati di seguito:
    - /var/pdweb/log/msg\_\*.log dove \* è un qualsiasi valore.
    - /var/pdweb/log/config\_data\_\*.log dove \* è un qualsiasi valore.
2. Accertarsi che i file system sui sistemi server di gestione e server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Verificare che i componenti richiesti di Tivoli Access Manager siano in esecuzione.
  - a. Collegarsi a una sessione di terminale su server di gestione come root.
  - b. Eseguire il comando **pd\_start status**. I risultati saranno simili a quanto riportato di seguito:  
Server di Tivoli Access Manager

Server	Abilitato	In esecuzione
pdmgrd	yes	yes
pdacld	yes	yes
pdmgrproxyd	no	no

- c. Se i server pdmgrd o pdacld non sono in esecuzione, avviarli eseguendo il comando **pd\_start start**.
- Nota:** Solo i server pdmgrd e pdacld sono abilitati su server di gestione. Entrambi sono avviati con il comando **pd\_start start** e possono essere arrestati con il comando **pd\_start stop**.
4. Verificare che i componenti richiesti di WebSEAL di Tivoli Access Manager siano in esecuzione.
    - a. Collegarsi a una sessione di terminale su server delle applicazioni come root.
    - b. Eseguire il comando **pd\_start status**. I risultati saranno simili a quanto riportato di seguito:  
Server di Tivoli Access Manager

Server	Abilitato	In esecuzione
pdmgrd	no	no
pdacld	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. Se il server webseald-default non è in esecuzione, avviarlo eseguendo il comando **pd\_start start**.

**Nota:** Solo il server webseald-default è abilitato su server delle applicazioni. Esso è avviato con il comando **pd\_start start** e può essere arrestato con il comando **pd\_start stop**.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Security (Tivoli Access Manager Web Portal Manager)

Il test di Security (Tivoli Access Manager Web Portal Manager) determina se è possibile accedere all'applicazione Tivoli Access Manager Web Portal dall'URL dell'applicazione Tivoli Access Manager Web Portal.

## Risorse

Il test di Security (Tivoli Access Manager Web Portal Manager) utilizza la seguente risorsa:

- Tivoli Access Manager - Web Portal Manager (su server di gestione).



## Determinazione del problema

Se il test di Security (Tivoli Access Manager Web Portal Manager) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema di accesso.

### Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. In server delle applicazioni, esaminare i log di WebSphere Portal riportati di seguito:
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. Nel server di gestione, esaminare i log di Tivoli Access Manager - WebSphere Portal Manager riportati di seguito:
    - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
2. Verificare che i file system sul sistema server di gestione non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Accertarsi che Tivoli Access Manager - Web Portal Manager sia avviato.
  - a. Sul sistema server di gestione, collegarsi in qualità di `ibmadmin`.
  - b. In una finestra comandi, eseguire: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere Application Server.
  - c. Se viene visualizzato un messaggio simile al seguente: `ADMU0509I: impossibile raggiungere il server delle applicazioni "dmgr". Il server sembra arrestato.`, avviare `dmgr` utilizzando il seguente comando: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh`. Ignorare questa operazione se viene visualizzato un messaggio simile al seguente: `ADMU0508I: il server delle applicazioni "dmgr" è AVVIATO.`. Se è stato necessario avviare `dmgr`, verrà visualizzato un messaggio simile al seguente: `ADMU3000I: server dmgr aperto per e-business; id processo 26654.`

WebSphere Application Server Deployment Manager, compreso Tivoli Access Manager - Web Portal Manager, vengono arrestati eseguendo il comando riportato di seguito in una finestra comandi su server di gestione: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password WAS_ADMIN_PWD`, dove `WAS_ADMIN_PWD` è la password dell'amministratore WebSphere.
4. Accertarsi che sia possibile accedere a Tivoli Access Manager - Web Portal Manager dal sistema WebSphere Portal.
  - a. Su server di gestione, accedere al seguente indirizzo URL: `http://MANAGEMENT_SERVER_HOST9060/admin`, dove `MANAGEMENT_SERVER_HOST` è il nome host per server di gestione.
  - b. Fare clic su **Tivoli Access Manager > Web Portal Manager > Utenti > Cerca utenti**.
  - c. Collegarsi come utente `sec_master`.

### Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

### Test di Security (WebSEAL Console)

Il test di Security (WebSEAL Console) determina se Tivoli Access Manager e Tivoli Access Manager WebSEAL sono in esecuzione con le risorse richieste accedendo all'URL HTTP WebSEAL sulla porta 80 e si sta verificando la pagina restituita per la stringa "Intelligent Operations Center".



## Risorse

Il test di Security (WebSEAL Console) utilizza le seguenti risorse:

- Tivoli Access Manager incluso i server di autorizzazione e della politica (su server di gestione)
- Tivoli Access Manager WebSEAL (su server delle applicazioni)

## Determinazione del problema

Se il test di Security (WebSEAL Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Informazioni su questa attività

Nei passi riportati di seguito, pdmgrd è Tivoli Access Manager Authorization Server, pdmgrproxyd è Policy Proxy Server e webseald-default è Tivoli Access Manager WebSEAL Server.

## Procedura

1. Rivedere i file di log per le eccezioni di runtime.
  - a. Nel server di gestione, esaminare i log di Tivoli Access Manager riportati di seguito:
    - /var/PolicyDirector/log/msg\_\_pdmgrd\_utf8.log
    - /var/PolicyDirector/log/msg\_\_pdaclld\_utf8.log
  - b. Nel server delle applicazioni, esaminare i log di Tivoli Access Manager riportati di seguito:
    - /var/pdweb/log/msg\_\_\*.log dove \* è un qualsiasi valore.
    - /var/pdweb/log/config\_data\_\_\*.log dove \* è un qualsiasi valore.
2. Accertarsi che i file system sui sistemi server di gestione e server delle applicazioni non abbiano raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
3. Verificare che i componenti richiesti di Tivoli Access Manager siano in esecuzione.
  - a. Collegarsi a una sessione di terminale su server di gestione come root.
  - b. Eseguire il comando **pd\_start status**. I risultati saranno simili a quanto riportato di seguito:  
Server di Tivoli Access Manager

Server	Abilitato	In esecuzione
pdmgrd	yes	yes
pdaclld	yes	yes
pdmgrproxyd	no	no

- c. Se i server pdmgrd o pdaclld non sono in esecuzione, avviarli eseguendo il comando **pd\_start start**.

**Nota:** Solo i server pdmgrd e pdaclld sono abilitati su server di gestione. Entrambi sono avviati con il comando **pd\_start start** e possono essere arrestati con il comando **pd\_start stop**.

4. Verificare che i componenti richiesti di WebSEAL di Tivoli Access Manager siano in esecuzione.
  - a. Collegarsi a una sessione di terminale su server delle applicazioni come root.
  - b. Eseguire il comando **pd\_start status**. I risultati saranno simili a quanto riportato di seguito:  
Server di Tivoli Access Manager

Server	Abilitato	In esecuzione
pdmgrd	no	no
pdaclld	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. Se il server webseald-default non è in esecuzione, avviarlo eseguendo il comando **pd\_start start**.

**Nota:** Solo il server `webseald-default` è abilitato su server delle applicazioni. Esso è avviato con il comando `pd_start start` e può essere arrestato con il comando `pd_start stop`.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Web Server (IBM HTTP Server Console)

Il test di Web Server (IBM HTTP Server Console) verifica l'accesso a IBM HTTP Server accedendo all'URL di IBM HTTP Server.

## Risorse

Web Server (IBM HTTP Server Console) utilizza le seguenti risorse:

- IBM HTTP Server (su server delle applicazioni).

## Determinazione del problema

Se il test di Web Server (IBM HTTP Server Console) ha esito negativo, effettuare le seguenti operazioni per individuare e risolvere il problema.

## Procedura

1. Controllare che vi sia una connettività di rete con server delle applicazioni. Ciò può essere effettuato inviando i comandi **ping** sia con il nome host completo che con quello breve di server delle applicazioni. I risultati dei comandi **ping** mostreranno se il DNS o il file `/etc/hosts` stanno risolvendo correttamente il nome host.
2. Rivedere i file di log per le eccezioni di runtime.
  - a. Nel server delle applicazioni, esaminare i log di IBM HTTP riportati di seguito:
    - `/opt/IBM/HTTPServer/logs/error_log`
    - `/opt/IBM/HTTPServer/logs/access_log`
3. Verificare che il file system su server delle applicazioni non abbia raggiunto la capacità massima. Ciò può essere determinato utilizzando il comando **df -h**.
4. Accertarsi che sia possibile accedere alla pagina predefinita di IBM HTTP Server dal sistema WebSphere Portal.
  - a. Su server delle applicazioni, accedere a `https://APPLICATION_SERVER_HOST:82/`, dove `APPLICATION_SERVER_HOST` è il nome host di server delle applicazioni.
  - b. Se non è possibile accedere alla pagina predefinita, eseguire il comando **ps -ef | grep HTTPServer** per determinare se i processi IBM HTTP Server sono in esecuzione. I processi IBM HTTP Server iniziano con `/opt/IBM/HTTPServer/bin/httpd`. Esistono sette processi.
  - c. Se una parte dei processi è in esecuzione, arrestare tali processi prima di riavviare tutti i processi.
    - 1) Sul sistema server delle applicazioni, collegarsi come root.
    - 2) Passare alla directory `/opt/IBM/HTTPServer/bin`.
    - 3) Eseguire i comandi riportati di seguito per arrestare tutti i processi IBM HTTP in esecuzione:

```
./apachectl stop
./adminctl stop
```
    - 4) Verificare che tutti i processi siano stati arrestati eseguendo il comando **ps -ef | grep HTTPServer**.
    - 5) Se alcuni processi IBM HTTP Server sono ancora in esecuzione, arrestarli utilizzando il comando **kill -9 pid** dove `pid` è l'identificativo del processo di IBM HTTP Server.
  - d. Se i processi HTTP Server non sono in esecuzione, avviare i componenti IBM HTTP Server.
    - 1) In server delle applicazioni, collegarsi come root.
    - 2) Passare alla directory `/opt/IBM/HTTPServer/bin`.

- 3) Eseguire i comandi riportati di seguito per avviare tutti i processi IBM HTTP in esecuzione:  
./adminctl start  
./apachectl start
- 4) Verificare che tutti i processi siano stati avviati eseguendo il comando **ps -ef | grep HTTPServer**.

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Intelligent Operations Center - Flusso di eventi

Il test di Intelligent Operations Center - Flusso di eventi verifica se i componenti critici correlati ai processi evento IBM Intelligent Operations Center funzionano come previsto. Ciò viene effettuato simulando gli eventi esterni e determinando se i risultati sono quelli previsti.

## Risorse

Il test Intelligent Operations Center - Flusso di eventi utilizza le seguenti risorse:

- IBM WebSphere Message Broker (sul server delle applicazioni).
- IBM WebSphere Message Queue (sul server delle applicazioni).
- IBM Netcool/OMNIBus (sul server eventi).
- IBM Netcool/Impact (sul server eventi).
- IBM DB2 (sul server di dati).

## Individuazione del problema

Se il test Intelligent Operations Center - Flusso di eventi non riesce fare quanto segue per individuare e risolvere il problema di accesso.

## Procedura

1. Accertarsi che i componenti IBM Intelligent Operations Center siano in esecuzione.
  - a. In una finestra comandi su server di gestione, eseguire **/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password**, dove *password* è la password dell'amministratore IBM Intelligent Operations Center definita quando IBM Intelligent Operations Center è stato distribuito.
  - b. Se esistono dei componenti che non sono in esecuzione, avviarli eseguendo **/opt/IBM/ISP/mgmt/scripts/IOControl.sh start ID\_componente password**, dove *password* è la password dell'amministratore IBM Intelligent Operations Center definita quando IBM Intelligent Operations Center è stato distribuito e *ID\_componente* è un ID riportato in opzioni di destinazione quando si esegue **/opt/IBM/ISP/mgmt/scripts/IOControl.sh help**.
2. Esaminare il log Netcool/OMNIBus (/opt/IBM/netcool/omnibus/log/ioc\_xml.log) su server eventi per eventuali errori.
3. Se necessario, avviare l'indagine di Tivoli Netcool/OMNIBus eseguendo quanto segue su server eventi.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log  
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linuxx86/ioc_xml.props &
```

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

## Test di Intelligent Operations Center - Flusso di notifiche

Il test Intelligent Operations Center - Flusso di notifiche verifica se i componenti critici correlati ai processi di notifica IBM Intelligent Operations Center funzionano come previsto. Ciò viene effettuato simulando le notifiche esterne e determinando se i risultati sono quelli previsti.

## Risorse

Il test di Intelligent Operations Center - Flusso di notifiche utilizza le seguenti risorse:

- IBM WebSphere Message Queue (su server delle applicazioni).
- IBM Netcool/OMNIBus (su the server eventi).
- IBM Netcool/Impact (su server eventi).
- IBM DB2 (su server di dati).

## Individuazione del problema

Se il test Intelligent Operations Center - Flusso di notifiche non riesce fare quanto segue per individuare e risolvere il problema di accesso.

## Procedura

1. Accertarsi che i componenti IBM Intelligent Operations Center siano in esecuzione.
  - a. In una finestra comandi su server di gestione, eseguire **`/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password`**, dove *password* è la password dell'amministratore IBM Intelligent Operations Center definita quando IBM Intelligent Operations Center è stato distribuito.
  - b. Se esistono dei componenti che non sono in esecuzione, avviarli eseguendo **`/opt/IBM/ISP/mgmt/scripts/IOControl.sh start ID_componente password`**, dove *password* è la password dell'amministratore IBM Intelligent Operations Center definita quando IBM Intelligent Operations Center è stato distribuito e *ID\_componente* è un ID riportato in Opzioni di destinazione quando si esegue **`/opt/IBM/ISP/mgmt/scripts/IOControl.sh help`**.
2. Esaminare il log Netcool/OMNIBus (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) su server eventi per eventuali errori.
3. Se necessario, avviare l'indagine di Tivoli Netcool/OMNIBus eseguendo quanto segue su server eventi.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

## Operazioni successive

Risolvere eventuali problemi o errori rilevati e riprovare il test.

---

## Capitolo 7. Manutenzione della soluzione

Eseguire le attività descritte in questa sezione per mantenere facilmente la soluzione in esecuzione.

---

### Esecuzione backup dei dati

Per evitare la perdita di dati importanti in IBM Intelligent Operations Center, eseguire, ad intervalli regolari, il backup di alcuni file, directory e database.

Quando si opera un'estensione IBM Intelligent Operations Center, è buona norma sviluppare una procedura di backup per gli elementi aggiunti, ad esempio:

- Report
- Database ausiliari
- Tabelle di database
- Analisi personalizzate
- Portlet
- Applicazioni Java

Considerare anche i dati che sono stati raccolti, ad esempio:

- Dati del database CAP (Common Access Protocol)
- Dati di database IBM WebSphere Business Monitor
- Dati registro utenti LDAP (Lightweight Directory Access Protocol)
- Dati GIS (Geographical Information System)

Adottare la convenzione di denominazione per rendere più facile l'identificazione delle estensioni aggiunte. In generale, tenere traccia dei dati creati o raccolti da quando si è installata la soluzione originale. Implementare le procedure per eseguire il backup dei dati in modo che quando si aggiorna la soluzione, non si perdono dati importanti.

### Esecuzione backup dei database

La seguente tabella elenca i database per i quali è consigliabile eseguire il backup in IBM Intelligent Operations Center.

Tabella 80. Database IBM Intelligent Operations Center

Servizio o componente	Istanza di database	Nomi database	Server
Intelligent Operations Center Database	db2inst1	<ul style="list-style-type: none"><li>• IOCDB</li></ul>	Server di dati
Portale	db2inst2	<ul style="list-style-type: none"><li>• CUSTDB</li><li>• FDBKDB</li><li>• LKMDDB</li><li>• JCRDB</li><li>• COMMDB</li><li>• RELDB</li></ul>	Server di dati
Business intelligence	db2inst3	<ul style="list-style-type: none"><li>• CXLOGDB</li><li>• CXCONTDB</li></ul>	Server di dati

Tabella 80. Database IBM Intelligent Operations Center (Continua)

Servizio o componente	Istanza di database	Nomi database	Server
Regola business e monitoraggio attività business	db2inst4	<ul style="list-style-type: none"> <li>• UDDIDB</li> <li>• WODMDCDB</li> <li>• MONITOR</li> <li>• WBMDB</li> <li>• RESDB</li> </ul>	Server di dati
Modello semantico	db2inst5	<ul style="list-style-type: none"> <li>• JTS</li> <li>• IIC</li> </ul>	Server di dati
Gestione richiesta di servizio	db2inst6	<ul style="list-style-type: none"> <li>• MAXIMO</li> </ul>	Server di dati
Gestione identità	db2inst7	<ul style="list-style-type: none"> <li>• TIMDB</li> </ul>	Server di dati
Applicazioni	db2inst8	<ul style="list-style-type: none"> <li>• LDAPDB</li> <li>• LDAPDB2B</li> </ul>	Server di dati

## Creazione istantanee dell'infrastruttura virtuale

La maggior parte delle infrastrutture virtuali dispongono di una funzione di istantanea che preserva lo stato e i dati dell'ambiente virtuale ad un determinato momento. È fortemente raccomandato eseguire un'istantanea del proprio ambiente prima di eseguire modifiche significative. Sono disponibili molti strumenti di gestione dell'infrastruttura virtuale la maggior parte dei quali dispone di una propria implementazione di una funzione di istantanea. È importante acquisire dimestichezza con i requisiti e le istruzioni specifici per eseguire correttamente il backup dell'ambiente virtuale leggendo attentamente le istruzioni nella guida alla gestione fornita dal fornitore dell'infrastruttura virtuale.

### Attività correlate:

“Backup prima della personalizzazione KPI” a pagina 172

Backup e ripristino KPI che sono stati creati o modificati con IBM WebSphere Business Monitor o con il portlet KPI (Key Performance Indicators).

### Informazioni correlate:

 [IBM Smarter Cities Software Solutions Redbooks](#)

## Ottimizzazione delle prestazioni

Le seguenti sezioni descrivono come ottimizzare server delle applicazioni e WebSphere Application Server.

### Informazioni correlate:

 [IBM Websphere Portal V 7.0 Performance Tuning Guide](#)

 [Centro informazioni di IBM Websphere Application Server, Network Deployment, Versione 7.0](#)

## Ottimizzazione di server delle applicazioni

### Informazioni su questa attività

Utilizzare le seguenti linee guida che si basano sui risultati dei test delle prestazioni per impostare la dimensione dell'heap della Java virtual machine

## Procedura

1. Impostare le dimensioni minima e massima dell'heap sullo stesso valore.
2. Impostare la dimensione heap su un valore compatibile con la memoria fisica e che sia superiore a 2 GB.

## Operazioni successive

Per ulteriori informazioni, consultare il link correlato alla fine dell'argomento.

## Ottimizzazione di WebSphere Application Server

Per informazioni relative all'ottimizzazione delle prestazioni di WebSphere Application Server Versione 7, consultare il link correlato alla fine dell'argomento.

---

## Gestione file di log

IBM Intelligent Operations Center memorizza i file di log in varie diverse ubicazioni. Per evitare problemi di prestazioni del sistema, periodicamente archiviare i file di log e rimuovere i file di log originali.

Se non vengono gestiti i file di log e il numero di file di log aumenta indefinitamente, i file di log possono probabilmente riempire una partizione del file system. Il riempimento della partizione del file system potrebbe avere conseguenze negative e potenzialmente causare l'arresto del sistema.

Per le informazioni relative ai file di log disponibili in IBM Intelligent Operations Center, consultare il link alla fine di questo argomento.

### Concetti correlati:

“Risoluzione dei problemi dei componenti” a pagina 300

È possibile utilizzare lo strumento Controllo di verifica del sistema per risolvere i problemi dei componenti in IBM Intelligent Operations Center.

---

## Aggiornamento del token LTPA per SSO (single sign-on)

IBM Intelligent Operations Center utilizza un token LTPA (Lightweight Third-Party Authentication) per abilitare il SSO (single sign-on) attraverso diversi servizi. Il token e chiavi generate durante l'installazione non scadono. È buona prassi di sicurezza rigenerare periodicamente il token LTPA e aggiornare i servizi che lo utilizzano.

## Prima di iniziare

Il prodotto IBM Intelligent Operations Center deve essere installato e tutti i servizi avviati prima di aggiornare il token LTPA.

Questa procedura richiede che tutti i servizi siano stati arrestati e avviati, quindi l'aggiornamento non deve essere eseguito quando il sistema è in produzione. Tutti gli utenti collegati al sistema sperimenterebbero un'interruzione del servizio e potrebbe determinare una perdita di dati.

## Procedura

Creazione di un nuovo token LTPA per server delle applicazioni

1. In server delle applicazioni aprire un browser Web e andare all'indirizzo `http://application_host:9060/ibm/console` dove `application_host` è il nome host di server delle applicazioni.
2. Collegarsi come utente `webwasadmin` con la password specificata nel parametro `WAS.ADMIN.ACCOUNT.PWD` del file delle proprietà della topologia.
3. Fare clic su **Sicurezza > Sicurezza globale > Meccanismi di autenticazione e scadenza > LTPA > Genera chiavi**.



4. Immettere due volte una password per il nuovo token LTPA. La password viene utilizzata per codificare il token LTPA. Questa password verrà utilizzata durante l'importazione del token LTPA. Registrare la password come parametro WAS.LTPA.PWD nel file delle proprietà della topologia.
5. Immettere il percorso e il nome file con cui il token LTPA verrà salvato, ad esempio, /tmp/newapp.ltpa. Se si specifica un percorso oppure un nome del file diverso, inserire il proprio percorso e il nome file per /tmp/newapp.ltpa nella parte rimanente di questa procedura.
6. Fare clic su **Esporta chiavi**. Il nuovo token LTPA viene salvato come /tmp/newapp.ltpa.
7. Fare clic su **Messaggi > Salva**. Gli aggiornamenti verranno salvati. Ignorare eventuali avvertenze relative al dominio SSO non definito.

Copiare il nuovo token LTPA nel server eventi.

8. Accedere a server delle applicazioni come utente root e aprire una finestra terminale.
9. Eseguire il comando **cp /tmp/newapp.ltpa /tmp/stproxy.ltpa**. Questa operazione sostituisce il file creato al momento dell'installazione di IBM Intelligent Operations Center.
10. Eseguire il comando **scp /tmp/newapp.ltpa root@event\_host :/tmp/newapp.ltpa** dove *event\_host* è il nome host del server eventi. Quando richiesto, immettere la password del root del server eventi. Il token LTPA viene copiato nel server eventi.

Importazione del nuovo token LTPA

11. Nel server eventi aprire un browser Web e andare all'indirizzo `http://event_host:9061/ibm/console` dove *event\_host* è il nome host completo di server eventi.
12. Collegarsi come utente `webwasadmin` con la password specificata nel parametro `TSRM.WAS.ADMIN.PWD` del file delle proprietà della topologia.
13. Fare clic **Sicurezza > Gestione sicura, applicazioni e infrastruttura > Meccanismi di autenticazione e scadenza**.
14. Immettere la password per il token LTPA e /tmp/newapp.ltpa per il nome file.
15. Fare clic su **Importa chiavi**.
16. Fare clic su **Messaggi > Salva**. Gli aggiornamenti verranno salvati.

Creazione di un nuovo token LTPA per server eventi.

17. Fare clic su **Meccanismi di autenticazione e scadenza > Genera chiavi**.
18. Immettere due volte una password per il nuovo token LTPA. Questa password verrà utilizzata durante l'importazione del token LTPA.
19. Immettere il percorso e il nome file con cui il token LTPA verrà salvato, ad esempio, /tmp/newevent.ltpa. Se si specifica un percorso oppure un nome del file diverso, inserire il proprio percorso e il nome file per /tmp/newevent.ltpa nella parte rimanente di questa procedura.
20. Fare clic su **Esporta chiavi**. Il nuovo token LTPA viene salvato come /tmp/newevent.ltpa.

Copiare il nuovo token LTPA del server eventi nel server delle applicazioni.

21. Accedere a server delle applicazioni come utente root e aprire una finestra terminale.
22. Eseguire il comando **scp /tmp/newevent.ltpa root@event\_host :/tmp/newevent.ltpa** dove *event\_host* è il nome host del server eventi. Quando richiesto, immettere la password del root del server eventi. Il token LTPA viene copiato nel server eventi.

Aggiornare il servizio di sicurezza con il nuovo token LTPA.

23. Accedere a server delle applicazioni come utente root e aprire una finestra terminale.
24. Eseguire il comando **cp /tmp/newapp.ltpa /opt/pdweb/etc/**.
25. Eseguire il comando **cp /tmp/newevent.ltpa /opt/pdweb/etc/**.
26. Creare un file di comandi denominato /tmp/pd.com contenente i seguenti comandi:

```
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task default-webseald-application_host create -t tcp -h application_host -p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task default-webseald-application_host create -t tcp -h event_host -p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsm
```

Dove:

*application\_host*

è il nome host completo del server delle applicazioni.

*event\_host*

è il nome host completo del server eventi.

*appLTPApw*

è la password specificata durante la creazione del token LTPA per il server delle applicazioni.

*eventLTPApw*

è la password specificata durante la creazione del token LTPA per il server eventi.

27. Eseguire il comando `/opt/PolicyDirector/bin/pdadmin -a sec_master -p password / tmp/pd.com`, dove *password* è la password definita nel parametro TAM.WEBSEAL.ADMIN.PWD del proprietà file della topologia.

Aggiornamento del servizio single sign-on per il servizio di collaborazione.

28. Seguire la procedura in “Configurazione di SSO (Single Sign-On) per i servizi di collaborazione” a pagina 54 per aggiornare il single sign-on del servizio di collaborazione.

Arrestare e riavviare tutti i servizi.

29. L'utilizzo dello Strumento di controllo della piattaforma arresta tutti i servizi.

30. L'utilizzo dello Strumento di controllo della piattaforma avvia tutti i servizi. I token LTPA verranno propagati a tutti i servizi.

---

## Suggerimenti per la manutenzione

Ulteriori suggerimenti per la manutenzione della soluzione vengono descritti sotto forma di singole note tecniche nel portale di supporto IBM.

Il seguente link avvia una query personalizzata di Support knowledge base attivo tutte le versioni di IBM Intelligent Operations Center: Visualizza tutti i suggerimenti di manutenzione per IBM Intelligent Operations Center.



---

## Capitolo 8. Utilizzo dell'interfaccia di soluzioni

IBM Intelligent Operations Center è una soluzione basata su Web che utilizza la tecnologia di portale. L'accesso alla soluzione è consentito con qualunque browser Web supportato.

Per avere informazioni sui browser Web supportati, consultare il link alla fine dell'argomento.

### Informazioni correlate:



Browser supportati da IBM Intelligent Operations Center

---

## Collegamento

Collegarsi per accedere all'interfaccia utente di IBM Intelligent Operations Center.

### Prima di iniziare

Contattare l'amministratore locale per ottenere l'ID utente e la password. L'amministratore è responsabile affinché venga garantito il livello di accesso sicurezza appropriato per il proprio ruolo nell'organizzazione. L'amministratore, inoltre, fornirà all'utente l'URL dell'indirizzo Web per l'accesso al portale della soluzione.

### Informazioni su questa attività

Utilizzare la seguente procedura per avviare una nuova sessione del browser e per accedere a IBM Intelligent Operations Center. È possibile inoltre accedere alla soluzione da altro software IBM Smarter Cities Software Solutions installato nel proprio ambiente. Dalla barra di navigazione principale nella parte superiore del portale, selezionare **Intelligent Operations Center**.

### Procedura

1. Immettere l'URL nel campo dell'indirizzo del browser.

**Nota:** Il nome dominio completo è necessario nell'URL, ad esempio `http://nomehost_server_applicazioni/wpsv70/wps/myportal`. Se si utilizza l'indirizzo IP invece del dominio completo registrato, alcuni portlet non vengono visualizzati correttamente.

2. Nella pagina di login, immettere i propri ID utente e password.
3. Fare clic su **Accedi**.

### Risultati

Vengono visualizzati solo le pagine, le funzioni ed i dati per cui si dispone di autorizzazione di accesso. Rivolgersi all'amministratore per richiedere ulteriori autorizzazioni di accesso.

#### Attività correlate:

“Scollegamento”

Scollegarsi per uscire dall'interfaccia utente di IBM Intelligent Operations Center e per terminare la sessione del server. Per impostazione predefinita, il link di **scollegamento** si trova nell'angolo in alto a destra di IBM Intelligent Operations Center.

---

## Scollegamento

Scollegarsi per uscire dall'interfaccia utente di IBM Intelligent Operations Center e per terminare la sessione del server. Per impostazione predefinita, il link di **scollegamento** si trova nell'angolo in alto a destra di IBM Intelligent Operations Center.

#### Attività correlate:

“Collegamento” a pagina 265

Collegarsi per accedere all'interfaccia utente di IBM Intelligent Operations Center.

---

## Visualizzazione o modifica del profilo utente

È possibile visualizzare o modificare le informazioni nel proprio profilo utente per IBM Intelligent Operations Center.

### Informazioni su questa attività

Il profilo contiene informazioni immesse precedentemente dall'utente o dall'amministratore. È possibile aggiornare il profilo modificando le informazioni nei campi degli attributi. Ad esempio, è possibile modificare la password esistente in una nuova.

Tabella 81. Attributi del profilo utente IBM Intelligent Operations Center

Attributo	Descrizione	Modifiche consentite dall'utente?
ID utente*	L'amministratore assegna un ID a ciascun nuovo utente per scopi di identificazione.	No
Password*	Una password viene assegnata dall'amministratore per la sicurezza. La password deve essere univoca e avere una lunghezza compresa tra 5 e 60 caratteri. Le password valide devono contenere solo i caratteri a-z, A-Z, punto ".", trattino "-" e sottolineatura "_".	Sì
Nome	Un nome può essere immesso dall'amministratore o dall'utente.	Sì
Cognome*	Un cognome viene immesso dall'amministratore.	Sì
Email	Un indirizzo email può essere immesso dall'amministratore o dall'utente.	Sì

**Nota:** Gli attributi contrassegnati con un asterisco sono obbligatori per la corretta creazione di un nuovo utente. Gli attributi non contrassegnati da un asterisco sono facoltativi.

### Procedura

1. A destra della barra di navigazione in alto, selezionare **Modifica profilo personale**. Vengono visualizzati gli attributi per il proprio profilo.
2. Per modificare la password:
  - a. Immettere la password corrente (il testo della password non viene visualizzato).
  - b. Nei campi **Nuova password** e **Conferma password**, immettere la nuova password.
3. Immettere o modificare le informazioni in qualsiasi campo tra quelli rimanenti.
4. Per inoltrare le modifiche, fare clic su **OK**.

## Risultati

Il proprio profilo utente viene aggiornato con le modifiche eventualmente apportate.

## Utilizzo di pagine

Una pagina è composta da uno o più portlet complementari. Mediante l'utilizzo di IBM Intelligent Operations Center è possibile interagire con i portlet su una pagina per accedere alle informazioni richieste e per rispondere agli eventi in base alle esigenze.

IBM Intelligent Operations Center fornisce sei viste di pagine di esempio di tipo diverso.

**Importante**

Se si dispone dell'accesso da amministratore, nella vista della pagina, è possibile accedere al servizio per la gestione delle pagine del portale. È possibile modificare una pagina o creare una nuova pagina. Fare clic sul lato destro della scheda del nome della pagina e selezionare un'opzione dal menu della pagina. Per ulteriori informazioni, consultare il link alla fine dell'argomento.

### Attività correlate:

“Creazione e personalizzazione di una pagina” a pagina 145

È possibile creare nuove pagine da includere in IBM Intelligent Operations Center e specificare quali portlet visualizzare in quelle pagine. È possibile personalizzare l'aspetto e il layout dei portlet inclusi in ogni pagina.

## Vista Supervisore: Stato

Utilizzare la vista Supervisore: Stato per ottenere una vista consolidata degli indicatori KPI (Key Performance Indicator) e degli eventi chiave. La vista Supervisore: Stato consente agli utenti con responsabilità nell'organizzazione di monitorare, gestire e rispondere alle modifiche di stato in relazione alle aree principali del bilancio e delle prestazioni organizzative.

La vista Supervisore: Stato è una pagina Web interattiva. La pagina contiene i portlet elencati nella Tabella 82. I portlet sono sezioni indipendenti della pagina interconnesse tra loro per fornire informazioni dettagliate e interazioni a livello esecutivo.

Tabella 82. Portlet della vista Supervisore: Stato

Portlet	Descrizione
“Stato” a pagina 291	Il portlet Stato fornisce un riepilogo di livello esecutivo dello stato degli indicatori KPI sulle organizzazioni per le quali si dispone dell'autorizzazione di visualizzazione. Utilizzare questo portlet per visualizzare modifiche aggiornate nello stato KPI, in modo che sia possibile pianificare e intraprendere eventuali azioni se necessario.
“Drill Down KPI (Key Performance Indicator)” a pagina 275	Per concentrarsi su una specifica categoria KPI nel portlet Drill Down KPI (Key Performance Indicator), fare clic sulla categoria nel portlet Stato. Questa categoria viene quindi visualizzata autonomamente nel portlet Drill Down KPI (Key Performance Indicator). È possibile utilizzare l'elenco per esaminare gli indicatori KPI sottostanti fino a quando si raggiungono i dettagli del KPI che ha causato la modifica dello stato.

Tabella 82. Portlet della vista Supervisore: Stato (Continua)

Portlet	Descrizione
“Notifiche” a pagina 287	Il portlet Notifiche fornisce un elenco interattivo e dinamico di avvisi determinato dalle modifiche degli indicatori KPI e degli eventi correlati. Lo scopo di questo portlet è di evidenziare le modifiche allo stato eventi o KPI. L'elenco contiene i dettagli chiave per ciascuno degli avvisi. Ad esempio quando un KPI cambia lo stato da giallo a rosso, viene inviato un avviso al portlet Notifiche.
“Attività personali” a pagina 284	Un utente collegato può visualizzare le attività che gli sono state assegnate nel portlet Attività personali. Nel portlet Attività personali, le attività vengono raggruppate dalle rispettive procedure operative standard principali. Ogni procedura operativa standard corrisponde a un singolo evento.
“Contatti” a pagina 271	Il portlet Contatti può visualizzare un elenco dei contatti organizzati per categoria. È possibile organizzare i contatti in categorie basate sulle persone con cui è necessario comunicare. Ad esempio, è possibile creare una categoria per i contatti di lavoro generali e un'altra categoria per i contatti di lavoro del progetto. Con il portlet Contatti è possibile comunicare con le persone e modificare i gruppi, i contatti o il proprio stato in linea.

## Vista Supervisore: Operazioni

Utilizzare la vista Supervisore: Operazioni per ottenere una panoramica degli eventi mentre accadono. La vista Supervisore: Operazioni è rivolta ai supervisori e ai responsabili che monitorano gli eventi correnti e pianificano gli eventi futuri.

La vista Supervisore: Operazioni è una pagina Web interattiva. La pagina contiene i portlet elencati in Tabella 83. I portlet sono sezioni indipendenti della pagina interconnesse tra loro per fornire informazioni esaurienti e interazioni a livello manageriale.

Tabella 83. Portlet della vista Supervisore: Operazioni

Portlet	Descrizione
“Mappa” a pagina 279	<p>Una mappa della regione geografica con i contrassegni di risorse e di eventi.</p> <p>Un modulo filtro per la selezione di categorie di eventi da mostrare sulla mappa e nei portlet collegati al portlet Mappa.</p> <p>Un modulo filtro per la selezione di funzionalità di risorse da mostrare sulla mappa e nella scheda <b>Risorse</b> sul portlet Dettagli collegato. Per visualizzare questo modulo, selezionare prima <b>Visualizza risorse vicine</b> sul portlet Dettagli.</p>
“Dettagli” a pagina 272	Dettagli è un portlet di elenco interattivo. Tutti gli eventi per cui è stata concessa la visualizzazione sono visibili nell'elenco di eventi e su qualsiasi portlet di mappe collegato al portlet Dettagli.



Tabella 83. Portlet della vista Supervisore: Operazioni (Continua)

Portlet	Descrizione
“Notifiche” a pagina 287	Il portlet Notifiche fornisce un elenco interattivo e dinamico di avvisi determinato dalle modifiche degli indicatori KPI e degli eventi correlati. Lo scopo di questo portlet è di evidenziare le modifiche allo stato eventi o KPI. L'elenco contiene i dettagli chiave per ciascuno degli avvisi. Ad esempio, quando si verificano incidenti correlati all'interno di un'area definita, viene inviato un avviso al portlet Notifiche.
“Attività personali” a pagina 284	Un utente collegato può visualizzare le attività che gli sono state assegnate nel portlet Attività personali. Nel portlet Attività personali, le attività vengono raggruppate dalle rispettive procedure operative standard principali. Ogni procedura operativa standard corrisponde a un singolo evento.
“Contatti” a pagina 271	Il portlet Contatti può visualizzare un elenco dei contatti organizzati per categoria. È possibile organizzare i contatti in categorie basate sulle persone con cui è necessario comunicare. Ad esempio, è possibile creare una categoria per i contatti di lavoro generali e un'altra categoria per i contatti di lavoro del progetto. Con il portlet Contatti è possibile comunicare con le persone e modificare i gruppi, i contatti o il proprio stato in linea.

## Vista Operatore: Operazioni

Utilizzare la vista Operatore: Operazioni per conservare la disponibilità di eventi e della relativa ubicazione. La vista Operatore: Operazioni è rivolta a operatori, responsabili o ad altre persone che monitorano e rispondono agli eventi correnti.

La vista Operatore: Operazioni è una pagina Web interattiva. La pagina contiene i portlet elencati in Tabella 84. I portlet sono sezioni indipendenti della pagina interconnesse tra loro per fornire informazioni dettagliate e interazioni a livello operazioni.

Tabella 84. Portlet della vista Operatore: Operazioni

Portlet	Descrizione
“Mappa” a pagina 279	<p>Una mappa della regione geografica con i contrassegni di risorse e di eventi.</p> <p>Un modulo filtro per la selezione di categorie di eventi da mostrare sulla mappa e nei portlet collegati al portlet Mappa.</p> <p>Un modulo filtro per la selezione di funzionalità di risorse da mostrare sulla mappa e nella scheda <b>Risorse</b> sul portlet Dettagli collegato. Per visualizzare questo modulo, selezionare prima <b>Visualizza risorse vicine</b> sul portlet Dettagli.</p>
“Dettagli” a pagina 272	Dettagli è un portlet di elenco interattivo. Tutti gli eventi per cui è stata concessa la visualizzazione sono visibili nell'elenco di eventi e su qualsiasi portlet di mappe collegato al portlet Dettagli.
“Notifiche” a pagina 287	<p>Il portlet Notifiche fornisce un elenco interattivo e dinamico di avvisi determinato dalle modifiche degli indicatori KPI e degli eventi correlati. Lo scopo di questo portlet è di evidenziare le modifiche allo stato eventi o KPI. L'elenco contiene i dettagli chiave per ciascuno degli avvisi.</p> <p>Ad esempio, quando si verificano due eventi gravi ravvicinati per ubicazione e ora, viene inviato un avviso al portlet Notifiche.</p>

Tabella 84. Portlet della vista Operatore: Operazioni (Continua)

Portlet	Descrizione
“Attività personali” a pagina 284	Un utente collegato può visualizzare le attività che gli sono state assegnate nel portlet Attività personali. Nel portlet Attività personali, le attività vengono raggruppate dalle rispettive procedure operative standard principali. Ogni procedura operativa standard corrisponde a un singolo evento.
“Contatti” a pagina 271	Il portlet Contatti può visualizzare un elenco dei contatti organizzati per categoria. È possibile organizzare i contatti in categorie basate sulle persone con cui è necessario comunicare. Ad esempio, è possibile creare una categoria per i contatti di lavoro generali e un'altra categoria per i contatti di lavoro del progetto. Con il portlet Contatti è possibile comunicare con le persone e modificare i gruppi, i contatti o il proprio stato in linea.

## Supervisore: Report

Utilizzare la vista Supervisore: Report per visualizzare un riepilogo dei dati evento generati dall'esecuzione dei report predefiniti. Inoltre, la vista Supervisore: Report può essere utilizzata per creare report personalizzati o per configurare report predefiniti. Tali report sono rivolti a operatori, responsabili o ad altre persone che monitorano gli eventi correnti e che pianificano eventi futuri.

La vista Supervisore: Report è una pagina Web interattiva che contiene diversi report basati su dati selezionati per fornire all'utente informazioni dettagliate e interazioni a livello supervisore. Queste informazioni vengono visualizzate nei grafici che riepilogano i dati evento presenti nel sistema.

Nella vista Supervisore: Report , è possibile configurare e visualizzare i report dei portlet “Report” a pagina 288. Per impostazione predefinita, alcuni dei portlet Report visualizzano report di esempio.

## Operatore: Report

Utilizzare la vista Operatore: Report per conservare la disponibilità di report, eventi e avvisi. La vista Operatore: Report è rivolta a operatori, responsabili o ad altre persone che monitorano i report.

La vista Operatore: Report fornisce un riepilogo dei dati evento generati dall'esecuzione di report predefiniti. È possibile inoltre utilizzare la vista Operatore: Report per visualizzare i report personalizzati. Tali report consentono di monitorare gli eventi correnti, intraprendere le azioni necessarie per gestire gli eventi e pianificare eventi futuri.

La vista Operatore: Report è una pagina Web interattiva. È possibile scegliere di visualizzare alcuni report differenti che forniscono informazioni esaurienti e interazioni a livello operatore.

Nella vista Operatore: Report, è possibile configurare e visualizzare i report dei portlet “Report” a pagina 288. Per impostazione predefinita, alcuni dei portlet Report visualizzano report di esempio.

## Vista Mappa ubicazioni

Utilizzare la vista Mappa ubicazioni per conservare la disponibilità di eventi e della relativa posizione su una mappa ubicazioni. La vista Mappa ubicazioni è rivolta a operatori, responsabili o ad altre persone che monitorano e rispondono agli eventi correnti.

La vista Mappa ubicazioni è una pagina Web interattiva. La pagina contiene i portlet elencati nella Tabella 85 a pagina 271. I portlet sono sezioni indipendenti della pagina interconnesse tra loro per fornire informazioni dettagliate e interazioni a livello operazioni.

Tabella 85. Portlet della vista Mappa ubicazioni

Portlet	Descrizione
“Mappa ubicazioni” a pagina 276	Un diagramma dell'ubicazione con i contrassegni per gli eventi. Un modulo filtro per la selezione di categorie dell'evento mostrato sulla mappa. Un elenco delle mappe ubicazioni disponibili organizzate in base alla classificazione.
“Dettagli” a pagina 272	Dettagli è un portlet di elenco interattivo. Tutti gli eventi per cui è stata concessa la visualizzazione sono visibili nell'elenco di eventi e su qualsiasi portlet di mappe collegato al portlet Dettagli.

## Utilizzo di portlet

Un portlet fornisce l'accesso alle informazioni che possono essere visualizzate e con le quali interagire su una pagina di portale.

IBM Intelligent Operations Center fornisce svariati portlet di tipo diverso.

Per un ausilio nell'utilizzo di ciascun portlet, fare clic nell'angolo superiore destro del portlet e selezionare **Guida** dal menu visualizzato.

Per modificare le dimensioni di un portlet, fare clic sull'angolo superiore destro del portlet e selezionare le opzioni dal menu visualizzato nel seguente modo:

- Per espandere il portlet per riempire la pagina, fare clic su **Ingrandisci**.
- Per nascondere il contenuto del portlet, fatta eccezione per la sua barra del titolo, fare clic su **Riduci a icona**.
- Per ripristinare un portlet ingrandito o ridotto a icona alla sua visualizzazione predefinita, fare clic su **Ripristina**.

## Personalizzazione di un portlet

In qualità di amministratore è possibile modificare le impostazioni del portlet facendo clic nell'angolo in alto a destra del portlet e selezionando un'opzione dal menu.

Esistono due modalità di personalizzazione, ciascuna che consente la modifica delle impostazioni del portlet per tutti gli utenti:

- L'opzione **Modifica impostazioni condivise** cambia solo l'istanza del portlet utilizzata quando si modificano le impostazioni.
- L'opzione **Configura** modifica le impostazioni globali del portlet per tutte le istanze del portlet ovunque si verifichino.

Le modalità di personalizzazione disponibili dipendono dalle autorizzazioni associate al proprio ID utente. Le impostazioni globali vengono sostituite dalle impostazioni condivise.

I portlet forniti con IBM Intelligent Operations Center dispongono di alcune impostazioni specifiche per un tipo di portlet, ad esempio, l'impostazione del livello di zoom predefinito per una mappa. Inoltre, è possibile impostare parametri di portlet generici comuni sui portlet forniti, ad esempio, il titolo del portlet.

## Contatti

Utilizzare il portlet Contatti per inviare messaggi istantanei all'interno della soluzione.

Il portlet Contatti può visualizzare un elenco dei contatti organizzati per categoria. È possibile organizzare i contatti in categorie basate sulle persone con cui è necessario comunicare. Ad esempio, è possibile creare una categoria per i contatti di lavoro generali e un'altra categoria per i contatti di lavoro del progetto. Con il portlet Contatti è possibile comunicare con le persone e modificare i gruppi, i contatti o il proprio stato in linea.

Fare clic sul menu nella parte superiore del portlet:

- **File** per aggiungere contatti, modificare gruppi o per scollegarsi
- **Strumenti** per impostare una conversione, riunione o annuncio; oppure per modificare le impostazioni sulla riservatezza
- **Guida** per ottenere ulteriori informazioni dettagliate su come utilizzare il portlet

Fare clic sul proprio stato per modificare lo stato e il messaggio. Lo stato predefinito indica che l'utente è disponibile. È possibile modificare lo stato per indicare che si è in riunione o non presenti al computer oppure che non si vuole essere disturbati.

Lo stato degli utenti collegati viene visualizzato nel portlet Contatti. Se un utente collegato chiude la finestra del browser o si scollega da WebSphere Portal, il suo stato continua ad essere visualizzato come collegato finché non scade la sessione. Tuttavia, i messaggi inviati a tale utente, dopo che questo ha chiuso la finestra del browser o si è scollegato, non vengono recapitati. Di conseguenza, viene proposto un messaggio di errore all'utente che sta tentando di inviare il messaggio. Per assicurarsi che lo stato venga aggiornato immediatamente nel portlet Contatti, scollegarsi facendo clic su **File > Disconnetti**.

**Nota:** Affinché questo portlet funzioni come previsto, è necessario collegarsi al portale della soluzione utilizzando il nome del dominio completo di IBM Intelligent Operations Centerserver delle applicazioni. Se ci si collega al portale utilizzando un indirizzo IP o un alias del nome host invece del nome di dominio completo registrato, questo portlet non viene visualizzato correttamente.

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Le impostazioni che è possibile modificare per il portlet Contatti sono:

- File della guida
- Altezza portlet
- Altezza del portlet quando ingrandito
- Titolo del portlet
- Raggruppamento di risorse

#### **Riferimenti correlati:**

“Impostazioni portlet Contatti” a pagina 147

Personalizzare il portlet Contatti modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## **Dettagli**

Utilizzare il portlet Dettagli per visualizzare, monitorare e gestire gli eventi in IBM Intelligent Operations Center.

Dettagli è un portlet di elenco interattivo. Tutti gli eventi per cui è stata concessa la visualizzazione sono visibili nell'elenco di eventi e su qualsiasi portlet di mappe collegato al portlet Dettagli.

Le risorse in prossimità di un evento possono essere visualizzate in un elenco risorse e su una mappa.

## Eventi e risorse

Il portlet Dettagli dispone di due elementi di interfaccia interattiva come mostrato nella seguente tabella:

Tabella 86. Visualizzazione del portlet Dettagli

Elemento interfaccia	Descrizione
Eventi e incidenti	L'elenco di eventi contiene i dettagli chiave per ciascun evento. È possibile visualizzare una descrizione più dettagliata di un evento al passaggio del mouse sulla riga nell'elenco.
Risorse	I dettagli chiave per le risorse in prossimità di un evento vengono elencati quando si fa clic con il tasto destro del mouse sull'evento selezionato. È possibile visualizzare una descrizione più dettagliata di una risorsa al passaggio del mouse sulla riga nell'elenco.

Inizialmente, quando si apre IBM Intelligent Operations Center, il portlet Dettagli mostra tutti gli eventi rilevanti.

È possibile selezionare nel portlet Mappa le categorie di eventi e le funzionalità delle risorse da mostrare. Le categorie di eventi mostrate nella scheda **Eventi e incidenti** e sul portlet Mappa sono uguali. Le funzionalità delle risorse mostrate nella scheda **Risorse** e sul portlet Mappa sono uguali.

L'elenco eventi viene aggiornato regolarmente con nuovi eventi e aggiornamenti, con la possibilità di eventuali filtri impostati per limitare le categorie mostrate.

Un contatore nell'angolo sinistro della barra delle azioni posto alla fine dell'elenco indica il numero di elementi visualizzati e il numero totale di elementi. Nella parte centrale della barra delle azioni è possibile selezionare il numero di elementi da visualizzare contemporaneamente. Se vi sono più righe rispetto al numero consentito che è possibile visualizzare contemporaneamente, l'utente può scorrere avanti o indietro le pagine facendo clic sui pulsanti nell'angolo destro della barra delle azioni.

## Proprietà dell'evento

Nella seguente tabella vengono riportate le proprietà che descrivono un evento:

Tabella 87. Proprietà dell'evento

Proprietà	Contenuto
<b>Chi</b>	
Mittente	Origine o ID utente
Nome contatto	Persona da contattare per informazioni aggiuntive
E-mail contatto	Indirizzo e-mail della persona da contattare
Telefono del contatto	Numero telefonico della persona da contattare
<b>Cosa</b>	
Tipo evento*	Testo che indica il tipo di evento all'interno della <i>Categoria</i>
Stato evento*	Istruzioni per la gestione eventi
Ambito evento*	Destinatari del messaggio
Limitazioni	Informazioni aggiuntive richieste quando <i>Ambito evento</i> è 'Limitato'
Titolo*	Breve descrizione dell'evento
Categoria*	Classificazione evento di livello superiore
Gravità*	Intensità dell'impatto dell'evento
Certezza*	Sicurezza nella previsione evento
Urgenza*	Intervallo di tempo per l'azione in risposta all'evento

Tabella 87. Proprietà dell'evento (Continua)

Proprietà	Contenuto
<b>Chi</b>	
Tipo di messaggio	Natura del messaggio
Descrizione	Descrizione aggiuntiva dell'evento
Indirizzo Web	Indirizzo Web per informazioni aggiuntive sull'evento
<b>Quando</b>	
Data e ora invio	La data e l'ora in cui il messaggio è stato inoltrato o inviato
Data e ora in vigore	La data e l'ora in cui il messaggio entra in vigore
Data e ora inizio	La data e l'ora in cui è previsto l'inizio dell'evento
Data e ora scadenza	La data e l'ora in cui è prevista la fine dell'evento
<b>Dove</b>	
Descrizione area	Descrizione dell'area interessata
Latitudine / Longitudine	Coordinate dell'ubicazione eventi

**Nota:** Le proprietà contrassegnate con un asterisco nella tabella sono obbligatori per la corretta creazione di un nuovo evento. Le proprietà non contrassegnate con un asterisco sono facoltative durante la creazione di un evento.

## Gestione di eventi e incidenti

Nel portlet Dettagli, è possibile eseguire diverse azioni sugli eventi presenti nell'elenco sulla scheda **Eventi e incidenti**. Nel portlet Mappa è possibile aggiungere un evento mostrato sia nella mappa che nell'elenco eventi del portlet Dettagli.

### Procedura

Nella scheda **Eventi e incidenti**, fare clic con il tasto destro del mouse su una riga nell'elenco eventi e selezionare un'opzione dal menu:

- Per aggiornare le informazioni relative a un evento, fare clic su **Aggiorna evento**. È possibile immettere le modifiche in una finestra con campi che contengono informazioni sull'evento. Quando un record evento viene aggiornato, la proprietà del tipo di messaggio cambia in *Aggiorna*.
- Per modificare lo stato di un evento in incidente, fare clic su **Incrementa a incidente** per visualizzare una finestra e immettere i dettagli del contatto. Quando un record evento viene incrementato, si verifica una modifica alle proprietà e all'icona presente nella mappa.
- Per rimuovere un evento dall'elenco e dalla mappa, fare clic su **Annulla evento** per visualizzare una finestra e immettere i dettagli del contatto.
- Per visualizzare le attività procedura operativa standard e flusso di lavoro associate a un evento, fare clic su **Visualizza dettagli SOP (Standard Operating Procedure)**. Se non vi sono procedure operative standard associate a un evento, questa opzione non è disponibile. Se è presente una procedura operativa standard associata, viene visualizzata la finestra Dettagli SOP (Standard Operating Procedure). Utilizzare il portlet Attività personali per gestire le attività flusso di lavoro associate a una procedura operativa standard.
- Per visualizzare un elenco di risorse in prossimità di un evento, fare clic su **Visualizza risorse vicine** e selezionare il raggio dell'area interessata. Viene visualizzato un elenco di risorse nella scheda **Risorse**.
- Per visualizzare le informazioni relative a un evento, fare clic su **Proprietà** per visualizzare una finestra che contiene campi con informazioni sull'evento.

## Gestione delle risorse

È possibile eseguire diverse azioni sulle risorse nell'elenco presente sulla scheda **Risorse**.

### Procedura

Nella scheda **Risorse**, fare clic con il tasto destro del mouse su una riga nell'elenco risorse e selezionare un'opzione dal menu:

- Per aggiornare le informazioni relative a una risorsa, fare clic su **Aggiorna**.
- Per rimuovere una risorsa dall'elenco e dalla mappa, fare clic su **Elimina**.
- Per visualizzare le informazioni relative a una risorsa, fare clic su **Proprietà**.

Qualsiasi opzione venga scelta, la risorsa viene visualizzata in Tivoli Service Request Manager sulla scheda **Risorse**. È possibile inoltre visualizzare le funzionalità della risorsa nella scheda Tivoli Service Request Manager **Funzionalità**. Per aggiornare o eliminare una risorsa, selezionare la risorsa e quindi selezionare l'opzione appropriata dall'elenco **Seleziona azione**.

## Personalizzazione del portlet Dettagli

**Importante**

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Impostare i parametri per il portlet Dettagli nel modo seguente:

Con l'impostazione dei parametri per il portlet Dettagli è possibile:

- Specificare il layout della colonna, le intestazioni, il criterio di ordinamento e la priorità.
- Specificare le condizioni aggiuntive per filtrare gli eventi o le risorse visualizzate.
- Mostrare o nascondere:
  - il pulsante **Aggiungi evento**
  - il pulsante **Aggiungi risorse**
  - la scheda **Eventi**
  - la scheda **Risorse**
  - la barra degli strumenti nella parte superiore dell'elenco.
- Specificare un nome gruppo per abilitare la comunicazione con altre mappe e portlet Dettagli.
- Impostare il portlet per acquisire o ignorare specifici tipi di messaggio che provengono da altri portlet nel gruppo.

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

### Riferimenti correlati:

“Impostazioni portlet Dettagli” a pagina 148

Personalizzare il portlet Dettagli modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Drill Down KPI (Key Performance Indicator)

Utilizzare il portlet Drill Down KPI (Key Performance Indicator) per visualizzare ulteriori informazioni su una categoria KPI, lo stato dei KPI sottostanti.



Il portlet Drill Down KPI (Key Performance Indicator) mostra tutti i KPI sottostanti associati a un'organizzazione o la categoria KPI mostrata nel portlet Stato. Gli indicatori KPI vengono visualizzati in formato di elenco nidificato che è possibile espandere o comprimere. Lo stato di ciascun KPI sottostante viene rappresentato per colore, in modo analogo al colore utilizzato per le categorie KPI visualizzate nel portlet Stato. I valori dei KPI sottostanti determinano il colore del KPI principale. Per visualizzare lo stato del KPI, spostare il cursore del mouse sul KPI.

Per concentrarsi su una specifica categoria KPI nel portlet Drill Down KPI (Key Performance Indicator), fare clic sulla categoria nel portlet Stato. Questa categoria viene quindi visualizzata autonomamente nel portlet Drill Down KPI (Key Performance Indicator). È possibile utilizzare l'elenco per esaminare gli indicatori KPI sottostanti fino a quando si raggiungono i dettagli del KPI che ha causato la modifica dello stato.

## Personalizzazione del portlet Drill Down KPI (Key Performance Indicator)

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Con l'impostazione dei parametri per il portlet Drill Down KPI (Key Performance Indicator) è possibile:

- Specificare il layout della colonna, le intestazioni, il criterio di ordinamento e la priorità.
- Personalizzare i colori KPI.
- Abilitare un filtro KPI aggiuntivo.
- Mostrare o nascondere la barra degli strumenti nella parte superiore dell'elenco.
- Specificare un nome gruppo per abilitare la comunicazione con un portlet Drill Down KPI (Key Performance Indicator).

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

### Concetti correlati:

“KPI (Key Performance Indicators)” a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

### Riferimenti correlati:

“Impostazioni portlet Drill Down KPI (Key Performance Indicator)” a pagina 152

Personalizzare il portlet Drill Down KPI (Key Performance Indicator) modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Mappa ubicazioni

Utilizzare il portlet Mappa ubicazioni per visualizzare gli eventi contrassegnati sulla mappa ubicazioni. Una mappa ubicazioni in IBM Intelligent Operations Center è una mappa o piano con aree predefinite per l'interazione, ad esempio, i posti a sedere di un principale stadio sportivo.

Il portlet Mappa ubicazioni fornisce una rappresentazione visiva degli eventi nella posizione in cui si verificano. Il portlet Mappa ubicazioni insieme a Mappa, e ai portlet Dettagli consente di identificare i problemi, i pattern di ubicazioni, i conflitti e le sinergie.

Il portlet Mappa ubicazioni, Mappa, e i portlet Dettagli possono essere collegati tra loro per condividere input e modifiche agli eventi visualizzati. È possibile selezionare nel portlet Mappa ubicazioni le categorie di eventi che si desidera visualizzare. La selezione dell'utente influisce sugli eventi visualizzati nel portlet Mappa ubicazioni e sui portlet Mappa e Dettagli che ad esso sono collegati.

## Mappa ubicazioni interfaccia

Il portlet Mappa ubicazioni dispone di tre elementi di interfaccia interattiva come mostrato nella seguente tabella:

Tabella 88. Elementi dell'interfaccia del portlet Mappa ubicazioni

Elemento interfaccia	Descrizione
Mappa ubicazioni	Un diagramma dell'ubicazione con i contrassegni per gli eventi.
Selezione del contenuto: Categorie di eventi	Un modulo filtro per la selezione di categorie dell'evento mostrato sulla mappa.
Menu Mappa	Un elenco delle mappe ubicazioni disponibili organizzate in base alla classificazione.

Inizialmente, la pagina del portale si apre con il portlet Mappa ubicazioni, mentre tutti gli eventi rilevanti vengono visualizzati sulla mappa ubicazioni. La mappa è aggiornata con nuovi eventi, sottoposti ad eventuali filtri impostati per limitare le categorie mostrate. Alla sinistra della mappa viene fornita una barra di menu che elenca tutte le mappe disponibili

Un evento che si verifica in un'area viene rappresentato da un contrassegno nella corrispondente posizione nella mappa ubicazioni. È possibile visualizzare un titolo e descrizione dell'evento al passaggio del mouse sul contrassegno dell'evento nella mappa. La finestra contiene il nome e la descrizione dell'area in cui si verifica l'evento. Se si verifica più di un evento nella stessa area, gli eventi vengono raggruppati e rappresentati da un contrassegno a cluster. Al passaggio del mouse su questo contrassegno, il titolo di ogni evento viene incluso nella finestra. È possibile anche visualizzare un nome area e una descrizione al passaggio del mouse su una qualsiasi delle aree predefinite nella mappa senza eventi.

Laddove i portlet sono collegati, è possibile fare clic sull'evento in questo portlet e vengono selezionati anche gli eventi corrispondenti in altri portlet del gruppo. Analogamente, la selezione di un evento in uno qualsiasi dei portlet collegati, fa sì che l'evento venga evidenziato in questo portlet.

**Nota:** Un evento deve avere un identificativo area per essere visualizzato nel portlet Mappa ubicazioni. Inoltre, un evento deve avere le coordinate di latitudine e longitudine per essere mostrato sui portlet Mappa ubicazioni e Mappa. Se un evento non dispone di un identificativo area o delle coordinate, può essere visualizzato solo nel portlet Dettagli.

## Contrassegni mappa

La mappa rappresenta l'ubicazione degli eventi con uno dei seguenti tipi di contrassegno:

Tabella 89. Contrassegni mappa

Tipo di contrassegno	Descrizione
Icona	Individua sulla mappa la posizione di un evento con un'icona univoca per ciascuna categoria di eventi.
Cluster	Indica più di un evento nella stessa area con un numero che rappresenta il numero di eventi in quell'area.

L'icona che rappresenta un tipo di evento viene definita nel campo categoria dei dettagli dell'evento nella scheda **Eventi e incidenti** del portlet Dettagli. Quando un evento viene valutato come incidente, l'icona visualizzata sulla mappa conserva il simbolo specifico di categoria, con l'aggiunta di un margine rosso attorno all'icona.

## Controlli della mappa

È possibile spostare il cursore all'interno della mappa utilizzando il mouse o la tastiera.

### I controlli della mappa si trovano sul lato superiore sinistro della mappa

I controlli della mappa si trovano sul lato superiore sinistro della mappa. Sono costituiti da:

- Freccia panoramica (su, giù, sinistra, destra)
- Zoom in avanti
- Vista mondo (zoom all'indietro fino alla massima estensione)
- Zoom all'indietro

### Controlli di panoramica per lo spostamento attorno alla mappa

Per spostarsi all'interno di una mappa è possibile:

- Fare clic e trascinare la mappa utilizzando il mouse
- Premere la freccia panoramica verso l'alto oppure il tasto freccia verso l'alto della tastiera per ottenere una panoramica lato nord
- Premere la freccia panoramica verso il basso oppure il tasto freccia verso il basso della tastiera per ottenere una panoramica lato sud
- Premere la freccia panoramica verso destra oppure il tasto freccia verso destra della tastiera per ottenere una panoramica lato est
- Premere la freccia panoramica verso sinistra oppure il tasto freccia verso sinistra della tastiera per ottenere una panoramica lato ovest

### Controlli dello zoom per l'ingrandimento o la riduzione della scala di una mappa

Per eseguire lo zoom in avanti e all'indietro della mappa, è possibile:

- Fare clic sull'icona + della mappa per eseguire lo zoom in avanti o l'icona - della mappa per eseguire lo zoom fuori dal centro della mappa
- Fare doppio clic per centrare la mappa ed eseguire lo zoom in avanti dell'ubicazione selezionata
- Fare clic sull'icona **Vista mondo** per eseguire completamente lo zoom all'indietro e visualizzare la vista mondo
- Premere il tasto + sulla tastiera per eseguire lo zoom in avanti
- Premere il tasto - sulla tastiera per eseguire lo zoom all'indietro
- Premere Maiusc mentre si utilizza il mouse per tracciare un rettangolo attorno l'area da ingrandire con lo zoom

### Selezione di categorie di eventi per la mappa

Con il filtro categorie di eventi, è possibile selezionare per categoria quali eventi vengono visualizzati nella mappa.

Per visualizzare il modulo del filtro, fare clic su **Seleziona contenuto**. Le categorie degli eventi visualizzati sulla mappa e nei portlet associati possono essere modificati qui in base alla selezione del modulo filtro. È possibile concentrarsi sulle categorie di eventi che si desidera analizzare utilizzando il filtro per nascondere le categorie di eventi non necessarie. La mappa risponde a qualsiasi modifica apportata sul modulo filtro. Quando la selezione è modificata, la mappa viene aggiornata e solo le posizioni degli eventi all'interno delle categorie selezionate vengono tracciate sulla mappa. Modificare le categorie degli eventi visualizzati selezionando o deselezionando le caselle di spunta presenti nel modulo filtro. Per chiudere il modulo filtro, fare clic su **Seleziona contenuto**. Se si esce e si ritorna alla pagina del portale, il filtro viene reimpostato sulla selezione predefinita.

È possibile focalizzare l'attenzione su singoli eventi che si desidera analizzare selezionando le caselle di spunta nel portlet Dettagli. Questi eventi vengono quindi evidenziati anche nei portlet collegati.

## Personalizzazione del portlet Mappa ubicazioni

**Informazioni**

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

I portlet Mappa e Mappa ubicazioni possono anche essere personalizzati modificando le impostazioni globali. Le impostazioni globali influiscono sul contenuto del portlet per tutti gli utenti e per tutte le ricorrenze del portlet. Le impostazioni globali vengono sostituite dalle impostazioni condivise.

Le impostazioni che possono essere modificate per il portlet Mappa ubicazioni sono riportate di seguito:

- La selezione predefinita sul filtro Categorie di eventi
- Il nome della mappa ubicazioni predefinita da visualizzare
- Il colore predefinito di evidenziazione dell'area quando si utilizza il cursore al passaggio del mouse sull'area.
- Il nome del gruppo che consente la comunicazione con le altre mappe e portlet Dettagli

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

## Personalizzazione delle mappe ubicazioni

È possibile utilizzare il portlet Gestore mappa ubicazioni per personalizzare i seguenti aspetti del portlet Mappa ubicazioni:

- Nome classificazione da visualizzare sul menu alla sinistra del portlet.
- La mappa che deve essere visualizzata nel portlet.
- Aree all'interno di una mappa.

### Concetti correlati:

“Gestore mappa ubicazioni” a pagina 176

Utilizzare il portlet Gestore mappa ubicazioni per personalizzare il portlet Mappa ubicazioni.

### Riferimenti correlati:

“Impostazioni portlet Mappa ubicazioni” a pagina 155

Personalizzare il portlet Mappa ubicazioni modificando le impostazioni nei campi della finestra

### Impostazioni condivise.

## Mappa

Utilizzare il portlet Mappa per visualizzare eventi e risorse presenti su una mappa.

Il portlet Mappa fornisce una rappresentazione visiva degli eventi e delle risorse su una mappa. Utilizzare il portlet Mappa in combinazione con i portlet Mappa ubicazioni e Dettagli, per identificare pattern, conflitti, problemi e sinergie dell'ubicazione.

I portlet Mappa, Mappa ubicazioni e Dettagli possono essere collegati tra loro per condividere gli input e le modifiche degli eventi visualizzati. È possibile selezionare nel portlet Mappa le categorie di eventi e le funzionalità delle risorse che si desidera visualizzare. La propria selezione influisce sugli elementi visualizzati nel portlet Mappa e nei portlet Mappa ubicazioni e Dettagli collegati.

## Interfaccia mappa

Il portlet Mappa dispone di tre elementi di interfaccia interattiva come mostrato nella seguente tabella:

Tabella 90. Elementi dell'interfaccia del portlet Mappa

Elemento interfaccia	Descrizione
Mappa	Una mappa della regione geografica con i contrassegni di risorse e di eventi.
Selezione del contenuto: Categorie di eventi	Un modulo filtro per la selezione di categorie di eventi da mostrare sulla mappa e nei portlet collegati al portlet Mappa.
Selezione del contenuto: Risorse	Un modulo filtro per la selezione di funzionalità di risorse da mostrare sulla mappa e nella scheda <b>Risorse</b> sul portlet Dettagli collegato. Per visualizzare questo modulo, selezionare prima <b>Visualizza risorse vicine</b> sul portlet Dettagli.

Inizialmente, la pagina del portale si apre con il portlet Mappa e con tutti gli eventi rilevanti sulla mappa. Se sono specificati i valori di latitudine e di longitudine di un evento, è possibile visualizzare l'ubicazione dell'evento sotto forma di contrassegno a icona sulla mappa. È possibile visualizzare il titolo e la descrizione di un evento al passaggio del mouse sul contrassegno dell'evento nella mappa. Se è presente più di un evento raggruppato nella stessa ubicazione, viene indicato il numero di eventi sul contrassegno. Al passaggio del mouse su quel contrassegno cluster, il titolo di ciascun evento viene incluso nella finestra. La mappa è aggiornata con nuovi eventi, sottoposti ad eventuali filtri impostati per limitare le categorie mostrate.

Quando i portlet sono collegati, è possibile fare clic su un contrassegno dell'evento in un portlet per far sì che venga selezionato anche l'evento corrispondente negli altri portlet del gruppo.

Esiste un limite al numero di contrassegni che può essere visualizzato nella mappa. Se il numero di contrassegni nell'area della vista supera la soglia, i contrassegni non vengono mostrati. Viene ricevuto un messaggio con il numero di contrassegni disponibili e il numero della soglia. Vengono fornite due opzioni per visualizzare tutti i contrassegni disponibili:

- Fare zoom avanti o eseguire una panoramica dell'area della mappa con il numero di contrassegni inferiore alla soglia.
- Fare clic su **Carica tutti gli elementi nella vista**.

Se si sceglie la seconda opzione, si potrebbe notare una più lenta visualizzazione dei contrassegni sulla mappa. È possibile una terza opzione, ovvero l'utilizzo del filtro per selezionare meno categorie.

Quando si seleziona **Visualizza risorse vicine** di un evento nel portlet Dettagli, le risorse vengono mostrate sulla mappa in base al raggio e alle funzionalità selezionate.

La mappa tiene l'utente aggiornato aggiungendo nuovi eventi alla mappa, con la possibilità di eventuali filtri impostati per limitare le categorie mostrate.

**Nota:** Se un evento dispone di un identificativo area in aggiunta alle coordinate di latitudine e longitudine, può essere mostrato in entrambi i portlet Mappa ubicazioni e Mappa. Tutti gli eventi possono essere mostrati sul portlet Dettagli.

## Contrassegni mappa

La mappa rappresenta l'ubicazione degli eventi e delle risorse con uno dei seguenti tipi di contrassegno:

Tabella 91. Contrassegni mappa

Tipo di contrassegno	Descrizione
Icona	individua sulla mappa l'ubicazione di un evento o di una risorsa con un'icona univoca per ciascun tipo di risorsa o categoria
Poligono	delinea sulla mappa l'area associata a un particolare evento
Cluster	indica più di un evento nella stessa ubicazione con un numero che rappresenta il totale degli eventi in quella ubicazione
Raggio	delinea sulla mappa l'area selezionata per <b>Visualizza risorse vicine</b> in relazione a un evento

L'icona che rappresenta un tipo di evento viene definita nel campo categoria dei dettagli dell'evento nella scheda **Eventi e incidenti** del portlet Dettagli. Quando un evento viene elevato a incidente, l'icona visualizzata sulla mappa conserva il simbolo specifico di categoria, con l'aggiunta di un margine rosso. Facendo clic su un contrassegno dell'evento nella mappa, è possibile evidenziare l'evento o gli eventi associati nel portlet Dettagli.

L'icona che rappresenta una risorsa viene definita nel campo tipo dei dettagli della risorsa sulla scheda **Risorse** del portlet Dettagli. Per visualizzare le icone delle risorse, selezionare prima **Visualizza risorse vicine** sul portlet Dettagli.

## Utilizzo dei controlli della mappa

È possibile spostare il cursore all'interno della mappa utilizzando il mouse o la tastiera.

### I controlli della mappa si trovano sul lato superiore sinistro della mappa

I controlli della mappa si trovano sul lato superiore sinistro della mappa. Sono costituiti da:

- Freccie panoramica (su, giù, sinistra, destra)
- Zoom in avanti
- Vista mondo (zoom all'indietro fino alla massima estensione)
- Zoom all'indietro

### Controlli di panoramica per lo spostamento attorno alla mappa

Per spostarsi all'interno di una mappa è possibile:

- Fare clic e trascinare la mappa utilizzando il mouse
- Premere la freccia panoramica verso l'alto oppure il tasto freccia verso l'alto della tastiera per ottenere una panoramica lato nord
- Premere la freccia panoramica verso il basso oppure il tasto freccia verso il basso della tastiera per ottenere una panoramica lato sud
- Premere la freccia panoramica verso destra oppure il tasto freccia verso destra della tastiera per ottenere una panoramica lato est
- Premere la freccia panoramica verso sinistra oppure il tasto freccia verso sinistra della tastiera per ottenere una panoramica lato ovest

### Controlli dello zoom per l'ingrandimento o la riduzione della scala di una mappa

Per eseguire lo zoom in avanti e all'indietro della mappa, è possibile:

- Fare clic sull'icona + della mappa per eseguire lo zoom in avanti o l'icona - della mappa per eseguire lo zoom fuori dal centro della mappa
- Fare doppio clic per centrare la mappa ed eseguire lo zoom in avanti dell'ubicazione selezionata
- Fare clic sull'icona **Vista mondo** per eseguire completamente lo zoom all'indietro e visualizzare la vista mondo
- Premere il tasto + sulla tastiera per eseguire lo zoom in avanti
- Premere il tasto - sulla tastiera per eseguire lo zoom all'indietro
- Premere Maiusc mentre si utilizza il mouse per tracciare un rettangolo attorno l'area da ingrandire con lo zoom

## Selezione di categorie di eventi per la mappa

Utilizzare il filtro Categorie di eventi per selezionare per categoria quali eventi vengono visualizzati sulla mappa.

Per visualizzare il modulo del filtro, fare clic su **Seleziona contenuto**. È possibile modificare le categorie di eventi visualizzati nel portlet della mappa in base alla selezione del modulo filtro effettuata. È possibile concentrarsi sulle categorie di eventi che si desidera analizzare utilizzando il filtro per nascondere le categorie di eventi non necessarie. La mappa risponde a qualsiasi modifica apportata sul modulo filtro. Una modifica sul modulo filtro influisce anche su altri portlet nello stesso gruppo. Quando una selezione è modificata, la mappa viene aggiornata e solo le ubicazioni degli eventi all'interno delle categorie selezionate vengono tracciate sulla mappa. Modificare le categorie degli eventi visualizzati selezionando o deselezionando le caselle di spunta presenti nel modulo filtro. Per chiudere il modulo filtro, fare clic su **Seleziona contenuto**. Se si esce e si ritorna alla pagina del portale, il filtro viene reimpostato sul valore predefinito (tutte le categorie selezionate).

È possibile concentrarsi sui singoli eventi che si desidera analizzare selezionando le caselle di spunta nel portlet Dettagli. Tali eventi sono evidenziati sulla mappa.

## Selezione di funzionalità di risorse per la mappa

Quando si seleziona **Visualizza risorse vicine** sul portlet Dettagli, il filtro Categorie di eventi viene sostituito dal filtro Risorse. Utilizzare il filtro Risorse per selezionare in base alla funzionalità quali risorse vengono visualizzate sulla mappa.

Per visualizzare il modulo del filtro, fare clic su **Seleziona contenuto**. È possibile modificare le funzionalità delle risorse visualizzate sulla mappa e nel portlet Dettagli in base alla selezione del modulo filtro effettuata. È possibile concentrarsi sulla funzionalità che si desidera analizzare utilizzando il filtro per nascondere le funzionalità non necessarie. La mappa risponde a qualsiasi modifica apportata sul modulo filtro. Una modifica sul modulo filtro influisce anche sul portlet Dettagli nello stesso gruppo. Quando una selezione è modificata, la mappa viene aggiornata e solo le ubicazioni delle risorse con le funzionalità selezionate vengono tracciate sulla mappa. Modificare le funzionalità delle risorse visualizzate selezionando o deselezionando le caselle di spunta presenti nel modulo filtro. Per chiudere il modulo filtro, fare clic su **Seleziona contenuto**. Se si esce dalla pagina del portale e si ritorna al modulo filtro delle risorse, il filtro viene reimpostato sul valore predefinito (tutte le funzionalità selezionate). Le funzionalità selezionate in modo predefinito dipendono dalla categoria dell'evento e da come quella categoria è associata alle funzionalità.

## Reimpostazione della mappa

Il portlet Mappa può essere reimpostato sulla vista predefinita configurata per IBM Intelligent Operations Center.

### Procedura

1. Sul portlet Mappa, fare clic su **Reimposta la mappa** oppure sulla freccia nell'angolo in alto a destra.
2. Selezionare una delle opzioni riportate di seguito:



- **Reimposta la mappa** per eseguire lo zoom e centrare la mappa sull'impostazione predefinita.
- **Reimposta la mappa e cancella i filtri** per eseguire lo zoom e centrare la mappa sull'impostazione predefinita e per reimpostare i valori impostati in **Seleziona contenuto** sui valori predefiniti.

## Risultati

La mappa viene reimpostata in base all'opzione selezionata, ma solo per l'utente e la vista correnti.

## Aggiunta di un evento

È possibile creare un evento, aggiungendolo contemporaneamente alla mappa del portlet Mappa e all'elenco del portlet Dettagli. La mappa e l'elenco forniscono due modalità di visualizzazione dello stesso contenuto.

## Informazioni su questa attività

Utilizzare la finestra di dialogo **Aggiungi evento** per specificare le proprietà dell'evento, come descritto nella seguente tabella:

Tabella 92. Proprietà dell'evento

Proprietà	Contenuto
<b>Chi</b>	
Mittente	Origine o ID utente
Nome contatto	Persona da contattare per informazioni aggiuntive
E-mail contatto	Indirizzo e-mail della persona da contattare
Telefono del contatto	Numero telefonico della persona da contattare
<b>Cosa</b>	
Tipo evento*	Testo che indica il tipo di evento all'interno della <i>Categoria</i>
Stato evento*	Istruzioni per la gestione eventi
Ambito evento*	Destinatari del messaggio
Limitazioni	Informazioni aggiuntive richieste quando <i>Ambito evento</i> è 'Limitato'
Titolo*	Breve descrizione dell'evento
Categoria*	Classificazione evento di livello superiore
Gravità*	Intensità dell'impatto dell'evento
Certezza*	Sicurezza nella previsione evento
Urgenza*	Intervallo di tempo per l'azione in risposta all'evento
Tipo di messaggio	Natura del messaggio
Descrizione	Descrizione aggiuntiva dell'evento
Indirizzo Web	Indirizzo Web per informazioni aggiuntive sull'evento
<b>Quando</b>	
Data e ora invio	La data e l'ora in cui il messaggio è stato inoltrato o inviato
Data e ora in vigore	La data e l'ora in cui il messaggio entra in vigore
Data e ora inizio	La data e l'ora in cui è previsto l'inizio dell'evento
Data e ora scadenza	La data e l'ora in cui è prevista la fine dell'evento
<b>Dove</b>	
Descrizione area	Descrizione dell'area interessata
Latitudine / Longitudine	Coordinate dell'ubicazione eventi

## Procedura

1. Fare clic con il tasto destro del mouse su un'ubicazione nella mappa e fare clic su **Aggiungi evento** per aprire la finestra di dialogo **Aggiungi evento**. Alcune proprietà dell'evento vengono completate automaticamente.
2. Specificare le rimanenti proprietà dell'evento nei campi della finestra di dialogo. Le proprietà contrassegnate con un asterisco sono obbligatorie per la corretta creazione di un nuovo evento; le proprietà non contrassegnate con un asterisco sono facoltative.
3. Fare clic su **OK** per salvare l'evento o **Annulla** per interrompere l'aggiunta dell'evento.

## Risultati

Un'icona che rappresenta la categoria del nuovo evento viene visualizzata nell'ubicazione richiesta sulla mappa. È possibile visualizzare i dettagli del nuovo evento nell'elenco portlet **Dettagli** collegato.

## Personalizzazione del portlet Mappa

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

I portlet **Mappa** e **Mappa ubicazioni** possono anche essere personalizzati modificando le impostazioni globali. Le impostazioni globali influiscono sul contenuto del portlet per tutti gli utenti e per tutte le ricorrenze del portlet. Le impostazioni globali vengono sostituite dalle impostazioni condivise.

È possibile modificare le seguenti impostazioni specifiche del portlet **Mappa**:

- Reimpostare il livello di zoom e il punto centrale predefinito per la mappa.
- Selezionare una nuova mappa base, quella predefinita è una mappa ArcGIS fornita da Esri.
- Aggiungere i livelli di visualizzazione e di annotazione geografica della mappa in KML (Keyhole Markup Language), per la rappresentazione di dati aggiuntivi.
- Impostare una soglia per il numero di contrassegni che è possibile visualizzare senza che venga emesso un messaggio di avvertenza.
- Impostare la selezione predefinita sui filtri della mappa, da visualizzare quando si fa clic su **Seleziona contenuto**.
- Specificare il nome del gruppo che abilita la comunicazione con altre mappe e portlet **Dettagli**

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

### Riferimenti correlati:

“Impostazioni portlet **Mappa**” a pagina 157

Personalizzare il portlet **Mappa** modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Attività personali

Il portlet **Attività personali** visualizza un elenco dinamico di attività di proprietà del gruppo di cui l'utente collegato all'interfaccia è membro.

Ogni volta che un evento attiva un procedura operativa standard in base ai criteri di selezione definiti in matrice di selezione procedura operativa standard, le attività associate vengono assegnate ai proprietari. Per ulteriori informazioni sulle procedure operative standard, accedere al collegamento alla fine dell'argomento.

Un utente collegato può visualizzare le attività che gli sono state assegnate nel portlet Attività personali. Nel portlet Attività personali, le attività vengono raggruppate dalle rispettive procedure operative standard principali. Ogni procedura operativa standard corrisponde a un singolo evento.

Per ogni procedura operativa standard, il portlet Attività personali visualizza solo le attività aperte e non quelle chiuse o completate. Le attività aperte comprendono le attività già avviate e quelle idonee da avviare. Ad esempio, se una o più attività specificate in un procedura operativa standard sono ordinate in una sequenza, viene visualizzata solo l'attività corrente nella sequenza. Se una particolare attività si basa sul completamento di un'attività predecessore, essa non viene visualizzata fino a quando l'attività predecessore viene completata o ignorata.

Le seguenti icone di completamento attività vengono visualizzate nella parte superiore del portlet Attività personali:

#### **Scaduta**

Attività il cui completamento è scaduto.

**Oggi** Attività che devono essere completate oggi.

**Futura** Attività il cui completamento è previsto in futuro.

Quando un'attività viene avviata, la data di fine attività viene calcolata aggiungendo l'ora di inizio alla durata dell'attività. Le date di fine attività vengono utilizzate per calcolare il numero visualizzato in ognuna delle icone di completamento attività.


Nel portlet Attività personali, le procedure operative standard che presentano attività scadute vengono visualizzate prima, mentre le procedure operative standard rimanenti vengono visualizzate in ordine alfabetico.

Accanto a ciascuna procedura operativa standard dell'elenco che presenta attività scadute, un'icona rossa indica il numero di attività scadute. Le procedure operative standard con attività scadute vengono ordinate in base al numero di attività scadute che contengono. La procedura operativa standard che contiene la maggior parte delle attività scadute viene visualizzata nella parte superiore dell'elenco.

## **Gestione delle attività nel portlet Attività personali**

Gestire le proprie attività nel portlet Attività personali:

- Per visualizzare i dettagli relativi a una procedura operativa standard, espandere il nome della procedura operativa standard.
  - Viene visualizzato il nome dell'evento che ha attivato la procedura operativa standard. Al passaggio del mouse sul nome evento vengono visualizzate le informazioni sulla guida, contenenti la data e l'ora di inizio evento e la categoria, gravità, certezza e urgenza dell'evento.
  - Se il portlet Dettagli viene visualizzato nella pagina, per consultare le proprietà dell'evento, fare clic sul nome dell'evento. Viene visualizzata la finestra Proprietà dell'evento.
  - Vengono visualizzate le operazioni in corso o idonee per essere avviate. Inoltre, vengono visualizzati lo stato e la data di fine di ciascuna operazione.
- Per visualizzare ulteriori dettagli relativi a un'operazione, inclusi i commenti e i riferimenti che gli utenti hanno aggiunto all'operazione, espandere il nome dell'operazione.
- Per iniziare, terminare o ignorare un'operazione, espandere il nome dell'operazione e scegliere una delle seguenti opzioni:
  - Per avviare un'operazione, selezionare **Avvia** dall'elenco. Se l'operazione è definita come un'attività automatizzata in procedura operativa standard, il flusso di lavoro assegnato all'attività viene avviato automaticamente e l'operazione viene completata automaticamente. L'utente che avvia un'operazione diventa il proprietario di tale operazione, e il relativo nome viene visualizzato nel campo **Proprietario**.

- Per ignorare un'operazione, selezionare **Ignora** dall'elenco.
- Per terminare un'operazione, selezionare **Fine** dall'elenco.
- Per aggiungere un commento a un'operazione, utilizzare le seguenti operazioni secondarie:
  1. Espandere il nome dell'operazione.
  2. Dall'elenco, selezionare **Aggiungi commento**.
  3. Nella finestra Aggiungi commento, immettere un commento nel campo **Commento**. **Nome commentatore** e **Nome attività** sono campi di sola lettura e contengono valori immessi automaticamente.
  4. Fare clic su **OK**.
  5. Espandere di nuovo il nome dell'operazione. Il nuovo commento viene visualizzato alla fine dell'elenco di commenti e riferimenti esistenti per l'operazione.
- Per aggiungere un riferimento a un'operazione, utilizzare le seguenti operazioni secondarie:
  1. Espandere il nome dell'operazione.
  2. Dall'elenco, selezionare **Aggiungi riferimento**.
  3. Nella finestra Aggiungi riferimento, immettere i valori per **Nome riferimento** e **URI di riferimento**. **Nome attività** è un campo di sola lettura che contiene un valore immesso automaticamente.
  4. Fare clic su **OK**.
  5. Espandere di nuovo il nome dell'operazione. Il nuovo riferimento viene visualizzato come collegamento alla fine dell'elenco di commenti e riferimenti esistenti per l'operazione.
- Per visualizzare i dettagli di una procedura operativa standard, fare clic sull'icona  accanto al nome della procedura operativa standard. Nella finestra dei dettagli di SOP (Standard Operating Procedure) vengono visualizzate tutte le operazioni dell'attività incluse in procedura operativa standard, tra cui quelle in corso, idonee per essere avviate, completate e chiuse. Inoltre, vengono visualizzati lo stato e la data di fine di ciascuna operazione. Per visualizzare ulteriori dettagli relativi a un'operazione, espandere il nome dell'operazione.

## Personalizzazione del portlet Attività personali

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Per il portlet Attività personali, è possibile specificare un nome gruppo per abilitare la comunicazione con altri portlet; ad esempio, i portlet Dettagli.

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

### Concetti correlati:

“SOP (Standard Operating Procedure)” a pagina 127

È possibile definire procedure operative standard e le attività per la gestione degli eventi inseriti in IBM Intelligent Operations Center. Utilizzare il portlet SOP (Standard Operating Procedure) per accedere alle applicazioni procedura operativa standard, matrice di selezione procedura operativa standard e designer flusso di lavoro in Tivoli Service Request Manager.

### Riferimenti correlati:

“Impostazioni portlet Attività personali” a pagina 159

Personalizzare il portlet Attività personali modificando le impostazioni nei campi della finestra

### Impostazioni condivise.

## Notifiche

Utilizzare il portlet Notifiche per visualizzare i messaggi di avviso ed i relativi dettagli.

Il portlet Notifiche è una finestra interattiva che contiene un elenco di tutti gli avvisi correnti rilevanti. L'utente può vedere solo gli avvisi inviati ai gruppi di utenti di cui è membro. Gli avvisi sono notifiche che vengono ricevute quando:

- Si verificano più eventi nella stessa vicinanza e ad un orario simile; ciò potrebbe determinare conflitti o richiedere coordinazione
- Si verifica una modifica del valore KPI (Key Performance Indicator) predefinito, definita come trigger di avviso del proprio amministratore

Inoltre, è possibile utilizzare il portlet per visualizzare ulteriori dettagli relativi ad un avviso.

### Elenco Notifiche

Il portlet Notifiche fornisce un elenco interattivo e dinamico di avvisi determinato dalle modifiche degli indicatori KPI e degli eventi correlati. Lo scopo di questo portlet è di evidenziare le modifiche allo stato eventi o KPI. L'elenco contiene i dettagli chiave per ciascuno degli avvisi.

Per visualizzare una descrizione più dettagliata di un avviso, spostare il cursore del mouse sulla riga. Per visualizzare tutte le informazioni associate a quell'avviso in una finestra, fare clic con il tasto destro del mouse sulla riga e selezionare **Proprietà**.

All'inizio, quando si apre la pagina del portale, vengono visualizzati tutti gli avvisi correnti. Rimuovere un qualsiasi avviso dal portlet facendo clic con il tasto destro del mouse sulla riga e selezionando **Chiudi avviso**. È possibile chiudere più avvisi in questo modo selezionando più righe. Si consiglia di chiudere un avviso solo dopo averlo gestito correttamente poiché l'avviso viene rimosso per tutti i destinatari quando lo si chiude.

Fare clic sul pulsante nell'angolo in alto a destra della finestra per eseguire la cancellazione e ritornare all'elenco.

Un contatore nell'angolo sinistro della barra delle azioni posto alla fine dell'elenco indica il numero di elementi visualizzati e il numero totale di elementi. Nella parte centrale della barra delle azioni è possibile selezionare il numero di elementi da visualizzare contemporaneamente. Se vi sono più righe rispetto al numero consentito che è possibile visualizzare contemporaneamente, l'utente può scorrere avanti o indietro le pagine facendo clic sui pulsanti nell'angolo destro della barra delle azioni.

## Proprietà dell'avviso

La finestra per i dettagli relativi all'avviso visualizza le seguenti proprietà:

Tabella 93. Proprietà dell'avviso

Proprietà	Contenuto
Titolo	Breve descrizione dell'avviso
Categoria	Classificazione di livello superiore dell'evento o KPI
Mittente	Origine dell'avviso
Inviato ai gruppi	Gruppi a cui è stato inviato l'avviso
Inviato	Data e ora di invio dell'avviso
Descrizione	Descrizione aggiuntiva dell'avviso
Riferimenti agli avvisi	Identificativo evento, se l'avviso è causato da eventi correlati
Riferimenti agli indicatori KPI	Nome del KPI, se l'avviso è causato da un valore KPI che cambia

## Personalizzazione del portlet Notifiche

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Con l'impostazione dei parametri per il portlet Notifiche è possibile:

- Specificare il layout della colonna, le intestazioni, il criterio di ordinamento e la priorità.
- Mostrare o nascondere la barra degli strumenti nella parte superiore dell'elenco.

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

### Riferimenti correlati:

“Impostazioni portlet Notifiche” a pagina 160

Personalizzare il portlet Notifiche modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Report

Utilizzare il portlet Report per visualizzare un report di eventi come grafico. Il portlet fornisce diverse opzioni in base alle quali raggruppare gli eventi, ed è possibile scegliere gli eventi in base a una data o intervallo di date particolare. I report in questione consentono di pianificare gli eventi correnti e futuri.

## Creazione di report

È possibile creare un report personalizzato per eventi utilizzando il portlet Report. Innanzitutto, selezionare il modo in cui si desidera raggruppare gli eventi. Ad esempio, per visualizzare tutti gli eventi di una particolare categoria, selezionare **Categoria** nel campo **Raggruppa per**. Quindi, nei campi **Selezione dati**, scegliere i dati specifici per le informazioni che si desidera visualizzare. È possibile inoltre indicare una data o un intervallo di date per gli eventi presenti nel report. Fare clic su **Aggiorna** e il grafico cambia per riflettere le informazioni richieste.

Per richiamare l'URL per il nuovo report, fare clic su **URL per questo report**.

La Tabella 1 mostra le opzioni in base alle quali è possibile raggruppare gli eventi.

Tabella 94. Report personalizzato

Raggruppa per	Descrizione
Tipo evento	Visualizza gli eventi in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Gravità	Visualizza gli eventi in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Certezza	Visualizza gli eventi in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Urgenza	Visualizza gli eventi in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Categoria eventi	Visualizza gli eventi in base alla categoria eventi. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.
Tipo di messaggio	Visualizza gli eventi in base ai tipi di messaggi, ad esempio aggiornamenti o avvisi.
Stato	Visualizza gli eventi per stato. I livelli di stato sono: <ul style="list-style-type: none"> <li>• Accettabile</li> <li>• Attenzione</li> <li>• Esegui azione</li> </ul>
Mittente	Visualizza gli eventi in base ad un particolare mittente. Ad esempio, l'evento potrebbe essere un problema di sicurezza o un problema che riguarda IBM Intelligent Operations for Water.
Incidente	Visualizza gli eventi in base al tipo di incidente. Ad esempio, è possibile visualizzare tutti gli incidenti o costruzioni stradali.
Codice di gestione	Visualizza gli eventi per codice di gestione. Ad esempio, il codice di gestione potrebbe essere "evento".
Nome mittente	Visualizza gli eventi per nome del mittente.

La Tabella 2 mostra i dati che possono essere selezionati per il report.

Tabella 95. Selezione dati

Selezione dati	Descrizione
Gravità	Visualizza gli eventi in base alla gravità. Ad esempio, gli eventi possono essere estremi o gravi.
Certezza	Visualizza gli eventi in base alla probabilità che si verifichino. Ad esempio, se si è verificato un incidente stradale, la certezza potrebbe essere "osservato."
Urgenza	Visualizza gli eventi in base al grado di urgenza. Ad esempio, l'evento potrebbe verificarsi e potrebbe essere descritto come "immediato."
Categoria eventi	Visualizza gli eventi in base alla categoria eventi. Ad esempio, è possibile visualizzare tutti gli eventi ambientali, incendiari o di trasporto.



Tabella 95. Selezione dati (Continua)

Selezione dati	Descrizione
Tipo evento	Visualizza gli eventi in base al tipo. Ad esempio, l'evento potrebbe essere l'arrivo di un tornado o un incidente stradale.
Dalla data	Immettere la data per cui si stanno visualizzando gli eventi. Per un intervallo di date, immettere la data di inizio.
Alla data	Immettere la data fino alla quale si stanno visualizzando gli eventi.

**Nota:** Affinché questo portlet funzioni come previsto, è necessario collegarsi al portale della soluzione utilizzando il nome del dominio completo di IBM Intelligent Operations Centerserver delle applicazioni. Se ci si collega al portale utilizzando un indirizzo IP o un alias del nome host invece del nome di dominio completo registrato, questo portlet non viene visualizzato correttamente.

## Copia di un URL di report

Per copiare un URL di report e far sì che il report venga visualizzato in un frame sul lato destro del portlet, fare clic con il tasto destro del mouse sull'URL e selezionare **Copia indirizzo link**. La dicitura dell'opzione **Copia indirizzo link** varia a seconda del browser utilizzato.

### Importante:

Per salvare un report definito dall'utente e utilizzare il link copiato, immettere la data di ieri nel campo **Dalla data** e la data di domani nel campo **Alla data**. Queste date assicurano l'acquisizione di tutti i dati che si desidera includere nel report definito dall'utente. Ad esempio, per l'intervallo di date dal 10.8.2012 al 18.8.2012, immettere le seguenti date per i criteri di filtro:

- Dalla data - immettere 9.8.2012
- Alla data - immettere 19.8.2012

## Esempi di report

IBM Intelligent Operations Center dispone di un portlet Report che contiene report grafici basati su dati del portlet Eventi.

Il frame del report grande è l'area in cui vengono selezionati i parametri relativi alle informazioni che vengono visualizzate nel grafico del report.

I due frame presenti sul lato destro del portlet costituiscono l'ubicazione in cui vengono copiati i report definiti dall'utente.

I report presenti nella parte inferiore della pagina sono grafici predefiniti. Per configurare tali report affinché mostrino gli eventi per data o intervallo di date, fare clic su **Configura il report**. Immettere le date e fare clic su **Visualizza il report**.

## Integrazione dei report

Il portlet Report fornisce un IFrame per integrare pagine o report di IBM Cognos Business Intelligence. È possibile specificare l'URL del report o della pagina che si desidera integrare con il portlet.



## Personalizzazione del portlet Report

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, larghezza portlet e titolo portlet. È possibile inoltre specificare l'URL del report visualizzato.

### Riferimenti correlati:

“Impostazioni portlet Report” a pagina 162

Personalizzare il portlet Report modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

## Stato

Utilizzare il portlet Stato per visualizzare lo stato degli indicatori KPI (key Performance Indicator) per una singola organizzazione o per più organizzazioni.

Il portlet Stato fornisce un riepilogo di livello esecutivo dello stato degli indicatori KPI sulle organizzazioni per le quali si dispone dell'autorizzazione di visualizzazione. Utilizzare questo portlet per visualizzare modifiche aggiornate nello stato KPI, in modo che sia possibile pianificare e intraprendere eventuali azioni se necessario.

## Codice colore KPI

Ogni colonna contiene informazioni KPI relative a un'organizzazione indicata nella parte superiore della colonna. Le categorie KPI associate a ogni organizzazione sono rappresentate da celle colorate. Il colore di sfondo di una categoria KPI rispecchia il relativo stato. Se è necessario visualizzare più di sei KPI in una colonna, la dimensione di ogni singola cella viene ridotta per accogliere gli indicatori KPI supplementari.

Il codice dei colori di sfondo forniti con i KPI di esempio della soluzione è il seguente:

- Il verde indica che lo stato è accettabile, in base ai parametri per quel KPI.
- Il giallo indica che si richiede attenzione o monitoraggio.
- Il rosso indica che è necessario intraprendere un'azione.
- Il grigio indica che non sono disponibili dati sufficienti per calcolare lo stato KPI.

Il codice colore è definito nella legenda nella parte superiore del portlet.

Uno stato indeterminato indica che non è disponibile alcun valore KPI nel periodo di tempo definito per il KPI in questione. Questa situazione si verifica quando la soluzione non riceve messaggi per il KPI nel periodo di tempo specificato. Ad esempio, il livello d'acqua di una sorgente viene calcolato quotidianamente. Se non si riceve alcun messaggio sul livello d'acqua per quella sorgente in un particolare giorno, non esistono dati per determinare il valore KPI.

Per visualizzare il nome del KPI e una definizione dello stato rappresentato dal colore di un KPI, posizionare il cursore del mouse sulla cella.

## Aggiornamenti KPI

Quando viene modificato un KPI sottostante, la modifica si riflette nel portlet Stato. Ad esempio, uno dei KPI di esempio che determina lo stato KPI della qualità dell'acqua, cambia stato da accettabile ad attenzione. La modifica si riflette nel portlet mediante un cambiamento nel colore di sfondo della cella Qualità dell'acqua da verde a giallo. Inoltre, il portlet Notifiche indica che un KPI è stato modificato.

Quando la soluzione riceve un messaggio relativo al calcolo di un KPI, il colore cambia immediatamente. Questa funzione costituisce un vantaggio quando è verosimile che la categoria KPI riceva modifiche in tempo reale, come ad esempio, i ritardi aeroportuali. Essa non è rilevante per quelle categorie che contengono KPI cronologici, come il controllo delle piene. Per quelle categorie di KPI, vengono acquisite regolari misure quotidiane ed è improbabile che si verifichino improvvisi cambiamenti che influiscono sullo stato.

Per ciascun KPI, è possibile visualizzare tutti i KPI sottostanti ed i dettagli nel portlet Drill Down KPI (Key Performance Indicator) collegato al portlet Stato.

Per concentrarsi solo su uno specifico KPI del portlet Drill Down KPI (Key Performance Indicator), fare clic sulla cella KPI della tabella nel portlet Stato. È anche possibile fare clic sul titolo dell'organizzazione proprietaria, ad esempio, "Water", per visualizzare i KPI correlati.

## Personalizzazione del portlet Stato

Se si dispone dell'accesso di amministratore, è possibile personalizzare questo portlet. Fare clic sul pulsante nell'angolo in alto a destra del portlet per visualizzarne le opzioni di personalizzazione del menu. Le impostazioni condivise influiscono sul contenuto di questo portlet per tutti gli utenti, ma solo per questa ricorrenza del portlet.

Con l'impostazione dei parametri per il portlet Stato è possibile:

- Personalizzare i colori KPI.
- Abilitare un filtro KPI aggiuntivo.
- Mostrare o nascondere la legenda KPI.
- Definire la modalità di ordinamento dei KPI.
- Specificare un nome gruppo per abilitare la comunicazione con un portlet Drill Down KPI (Key Performance Indicator).

È possibile impostare parametri di portlet generici comuni sui portlet forniti: ubicazione file della guida, altezza portlet, titolo portlet e raggruppamento di risorse.

## Personalizzazione dei KPI

Viene fornito un insieme di KPI di esempio con la soluzione. I KPI in questione sono realizzati per fornire una guida alla pianificazione e all'implementazione dei diversi tipi di KPI ed essere adatti alla propria organizzazione. Sono forniti esempi in campo idrico, trasporti e sicurezza pubblica.

### Related concepts:

"KPI (Key Performance Indicators)" a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

### Related reference:

"Impostazioni portlet Stato" a pagina 164

Personalizzare il portlet Stato modificando le impostazioni nei campi della finestra **Impostazioni condivise**.

---

## Capitolo 9. Risoluzione dei problemi e supporto

Per isolare e risolvere problemi con il software IBM, è possibile utilizzare le informazioni della risoluzione dei problemi e del supporto, che contengono le istruzioni per utilizzare le risorse della determinazione dei problemi fornite con i prodotti IBM.

---

### Tecniche per la risoluzione dei problemi

La risoluzione dei problemi è un approccio sistematico per risolvere un problema. L'obiettivo della risoluzione dei problemi è determinare perché qualcosa non funziona come previsto e come risolvere il problema.

Il primo passo nel processo di risoluzione dei problemi è descrivere completamente il problema. Le descrizioni del problema sono utili all'utente e al rappresentante del supporto tecnico IBM per capire dove iniziare la ricerca della causa del problema. Questo passo include porsi alcune domande di base:

- Quali sono i sintomi del problema?
- Dove si verifica il problema?
- Quando si verifica il problema?
- In quali condizioni si verifica il problema?
- È possibile riprodurre il problema?

Le risposte a queste domande in genere portano ad una buona descrizione del problema, che in seguito può condurre ad una risoluzione del problema.

#### Quali sono i sintomi del problema?

Quando si inizia a descrivere un problema, la domanda più ovvia è "Qual è il problema?" Questa domanda potrebbe sembrare diretta, tuttavia è possibile scomporla in alcune domande più precise che creano un quadro più descrittivo del problema. Queste domande possono includere:

- Chi, o cosa, sta riportando il problema?
- Quali sono i codici di errore e i messaggi di errore?
- In che modo il sistema dà errore? Ad esempio, è un loop, un blocco, un arresto anomalo, un calo delle prestazioni o un risultato non corretto?

#### Dove si verifica il problema?

Determinare dove ha origine il problema non è sempre facile ma è uno dei passi più importanti nella risoluzione di un problema. Possono esistere molti livelli di tecnologia tra la segnalazione e i componenti in errore. Reti, dischi e driver sono solo alcuni dei componenti da prendere in considerazione quando si indaga sui problemi.

Le seguenti domande sono utili per concentrare l'attenzione su dove si verifica il problema per isolarne il livello:

- Il problema è specifico ad una piattaforma o un sistema operativo, o è comune a più piattaforme o sistemi operativi?
- L'ambiente e la configurazione correnti sono supportati?

Se un livello riporta un problema, non necessariamente ha origine in quel livello. Parte dell'identificazione del punto in cui ha origine un problema è capire l'ambiente in cui esiste. Descrivere completamente l'ambiente del problema, incluso il sistema operativo e la versione, tutto il software

corrispondente e le versioni, e le informazioni hardware. Confermare che si è in esecuzione in un ambiente con una configurazione supportata; molti problemi possono risalire a livelli non compatibili del software che non sono intesi per essere eseguiti insieme o che non sono stati testati insieme in modo esauriente.

## **Quando si verifica il problema?**

Sviluppare una sequenza temporale dettagliata degli eventi che portano ad un errore, specialmente per i casi in cui si verifica un'unica volta. È possibile sviluppare una sequenza temporale molto facilmente andando all'indietro: iniziare dal momento in cui è stato riportato l'errore (il più precisamente possibile, fino al millisecondo), e andare a ritroso tra i log e le informazioni disponibili. In genere è necessario tornare indietro solo fino al primo evento sospetto individuato in un log diagnostico.

Per sviluppare una sequenza temporale dettagliata degli eventi, rispondere a queste domande:

- Il problema si verifica ad una certa ora del giorno o della notte?
- Con che frequenza si verifica il problema?
- Quale sequenza di eventi porta al momento in cui viene riportato il problema?
- Il problema si verifica dopo un cambiamento di ambiente, ad esempio dopo un aggiornamento o un'installazione di software o hardware?

La risposta a questi tipi di domande può fornire una cornice di riferimento in cui indagare sul problema.

## **In quali condizioni si verifica il problema?**

Sapere quali sistemi e applicazioni sono in esecuzione quando si verifica un problema è una parte importante della risoluzione dei problemi. Queste domande relative all'ambiente possono aiutare l'utente a identificare la causa principale del problema:

- Il problema si verifica sempre quando viene eseguita la stessa attività?
- Deve verificarsi una determinata sequenza di eventi perché si verifichi il problema?
- Altre applicazioni presentano errori in contemporanea?

La risposta a questi tipi di domande può essere utile per spiegare l'ambiente in cui si verifica il problema e correlare eventuali dipendenze. Tenere presente che più problemi non sono necessariamente correlati solo perché si sono verificati più o meno contemporaneamente.

## **È possibile riprodurre il problema?**

Da un punto di vista della risoluzione dei problemi, il problema ideale è quello che può essere riprodotto. In genere, quando un problema può essere riprodotto si ha a disposizione una serie più ampia di strumenti o procedure per facilitare le indagini. Di conseguenza, i problemi che possono essere riprodotti sono spesso i più facili da risolvere e di cui eseguire il debug. Tuttavia, i problemi che possono essere riprodotti possono avere uno svantaggio: se il problema ha un impatto significativo sul business, non si desidera che si ripeta. Se possibile, ricreare il problema in un ambiente di test o di sviluppo, che in genere offre una maggiore flessibilità e un maggiore controllo durante l'indagine.

- È possibile ricreare il problema su un sistema di test?
- Più utenti o applicazioni riscontrano lo stesso tipo di problema?
- È possibile ricreare il problema eseguendo un singolo comando, una serie di comandi o un'applicazione particolare?

### **Informazioni correlate**

“Ricerca nei knowledge base” a pagina 322

Spesso è possibile trovare le soluzioni ai problemi effettuando ricerche nei knowledge base IBM. È possibile ottimizzare i risultati utilizzando le risorse disponibili, gli strumenti di supporto e i metodi di ricerca.

---

## Abilitazione delle tracce e visualizzazione dei file di log

Per risolvere un problema in IBM Intelligent Operations Center, potrebbe essere necessario analizzare i file di log in diversi sistemi. I seguenti argomenti forniscono una guida su come accedere ai file di log.

Per avviare le tracce e visualizzare i log, immettere i comandi al runtime come utente root.

### Concetti correlati:

“Verifica dei componenti” a pagina 210

Lo strumento Controllo di verifica del sistema esegue il test dei componenti presenti in IBM Intelligent Operations Center per verificare se sono accessibili e funzionanti.

“Installazione ed utilizzo di IBM Support Assistant Lite” a pagina 303

IBM Support Assistant Lite (ISA Lite) è uno strumento che raccoglie dati di diagnostica comuni utili per analizzare problemi generali.

### Attività correlate:

“Esecuzione dello strumento "must gather" dell'installazione” a pagina 299

Durante l'installazione di IBM Intelligent Operations Center vengono generati dei file di log. Uno strumento è disponibile per raccogliere questi file di log per l'analisi.

## File di log del Server delle applicazioni

Utilizzare le seguenti procedure per abilitare le tracce e visualizzare i log per alcuni dei sistemi sul server delle applicazioni.

Le seguenti procedure descrivono come abilitare le tracce e visualizzare i log per i seguenti sistemi:

- WebSphere Portal
- IBM WebSphere Business Monitor

## Abilitazione della traccia e visualizzazione dei log su WebSphere Portal

### Informazioni su questa attività

I log di WebSphere Portal sono in `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal`. Seguire i passi contenuti nella procedura per avviare una traccia e visualizzare un log.

### Procedura

1. Collegarsi alla console di gestione all'indirizzo `http://app-host:9060/ibm/console`, dove **app-host** è il nome host completo del server delle applicazioni.
2. Fare clic su **Risoluzione dei problemi > Log e traccia**.
3. Fare clic su **WebSphere\_Portal > Modifica dettagli livello di log**.
4. Fare clic sulla scheda **Runtime** e inserire il seguente comando:  

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```
5. Fare clic su **OK**.
6. Per visualizzare un log, immettere i seguenti comandi:  

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

## Abilitazione della traccia e visualizzazione dei log per IBM WebSphere Business Monitor sul server delle applicazioni

### Informazioni su questa attività

I log per IBM WebSphere Business Monitor sul server delle applicazioni si trovano all'indirizzo `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/`. Seguire i passi contenuti nella procedura per avviare una traccia e visualizzare un log.

## Procedura

1. Collegarsi alla console di gestione all'indirizzo `http://app-host:9060/ibm/console`, dove **app-host** è il nome host completo del server delle applicazioni.
2. Fare clic su **Risoluzione dei problemi > Log e traccia**.
3. Fare clic su **WBM\_DE.AppTarget.WBMNode1.0 > Modifica dettagli livello di log**.
4. Fare clic sulla scheda **Runtime** ed incollare il codice a livello di traccia riportato di seguito: `*=info: com.ibm.wbm.*=finest: com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all: com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Fare clic su **OK**.

### Informazioni correlate:

 [Documentazione del prodotto IBM WebSphere Portal 7](#)

## File di log del Server eventi

Utilizzare le seguenti procedure per abilitare le tracce e visualizzare i log per alcuni dei sistemi sul server eventi.

Le seguenti procedure descrivono come abilitare le tracce e visualizzare i log per i seguenti sistemi:

- Tivoli Service Request Manager
- WebSphere MQ e WebSphere Message Broker
- Probe XML Tivoli Netcool/OMNIBus
- Database Tivoli Netcool/OMNIBus (server di oggetti)
- Database Tivoli Netcool/OMNIBus (agent processo)
- Tivoli Netcool/Impact

## Abilitazione della traccia e visualizzazione dei file di log per Tivoli Service Request Manager

### Informazioni su questa attività

Utilizzare la seguente procedura per eseguire il debug del flusso di informazioni da Tivoli Service Request Manager a IBM Intelligent Operations Center.

## Procedura

1. Nell'interfaccia utente di Tivoli Service Request Manager, fare clic su **Go To > System configuration > Platform Configuration > Logging**.
2. In **Root Loggers**, nel campo del filtro, immettere **integration**.
3. Espandere **integration**.
4. Configurare il logger di integrazione:
  - a. Per **Log Level**, fare clic sull'icona **Select Value**. Nella finestra **Select Value**, fare clic su **DEBUG**.
  - b. Per **Appenders**, fare clic sull'icona **Manage Appenders**. Nella finestra **Manage Appenders**, selezionare la casella di spunta **Dailyrolling** e fare clic su **OK**.
  - c. Selezionare la casella di spunta **Active?**.
  - d. Fare clic sull'icona **Save Logger**.
5. Dall'elenco **Select Action**, selezionare **Set Logging Root Folder**.
6. Nella finestra **Set Logging Root Folder**, per **Root Logging Folder**, immettere `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1` e fare clic su **OK**.
7. Fare clic sull'icona **Save Logger**.
8. Dall'elenco **Select Action**, selezionare **Apply Settings**.



9. Per visualizzare il log, in un terminale di server Tivoli Service Request Manager, immettere i seguenti comandi:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs
tail -f event-host_MXServer_maximo_scheduled.log
```

dove *event-host* è il nome host del server eventi.

#### Attività correlate:

“Verifica dei file di log” a pagina 338

Verificare il file di log della politica Tivoli Netcool/OMNIBus ed i file di log di Tivoli Service Request Manager.

## Abilitazione della traccia e visualizzazione dei file di log per WebSphere MQ e WebSphere Message Broker

### Informazioni su questa attività

I log per WebSphere MQ e WebSphere Message Broker vengono memorizzati nelle seguenti ubicazioni:

- /var/mqm/errors
- /var/mqm/qmgrs/IOC!MB!QM/errors

I file di traccia vengono scritti nella directory /var/mqm/trace. È possibile attivare la traccia per un singolo gestore code o tutti i gestori code, come illustrato nella procedura riportata di seguito.

### Procedura

1. Per avviare, arrestare o formattare una traccia, scegliere il comando appropriato:
  - Per avviare una traccia per tutti i processi, immettere il seguente comando: `strmqtrc -e`
  - Per avviare una traccia per il gestore code IBM Intelligent Operations Center, immettere il seguente comando: `strmqtrc -m IOC.MB.QM`
  - Per avviare una traccia dettagliata per il gestore code IBM Intelligent Operations Center, immettere il seguente comando: `strmqtrc -t all -t detail -m IOC.MB.QM`
  - Per arrestare tutte le tracce, immettere il seguente comando: `endmqtrc -a`
  - Per formattare i file di traccia binari in formato ASCII, immettere il seguente comando: `dspmqtrc *.TRC`
2. Per controllare lo stato di WebSphere Message Broker:
  - a. Immettere il seguente comando: `ps -ef | grep IOC_BROKER`
  - b. Controllare lo stato dei seguenti processi:
    - `bipservice IOC_BROKER`
    - `bipbroker IOC_BROKER`
    - `biphttplistener IOC_BROKER`
    - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

## Abilitazione della traccia e visualizzazione dei file di log per il probe XML di Tivoli Netcool/OMNIBus

### Informazioni su questa attività

I log di WebSphere Portal si trovano in /opt/IBM/netcool/omnibus/log/ioc\_xml.log. Seguire i passi contenuti nella procedura per avviare una traccia e visualizzare un log.

### Procedura

1. Aprire un terminale sul server eventi.
2. Immettere il seguente comando: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`

3. Se non viene visualizzato il messaggio Connection status OK in fondo al file, per ridenominare il file di log corrente, immettere il seguente comando: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. Se non viene visualizzato il messaggio Connection status OK, potrebbe anche essere visualizzato il messaggio Probe shutting down. Per riavviare il probe, immettere il seguente comando:  
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
5. Dopo circa 1 minuto, immettere nuovamente il seguente comando: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
6. Se il messaggio Connection status OK non viene ancora visualizzato, cercare gli errori nel file `/opt/IBM/netcool/omnibus/log/ioc_xml.log`. Un problema di connessione potrebbe indicare che il server di oggetti non sia attivo. Consultare la seguente sezione, *Abilitazione della traccia e visualizzazione dei log per il database Tivoli Netcool/OMNIBus (server di oggetti)*.

## Abilitazione della traccia e visualizzazione dei file di log per il database Tivoli Netcool/OMNIBus (server di oggetti)

### Informazioni su questa attività

I file di log si trovano nelle seguenti ubicazioni:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`, ad esempio:
  - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`

Seguire i passi contenuti nella procedura per avviare una traccia e visualizzare un log.

### Procedura

1. Collegarsi ad un terminale come utente root.
2. Immettere il seguente comando: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. Se viene richiesto se si desidera importare da `omni.dat`, fare clic su **yes** e quindi su **finish**.
4. Ridurre a icona la finestra dell'agent del processo.
5. Fare clic con il tasto destro del mouse su **NCOMS**.
6. Scegliere l'opzione appropriata:
  - Se l'opzione **Connect As...** non è visualizzata, è necessario avviare il server di oggetti NCOMS:
    - a. Per avviare il server di oggetti NCOMS, chiudere `nco_config` ed immettere il seguente comando:  
`/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
    - b. Se il server di oggetti NCOMS non si avvia, cercare un file `NCOMS.pid` nella directory `/opt/IBM/netcool/omnibus/var` ed eliminarlo, quindi provare di nuovo ad avviare il server.
  - Se l'opzione **Connect As...** è visualizzata, fare clic su **Connect As...**, quindi per il nome utente immettere `root` ed inserire la password.
7. Una volta avviato il server NCOMS, per riavviare il probe immettere il seguente comando:  
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
8. Per visualizzare un file di log, immettere il seguente comando: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

### File di log del database Tivoli Netcool/OMNIBus (agent processo)

Il file di log del Database Tivoli Netcool/OMNIBus (agent processo) si trova in `/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

## Abilitazione e visualizzazione dei file di log Tivoli Netcool/Impact

### Informazioni su questa attività

Il file di log si trova in `opt/IBM/netcool/impact/log/`. Seguire i passi contenuti nella procedura per avviare una traccia e visualizzare un log.

#### Procedura

1. Accedere alla console di gestione Tivoli Netcool/Impact all'indirizzo `http://event-host:9080/nci` con il nome utente `admin`, dove `event-host` è il nome host completo del server eventi. Se non viene visualizzata una richiesta di login, immettere i seguenti comandi in una finestra di terminale:  

```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```
2. Nella finestra dello stato dei servizi scorrere verso il basso ed accertarsi che i seguenti servizi siano in esecuzione, indicato da un simbolo verde:
  - IOC\_CAP\_Event\_Reader
  - IOC\_Notification\_Reader
3. Inoltre, nella finestra dello stato dei servizi fare clic sull'icona **View Log** accanto a **PolicyLogger** per vedere se sono visualizzati eventuali errori nel log.
4. Se nel log sono presenti uno o più errori, per ulteriori dettagli consultare i file di log nella seguente directory: `/opt/IBM/netcool/impact/log/`
5. Se sono necessari ulteriori dettagli, impostare i livelli di log superiori. Fare clic su **PolicyLogger**, impostare il valore **Highest log level** su 3 e selezionare le caselle di spunta appropriate.

#### Operazioni successive

È possibile attivare vari log al runtime tramite la console di gestione di WebSphere Application Server. Per ulteriori informazioni sull'attivazione della traccia del portale ed altre tracce disponibili da WebSphere Portal, vedere il link accanto all'inizio dell'argomento della documentazione prodotto di WebSphere Portal e cercare *Registrazione e traccia*.

#### Attività correlate:

“Verifica dei file di log” a pagina 338

Verificare il file di log della politica Tivoli Netcool/OMNIBus ed i file di log di Tivoli Service Request Manager.

## Esecuzione dello strumento "must gather" dell'installazione

Durante l'installazione di IBM Intelligent Operations Center vengono generati dei file di log. Uno strumento è disponibile per raccogliere questi file di log per l'analisi.

#### Procedura

1. Collegarsi a server di installazione come `root` e aprire una finestra terminale.
2. Passare alla directory `install_home/ioc/bin`.
3. Eseguire il comando `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` per impostare la variabile `JAVA_HOME` in modo che utilizzi Java 6 runtime JRE.
4. Eseguire il comando `./mustgather.sh -p password` dove `password` è la password della topologia. Lo strumento analizza il file delle proprietà della topologia la prima volta che viene eseguito. Se il file delle proprietà della topologia viene modificato dopo l'esecuzione dello strumento, aggiungere `-n` al comando per far sì che lo strumento esegua nuovamente la scansione del file delle proprietà della topologia. Ad esempio, `./mustgather.sh -n -p password`.

## Risultati

I log raccolti e le altre informazioni vengono scritti nella directory `install_media/mustGather` su server di installazione. Vi sarà un file con estensione `.tar` per ciascuno dei server.

Le informazioni raccolte includono:

- Log per tutte le fasi di installazione, compreso un log per ciascun componente installato su ciascun nodo.
- Log di installazione dello strumento Controllo di verifica del sistema.
- I file XML della topologia.
- Tutti gli script utilizzati durante il processo di installazione.
- Tutti gli indirizzi delle vulnerabilità di Cyber hygiene.
- Gli script di Cyber hygiene.

### Concetti correlati:

“Abilitazione delle tracce e visualizzazione dei file di log” a pagina 295

Per risolvere un problema in IBM Intelligent Operations Center, potrebbe essere necessario analizzare i file di log in diversi sistemi. I seguenti argomenti forniscono una guida su come accedere ai file di log.

“Risoluzione dei problemi dei componenti”

È possibile utilizzare lo strumento Controllo di verifica del sistema per risolvere i problemi dei componenti in IBM Intelligent Operations Center.

### Attività correlate:

“Riavvio dell'installazione dell'architettura IBM Intelligent Operations Center durante un'installazione dettagliata” a pagina 49

In caso di errore dell'installazione dell'architettura, è possibile riavviare l'installazione.

“Scambio di informazioni con IBM” a pagina 326

Per diagnosticare o identificare un problema, potrebbe essere necessario fornire al supporto IBM i dati e le informazioni dal proprio sistema. In altri casi il supporto IBM potrebbe fornire all'utente gli strumenti o le utilità da utilizzare per la determinazione dei problemi.

---

## Risoluzione dei problemi dei componenti

È possibile utilizzare lo strumento Controllo di verifica del sistema per risolvere i problemi dei componenti in IBM Intelligent Operations Center.

Per ulteriori informazioni sullo strumento Controllo di verifica del sistema vedere il link alla fine dell'argomento.

Le tabelle delle sezioni che seguono elencano le ubicazioni dei file di log per ognuno dei server contenuti in IBM Intelligent Operations Center. Tutti i file di log vengono creati automaticamente. Visualizzarli utilizzando i comandi `tail` appropriati.

### Server di installazione

Per informazioni sulla raccolta di file di log di installazione, vedere l'argomento relativo all'esecuzione dello strumento di raccolta delle informazioni. Andare al link alla fine dell'argomento.

## Server delle applicazioni

Tabella 96. Componenti e file di log del Server delle applicazioni

Componente	File di log
IBM Cognos Administration	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemErr.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log</li> <li>• Tutti i log della directory /opt/IBM/cognos/c10_64/logs/</li> </ul>
IBM HTTP Server	<ul style="list-style-type: none"> <li>• /opt/IBM/HTTPServer/logs/error_log</li> <li>• /opt/IBM/HTTPServer/logs/access_log</li> </ul>
IBM WebSphere Business Monitor	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log</li> </ul>
IBM Lotus Sametime Proxy Server	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log</li> </ul>
Tivoli Access Manager	<ul style="list-style-type: none"> <li>• /var/pdweb/log/msg_*.log dove * è un qualsiasi valore.</li> <li>• /var/pdweb/log/config_data_*.log dove * è qualsiasi valore</li> </ul>
Tivoli Access Manager WebSEAL	<ul style="list-style-type: none"> <li>• /var/pdweb/log/msg_webseald-default.log</li> <li>• Tutti i log della directory /var/pdweb/www-default/log/</li> </ul>
Log di configurazione di Tivoli Directory Server Proxy	<ul style="list-style-type: none"> <li>• /datahome/proxy/idsslpad-tdsproxy/logs/ibmslapd.log</li> </ul>
WebSphere Operational Decision Management	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log</li> </ul>
WebSphere Portal	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log</li> <li>• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log</li> </ul>
WebSphere UDDI Registry	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log</li> </ul>

## Server di dati

Tabella 97. Componenti e file di log del Server di dati

Componente	File di log
Tivoli Directory Server	<ul style="list-style-type: none"> <li>• /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log</li> <li>• Tutti i log della directory /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/</li> </ul>

## Server eventi

Tabella 98. Componenti e file di log del Server eventi

Componente	File di log
Lotus Domino	<ul style="list-style-type: none"> <li>• /local/notesdata/console.out</li> <li>• /local/notesdata/log.nsf</li> <li>• Tutti i file di log presenti nella directory /local/notesdata/IBM_TECHNICAL_SUPPORT/.</li> </ul>
Lotus Sametime Community Server	Per raccogliere e scrivere tutti i file log pertinenti nella directory /local/notesdata/, immettere il seguente comando: /local/notesdata/sh stdiagzip.sh
Tivoli Netcool/Impact	<ul style="list-style-type: none"> <li>• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log</li> <li>• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log</li> </ul>
Tivoli Netcool/OMNIBus	<ul style="list-style-type: none"> <li>• /opt/IBM/netcool/log</li> <li>• /opt/IBM/netcool/omnibus/log</li> </ul>
Tivoli Service Request Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log</li> </ul>

## Server di gestione

Tabella 99. Componenti e file di log del Server di gestione

Componente	File di log
Server di gestione	<ul style="list-style-type: none"> <li>• Tivoli Event Monitoring Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log</li> <li>• Tivoli Event Portal Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log</li> <li>• File di log Embedded WebSphere Application Server: <ul style="list-style-type: none"> <li>– Log di errori: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log</li> <li>– Log di output: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log</li> <li>– Log di avvio: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log</li> </ul> </li> </ul>
Tivoli Access Manager e WebSphere Portal Manager	<ul style="list-style-type: none"> <li>• /var/PolicyDirector/log/msg__pdmgrd_utf8.log</li> <li>• /var/PolicyDirector/log/msg__pdacld_utf8.log</li> </ul>

Tabella 99. Componenti e file di log del Server di gestione (Continua)

Componente	File di log
Tivoli Access Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log</li> </ul>
Tivoli Enterprise Monitoring Agent	<ul style="list-style-type: none"> <li>• /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log</li> </ul>
Tivoli Enterprise Portal	<ul style="list-style-type: none"> <li>• /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log</li> </ul>
Tivoli Identity Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log</li> <li>• Tutti i log delle directory secondarie V6 della directory /var/idsldap/</li> </ul>

**Concetti correlati:**

“Gestione file di log” a pagina 261

IBM Intelligent Operations Center memorizza i file di log in varie diverse ubicazioni. Per evitare problemi di prestazioni del sistema, periodicamente archiviare i file di log e rimuovere i file di log originali.

**Attività correlate:**

“Esecuzione dello strumento "must gather" dell'installazione” a pagina 299

Durante l'installazione di IBM Intelligent Operations Center vengono generati dei file di log. Uno strumento è disponibile per raccogliere questi file di log per l'analisi.

**Informazioni correlate:**

Come utilizzare lo strumento Controllo di verifica del sistema

Lo strumento Controllo di verifica del sistema viene utilizzato per determinare lo stato operativo di servizi compreso il sistema IBM Intelligent Operations Center.

## Installazione ed utilizzo di IBM Support Assistant Lite

IBM Support Assistant Lite (ISA Lite) è uno strumento che raccoglie dati di diagnostica comuni utili per analizzare problemi generali.

ISA Lite raccoglie i seguenti tipi di informazione:

- File di determinazione dei problemi di piattaforma
- File di log e di traccia di sistema
- File di provisioning di piattaforma
- File di configurazione del sistema
- File di dump Java™
- File di log interni del framework di determinazione dei problemi

Per scaricare ISA Lite per IBM Intelligent Operations Center 1.5, vedere il link alla fine dell'argomento.

Per installare e utilizzare ISA Lite, seguire le istruzioni nella documentazione Quick Start Guide inclusa nel package del download.



**Informazioni correlate:**

 Download di IBM Support Assistant Lite per IBM Intelligent Operations Center 1.5

---

## Messaggi di IBM Intelligent Operations Center

Ogni argomento di messaggio è utile per identificare la causa di una particolare condizione di errore in IBM Intelligent Operations Center e suggerisce le azioni da intraprendere per risolvere l'errore.

Per facilitare la comprensione degli errori che potrebbero verificarsi durante l'utilizzo di IBM Intelligent Operations Center, ogni argomento di messaggio viene suddiviso in tre sezioni: il messaggio visualizzato in IBM Intelligent Operations Center o nei relativi log, una spiegazione e un'azione.

**Il messaggio**

Contiene due identificativi, che sono l'identificazione dell'errore e il testo associato. L'identificazione dell'errore è l'ID messaggio. Si tratta di un numero univoco che identifica un messaggio. Il carattere finale E indica che il messaggio deriva da un errore, W indica un messaggio di avvertenza e I indica un messaggio informativo.

**La spiegazione**

Contiene un'ulteriore spiegazione del messaggio.

**La risposta utente**

Suggerisce l'azione correttiva per risolvere l'errore.

Per facilitare la ricerca di informazioni relative ad un messaggio di errore, immettere il numero ID del messaggio di errore nel campo di ricerca nel centro informazioni.

**Nota:** Gli argomenti di questa sezione contengono solo messaggi specifici di IBM Intelligent Operations Center. Per tutti gli altri messaggi, consultare la documentazione del prodotto.

---

### CIYBA0101E Il file della topologia {0} non è valido.

**Spiegazione:** Il programma di installazione ha tentato di convalidare il file della topologia {0} ed ha rilevato che il file della topologia conteneva degli errori. Questi errori possono includere:

- Non tutti i componenti richiesti esistono nel file della topologia.
- I componenti prerequisiti non sono elencati prima dei componenti dipendenti.
- I componenti che dovrebbero essere distribuiti in sequenza sono in stanza di sviluppo parallelo.

**Risposta dell'utente:** Correggere il file della topologia ed eseguire nuovamente l'installazione.

---

### CIYBA0102E Impossibile trovare la topologia o i file delle specifiche della topologia.

**Spiegazione:** Ogni topologia di installazione ha un file .xml ed una specifica associati. Impossibile trovare uno o più di questi file.

**Risposta dell'utente:** Accertarsi che tutti i file di installazione sono stati estratti in server di installazione. Verificare che la proprietà `image.basedir.local` nel file `custom.properties` è impostata nell'ubicazione corretta. Il file `custom.properties` è presente nella sottodirectory `/resource` in server di installazione dove è stato

estratto il package di installazione.

---

### CIYBA0103E Non esiste lo script {0} per installare un componente.

**Spiegazione:** Il programma di installazione ha tentato di individuare uno script per un componente ed è impossibile trovare tale script.

**Risposta dell'utente:** Verificare che il supporto di installazione è stato estratto in server di installazione. Verificare che la directory di base è stata configurata correttamente nel file `custom.properties`. La directory di base viene utilizzata per dedurre l'ubicazione dello script di installazione.

---

### CIYBA0104E Il file della topologia contiene voci non valide.

**Spiegazione:** Il programma di installazione ha rilevato un errore durante la lettura del file della topologia e la creazione delle unità distribuibili per ogni componente. In genere si tratta di un errore interno a meno che non sia installata una topologia personalizzata.

Il file della topologia potrebbe essere danneggiato oppure specificato in modo non corretto

**Risposta dell'utente:** Verificare il file della topologia per i seguenti problemi:

- ID componenti duplicati.
- Attributi ID componenti o tipo mancanti.
- Specifica di un attributo di connessione in cui non esiste alcun componente principale.
- La topologia non riesce a convalidare lo schema XML.

---

**CIYBA0105E Impossibile trovare il file {0}.**

**Spiegazione:** Il programma di installazione non ha trovato il file {0}.

**Risposta dell'utente:** Accertarsi che tutti i file di installazione sono stati estratti in server di installazione. Verificare che il file `image.basedir.local` property in the `custom.properties` è impostato per l'ubicazione corretta. Il file `custom.properties` è presente nella sottodirectory `/resource` in server di installazione dove è stato estratto il package di installazione.

---

**CIYBA0106E Impossibile salvare il file {0}.**

**Spiegazione:** Il programma di installazione ha tentato di scrivere il file denominato {0} ed è stato restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che è possibile accedere all'ubicazione specificata utilizzando l'ID utente del programma di installazione. Accertarsi che ci sia spazio sufficiente sul disco e che la partizione non è danneggiata.

---

**CIYBA0107E Impossibile trovare il riferimento della proprietà {0} nel file della topologia {1}**

**Spiegazione:** Durante l'installazione alcuni componenti richiedono i valori proprietà dal software prerequisite. Questi componenti utilizzano i riferimenti alle proprietà nel file della topologia per determinare i valori proprietà richiesti. Impossibile trovare il riferimento alla proprietà nel file della topologia.

**Risposta dell'utente:** Il file della topologia è danneggiato. Ciò potrebbe essere causato da modifiche manuali che hanno introdotto voci non valide o perché l'installazione non ha scritto un file della topologia con valori corretti. Determinare quali componenti sono stati installati in modo non corretto. Rimuovere i componenti installati in modo non corretto, correggere il file della topologia e installare di nuovo.

---

**CIYBA0108E Impossibile trovare il componente {0} nel file della topologia {1}.**

**Spiegazione:** Il programma di installazione prevedeva di trovare l'ID componente {0} nel file della topologia {1}. Impossibile trovare l'ID componente. Il problema potrebbe essere causato da una dipendenza specificata in modo non corretto in un elemento di connessione di un altro componente.

**Risposta dell'utente:** Esaminare il file della topologia

per i riferimenti a {0}. Correggere gli elementi di connessione non corretti per il componente {0} e installare di nuovo.

---

**CIYBA0109E La proprietà {0}.{1} nel file della topologia {2} non è valida.**

**Spiegazione:** La proprietà non è stata trovata nel file della topologia o in un file delle proprietà delle specifiche.

**Risposta dell'utente:** Se manca, aggiungere la proprietà al file delle proprietà delle specifiche o al file della topologia. Questo errore potrebbe anche essere causato dalla proprietà che non era corretta. Correggere il file della topologia o il file delle proprietà delle specifiche e installare di nuovo.

---

**CIYBA0110E Impossibile trovare la proprietà {0}.{1} nel file della topologia {2}.**

**Spiegazione:** Un'unità distribuibile fa riferimento ad un'altra unità distribuibile indicata dal ruolo {1}. Impossibile trovare l'unità distribuibile dipendente o si è verificata una mancata corrispondenza nei ruoli.

**Risposta dell'utente:** Il file della topologia indicato contiene riferimenti alla proprietà mostrata, ma è impossibile trovare la definizione della proprietà nel file della topologia. Questa situazione può verificarsi se il file della topologia è stato modificato manualmente ed è stato rimosso un componente, ma esistono ancora dei riferimenti a tale componente.

---

**CIYBA0111E Impossibile richiamare l'host principale per il componente {0}.**

**Spiegazione:** Un componente della topologia deve essere associato ad un host di destinazione. Viene specificato un componente della topologia orfano.

**Risposta dell'utente:** Verificare il componente della topologia {0} ed accertarsi che ha una sequenza di attributi di connessione che alla fine ha un componente con un attributo host.

---

**CIYBA0112E Impossibile leggere il file della topologia {0}**

**Spiegazione:** Il programma di installazione non è stato in grado di leggere il file della topologia specificato.

**Risposta dell'utente:** Verificare che il file della topologia indicato è presente nella directory di installazione e che il programma di installazione può accedere alla directory.

---

**CIYBA0113E Impossibile salvare il file {0}.**

**Spiegazione:** Il programma di installazione non è riuscito a salvare il file indicato

**Risposta dell'utente:** Verificare che il programma di installazione ha accesso alla directory di installazione.

---

**CIYBA0114E Impossibile impostare la proprietà 0}{1}.**

**Spiegazione:** Il programma di installazione non è stato in grado di aggiornare la proprietà indicata.

**Risposta dell'utente:** Il file della topologia è danneggiato o è stato modificato manualmente e sono stati introdotti valori della proprietà non validi. Correggere il file della topologia ed eseguire nuovamente l'installazione.

---

**CIYBA0115E Impossibile trovare il file della topologia {0}.**

**Spiegazione:** Il programma di installazione non è stato in grado di accedere al file della topologia indicato.

**Risposta dell'utente:** Verificare che il file della topologia è presente nella directory specificata dal programma di installazione e accertarsi che il programma di installazione può accedere alla directory.

---

**CIYBA0116E Impossibile scrivere il file delle proprietà {0}.**

**Spiegazione:** Il programma di installazione non è stato in grado di scrivere il file delle proprietà indicato.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione ha accesso alle directory temporanee sui server di destinazione. La directory sui server di destinazione in cui verranno scritti gli script di installazione temporanei viene specificata dalla proprietà `Unix.script.basedir.remote` nel file `custom.properties`. Correggere il valore di questa proprietà se non è stato specificato correttamente.

---

**CIYBA0117E Il programma di installazione non è riuscito a creare il keystore.**

**Spiegazione:** Il programma di installazione non è riuscito a creare il keystore.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le sottodirectory in cui il supporto di installazione è stato estratto.

---

**CIYBA0118E Il programma di installazione non è stato in grado di accedere al keystore utilizzando la password fornita. La password non è corretta o il keystore è danneggiato.**

**Spiegazione:** Il programma di installazione non è stato in grado di accedere al keystore.

**Risposta dell'utente:** Verificare che la password fornita è corretta e il keystore non è danneggiato. Rigenerare il keystore con una nuova password installando di nuovo la soluzione.

---

**CIYBA0119E Impossibile codificare la proprietà {0} nel file della topologia {1}.**

**Spiegazione:** Il programma di installazione ha tentato di codificare la proprietà indicata utilizzando la password fornita nel file della topologia e non è stato in grado di farlo.

**Risposta dell'utente:** Verificare che il keystore non è danneggiato e che la password per la topologia è corretto. Se necessario, ricreare il keystore con una nuova password mediante la reinstallazione.

---

**CIYBA0120E Impossibile decodificare la proprietà {0} nel file della topologia {1}**

**Spiegazione:** Non è riuscito il tentativo di leggere e decodificare la proprietà indicata.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione può accedere al file della topologia indicato e che il file della topologia è presente nell'ubicazione prevista. Verificare che la password e la chiave segreta siano corrette. Rieseguire l'installazione.

---

**CIYBA0121E Il file keystore {0} già esiste.**

**Spiegazione:** Questo errore non dovrebbe verificarsi utilizzando l'installazione IBM Installation Manager. IBM Installation Manager controlla il flusso di installazione ed assicura, laddove non viene effettuato un tentativo, di rigenerare il keystore.

**Risposta dell'utente:** Verificare che l'installazione non è stata già eseguita. Rieseguire il programma di installazione una volta che è stato rimosso il keystore esistente da un precedente tentativo di installazione.

---

**CIYBA0122E Il keystore per la topologia non esiste. Eseguire il comando `createSecretKey`.**

**Spiegazione:** Questo errore non dovrebbe verificarsi quando si esegue l'installazione IBM Installation Manager. L'installazione IBM Installation Manager accetta automaticamente la `SecretKey` e genera il keystore.

**Risposta dell'utente:** Se si esegue un'installazione

step-by-step seguire le procedure per generare un keystore.

---

**CIYBA0123E La topologia {0} non è completamente installata.**

**Spiegazione:** Il programma di installazione ha rilevato che non tutti i componenti nella topologia sono stati installati.

**Risposta dell'utente:** Verificare il file della topologia e individuare quali componenti non sono stati installati. Riavviare l'installazione.

---

**CIYBA0124E Impossibile trovare il file delle proprietà {0}.**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file delle proprietà indicato. Tuttavia, è impossibile trovare il file.

**Risposta dell'utente:** Verificare che il package di installazione è stato estratto correttamente. Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le directory in cui è stato estratto il package.

---

**CIYBA0125E Impossibile scrivere nel file delle proprietà {0}**

**Spiegazione:** Il programma di installazione ha tentato di aggiornare un file con i valori della variabile di runtime ed è stata restituita un'eccezione di I/O.

**Risposta dell'utente:** Verificare che è possibile accedere all'ubicazione specificata utilizzando l'ID utente del programma di installazione. Verificare che è disponibile spazio sufficiente nel file system e che la partizione del disco non è danneggiata.

---

**CIYBA0126E Impossibile impostare il valore per la proprietà {0} dal file della topologia {1}**

**Spiegazione:** Il programma di installazione non è riuscito ad impostare il valore della proprietà specificata.

**Risposta dell'utente:** Verificare che la proprietà nel file della topologia indicato ha la sintassi XML corretta. Verificare che il file della topologia non è danneggiato o nel formato corretto. Rimuovere i caratteri speciali dal file e riavviare l'installazione.

---

**CIYBA0127E Impossibile leggere il file delle specifiche della soluzione {0}**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file indicato ed è stato restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che il file esiste nell'ubicazione specificata. Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a

tutte le directory in cui è stato estratto il package.

---

**CIYBA0128E Impossibile salvare il file {0}.**

**Spiegazione:** Il programma di installazione ha tentato di scrivere il file indicato ed è stato restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione può accedere all'ubicazione specificata. Verificare che esiste spazio sufficiente nel file system e che la partizione del disco non è danneggiata.

---

**CIYBA0129E Impossibile leggere il file del package della soluzione {0}.**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file indicato e viene restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che il file esiste nell'ubicazione specificata. Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le directory in cui è stato estratto il package.

---

**CIYBA0130E Il file del package della soluzione : {0} non esiste.**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file indicato e viene restituito un errore di I/O del file

**Risposta dell'utente:** Verificare le autorizzazioni per il file indicato nel messaggio. Accertarsi che l'ID utente utilizzato dal programma di installazione dispone dell'autorizzazione per leggere il file. Modificare le autorizzazioni per il file, se necessario

---

**CIYBA0131E Il programma di installazione non è riuscito a caricare il file della topologia {0}. Il messaggio di I/O del file era {1}.**

**Spiegazione:** L'errore indicato è stato restituito quando si è tentato di importare il file della topologia specificato.

**Risposta dell'utente:** Verificare che il file della topologia indicato è presente nella corretta directory. Verificare che il file della topologia non contiene alcun carattere non valido. Verificare che il programma di installazione può accedere alla directory contenente il file della topologia.

---

**CIYBA0140E Impossibile accedere ai file di installazione richiesti.**

**Spiegazione:** Il programma di installazione ha tentato di leggere un file richiesto e non è stato in grado di farlo.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione può accedere

all'ubicazione in cui è stato estratto il package di installazione. Accertarsi che la partizione del disco non è danneggiata. Estrarre di nuovo il package di installazione e ritentare l'installazione.

---

**CIYBA0141E Impossibile individuare il file di installazione {0}.**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file indicato ed è stato restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che il file esiste nell'ubicazione specificata. Verificare che l'ID utente utilizzato dal programma di installazione può accedere a tutte le directory contenenti il package di installazione estratto.

---

**CIYBA0142E Impossibile scrivere il file di installazione {0}.**

**Spiegazione:** Il programma di installazione ha tentato di scrivere il file indicato e viene restituito un errore di I/O del file.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le directory contenenti il package di installazione estratto. Verificare che la partizione del disco non è danneggiata e non è eseguita senza spazio sufficiente.

---

**CIYBA0143E Il programma di installazione non è riuscito ad elaborare il file della topologia.**

**Spiegazione:** Il programma di installazione legge il file della topologia e genera dei file intermedi contenenti i valori di runtime. Il programma di installazione ha rilevato un errore durante l'elaborazione del file della topologia e durante la scrittura dei file intermedi. Gli errori di I/O del file costituiscono la probabile causa di questo errore.

**Risposta dell'utente:** Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le directory in cui il package di installazione è stato estratto. Verificare che la partizione del disco non è danneggiata o non abbia spazio sufficiente.

---

**CIYBA0150E Impossibile leggere il file delle specifiche della topologia {0}.**

**Spiegazione:** Il programma di installazione ha tentato di leggere il file indicato ed è stato restituito un I/O file.

**Risposta dell'utente:** Verificare che il file esiste nell'ubicazione specificata. Verificare che l'ID utente utilizzato dal programma di installazione ha accesso a tutte le directory da cui il package di installazione è stato estratto.

---

**CIYBA0160E Impossibile trovare il file delle specifiche della regola nella directory {0}.**

**Spiegazione:** Il programma di installazione ha tentato di caricare il file rule-spec.xml che definisce le regole di pre-verifica e non è stato in grado di caricarlo.

**Risposta dell'utente:** Verificare che la directory indicata esiste. Inoltre accertarsi che l'ID utente utilizzato dal programma di installazione può accedere a tale directory.

---

**CIYBA0161E Il nome della regola {0} non è valido.**

**Spiegazione:** Il programma di installazione ha identificato un nome regola non corretto nel file rule-spec.xml. Questo file definisce le regole utilizzate dalla fase di pre-verifica.

**Risposta dell'utente:** Verificare che il nome regola sia corretto nel file rule-spec.xml. Fare riferimento ad una versione non modificata del file rule-spec.xml per il nome regola corretto.

---

**CIYBA0162E La verifica dei prerequisiti di installazione non è riuscita per la topologia {0}.**

**Spiegazione:** La fase di pre-verifica non è riuscita in quanto una o più destinazioni di configurazione non soddisfa i requisiti di sistema supportati.

**Risposta dell'utente:** Verificare che la topologia pianificata soddisfi i requisiti minimi supportati.

---

**CIYBA0163W Il tipo di sistema operativo del server di destinazione {0} non è {1}.**

**Spiegazione:** La fase di pre-verifica ha rilevato un sistema operativo non supportato sul server di destinazione indicato.

**Risposta dell'utente:** Accertarsi che il sistema operativo sul server di destinazione soddisfi i requisiti di sistema.

---

**CIYBA0164W Era previsto che il server {0} avesse un sistema operativo a {1} bit.**

**Spiegazione:** La fase di pre-verifica ha rilevato un sistema operativo non corretto sul server di destinazione.

**Risposta dell'utente:** Verificare che il tipo di sistema operativo sul server di destinazione soddisfi i requisiti di sistema.

---



---

**CIYBA0165W** La CPU del server di destinazione {0} non è una CPU x86 o s390 64bit.

**Spiegazione:** La fase di pre-verifica ha rilevato un tipo di CPU non supportato per il server di destinazione indicato.

**Risposta dell'utente:** Verificare che il tipo di CPU per il server di destinazione soddisfi i requisiti di sistema.

---

**CIYBA0166E** Impossibile connettersi al server di destinazione {0}.

**Spiegazione:** Il programma di installazione non si connette al server remoto durante l'esecuzione della fase di pre-verifica.

**Risposta dell'utente:** Verificare la connettività tra server di installazione e i server di destinazione. Verificare i log di pre-verifica per gli altri errori.

---

**CIYBA0167E** Impossibile connettersi al server {0} perché è stato specificato un nome host, account o password errato.

**Spiegazione:** Il programma di installazione ha avuto esito negativo durante la fase di pre-verifica. Il programma di installazione non è stato in grado di connettersi al server di destinazione.

**Risposta dell'utente:** Verificare che il nome host è nel formato corretto e che i dettagli di login siano corretti per il server remoto. Verificare i log di pre-verifica per ulteriori informazioni.

---

**CIYBA0168E** L'ora o il fuso orario per i server {0} {0} non sono sincronizzati.

**Spiegazione:** Esiste una differenza tra gli orari o i fusi orari impostati per i server.

**Risposta dell'utente:** Verificare che l'ora e i fusi orari siano uguali per tutti i server.

---

**CIYBA0169W** Verificare il tipo di sistema operativo e l'architettura CPU sul server {0}

**Spiegazione:** La fase di pre-verifica del programma di installazione ha rilevato un sistema operativo e un'architettura CPU non supportati per il server di destinazione.

**Risposta dell'utente:** Accertarsi che tutti i server soddisfano i requisiti di sistema per la soluzione.

---

**CIYBA0170W** Verifica del fuso orario e data e & ora su tutti i server.

**Spiegazione:** Questo messaggio è seguito dalla parola "riuscito" o "non riuscito". Quanto di seguito riportato determina l'azione da compiere.

**Risposta dell'utente:** Se il messaggio è seguito da

"riuscito", non è richiesta alcuna risposta. Se il messaggio è seguito da "non riuscito", i server devono essere sincronizzati. I parametri di sistema relativi al fuso orario, data e ora devono essere uguali per ogni nodo nella topologia.

---

**CIYBA0171I** La verifica dei prerequisiti di installazione è iniziata utilizzando l'istanza {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0172I** La verifica dei prerequisiti di installazione è terminata correttamente.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0173I** La verifica dei prerequisiti di installazione è terminata con {0} avvertenze e {1} errori:

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0176E** Le informazioni di login per il server {0} non sono corrette. Verificare l'ID utente e password per il server.

**Spiegazione:** La fase di pre-verifica del programma di installazione ha rilevato informazioni di login non corrette per il server di destinazione.

**Risposta dell'utente:** Verificare che i dettagli account per il server hanno ID utente e password corretti.

---

**CIYBA0177W** Impossibile connettersi al server remoto. Attendere per ritentare.

**Spiegazione:** La fase di pre-verifica del programma di installazione non è riuscita a connettersi al server remoto. Si ritenterà la connessione.

**Risposta dell'utente:** Non è richiesta alcuna azione. Il programma di installazione attenderà il tempo specificato nella proprietà `waiting.time` nel file `custom.properties` e quindi ritenterà la connessione.

---

**CIYBA0178W** Impossibile connettersi a {0}, attendere {1} millisecondi prima del prossimo tentativo di connessione

**Spiegazione:** Nel sistema sono presenti problemi di connettività.

**Risposta dell'utente:** Se più tentativi di connessione

hanno avuto esito negativo, contattare l'amministratore di rete per risolvere i problemi di connettività e ritentare l'installazione.

---

**CIYBA0179E Nel file delle proprietà della topologia non è stato fornito alcun valore per la chiave {0}.**

**Spiegazione:** La fase di pre-verifica del programma di installazione non è riuscita a recuperare i valori per il nome host, il nome utente o la password dal file delle proprietà.

**Risposta dell'utente:** Verificare che il nome host, il nome utente e la password siano specificati correttamente nel file delle proprietà.

---

**CIYBA0180E L'ID utente immesso per il server {0} non dispone dei privilegi root.**

**Spiegazione:** La fase di pre-verifica del programma di installazione ha rilevato che l'account utilizzato per il server indicato non dispone dei privilegi root.

**Risposta dell'utente:** Modificare l'ID utente per il server in uno che dispone dei privilegi oppure aggiungere i privilegi root all'ID utente specificato per il server.

---

**CIYBA0181E Verificare l'ID e la password dell'utente root per il server {0}.**

**Spiegazione:** L'operazione di pre-verifica del programma di installazione ha rilevato che l'ID utente utilizzato per il server ha diritti di accesso insufficienti.

**Risposta dell'utente:** Verificare che l'account dispone dei diritti di accesso sufficienti.

---

**CIYBA0182E Verificare la connettività dal server di installazione per {0}**

**Spiegazione:** L'operazione di pre-verifica del programma di installazione non è riuscita a connettersi tra server di installazione e il server di destinazione

**Risposta dell'utente:** Verificare la connettività tra i server. Esaminare i log di pre-verifica per ulteriori informazioni.

---

**CIYBA0183E Il valore {0} per la chiave {1} non è valido, dovrebbe essere "EM64T" o "AMD64" o "S390".**

**Spiegazione:** Il valore della chiave dovrebbe essere uno dei valori specificati.

**Risposta dell'utente:** Correggere il valore e rieseguire l'installazione.

---

**CIYBA0184E Il valore {0} per la chiave {1} non è un nome host valido**

**Spiegazione:** L'operazione di pre-verifica del programma di installazione ha determinato che il valore fornito non è un nome host valido.

**Risposta dell'utente:** Verificare che il nome host sia nel formato corretto e abbia un valore corretto.

---

**CIYBA0185E La verifica dei prerequisiti di installazione non è riuscita per la regola {0}**

**Spiegazione:** La fase di pre-verifica del programma di installazione ha avuto esito negativo durante il controllo della regola specificata.

**Risposta dell'utente:** Verificare i log di pre-verifica per ulteriori messaggi. Correggere l'errore e tentare nuovamente l'installazione.

---

**CIYBA0187E Il keystore SSH "{0}" è stato specificato, ma non è possibile accedervi. Il protocollo SSH basato sui certificati non sarà disponibile. Dettagli: {1}.**

**Spiegazione:** L'operazione di pre-verifica del programma di installazione ha rilevato dei dati non validi nel keystore SSH durante il tentativo di connessione al server di destinazione.

**Risposta dell'utente:** Esaminare i dettagli nel messaggio e verificare che il keystore fornito abbia voci adeguate.

---

**CIYBA0190E Il componente {0} deve comparire prima del componente {1} nel file della topologia.**

**Spiegazione:** Il file della topologia è stato modificato in modo non corretto. Un componente prerequisito compare dopo un componente che dipende da questo.

**Risposta dell'utente:** Modificare il file della topologia in modo che i componenti che hanno dipendenze vengano dopo i componenti da cui dipendono.

---

**CIYBA0191E Esiste una dipendenza tra il componente {0} e il componente {1} nel file della topologia. I componenti non possono essere distribuiti in parallelo.**

**Spiegazione:** I componenti non possono essere distribuiti in parallelo se esiste una dipendenza tra di loro. Ad esempio, se il componente 2 è un prerequisito del componente 1.

**Risposta dell'utente:** Rimuovere i componenti dalla stanza parallela del file della topologia.



---

**CIYBA0192E** La proprietà {1}.{2} ha un valore di riferimento non valido di {0} nel file della topologia.

**Spiegazione:** Il valore di riferimento incluso nel messaggio non è valido per la proprietà indicata.

**Risposta dell'utente:** Utilizzare il campo ID per trovare la definizione della proprietà ed accertarsi che tutti i riferimenti alla proprietà abbiano il valore corretto.

---

**CIYBA0193E** Il componente {0} ha connessioni duplicate {1} identificate nel file della topologia.

**Spiegazione:** Le connessioni duplicate per il componente sono definite nel file della topologia.

**Risposta dell'utente:** Rimuovere le informazioni di connessione duplicata nel file della topologia e rieseguire il programma di installazione.

---

**CIYBA0194E** La proprietà {0} è duplicata nel componente {0}

**Spiegazione:** È definita una proprietà duplicata per il componente

**Risposta dell'utente:** Rimuovere la proprietà duplicata per il componente nel file delle proprietà.

---

**CIYBA0195E** Il componente {0} nel file della topologia ha una proprietà non valida {0}.

**Spiegazione:** La proprietà specificata era imprevista per il componente indicato. Ciò potrebbe essere causato da una proprietà digitata non correttamente o da una proprietà mancante dalla specifica della proprietà

**Risposta dell'utente:** Aggiungere la proprietà specificata al file delle proprietà o alla topologia. Se la proprietà non era digitata correttamente, correggere l'ortografia. Correggere il file della topologia o il file delle proprietà della specifica e riavviare l'installazione.

---

**CIYBA0196E** Al componente {1} manca la proprietà {0}

**Spiegazione:** Il componente deve avere la proprietà indicata. L'errore potrebbe essere causato da una proprietà con errore di ortografia o manca una proprietà dal file di specifica delle proprietà.

**Risposta dell'utente:** Aggiungere la proprietà al file di specifica delle proprietà o alla topologia. Se si tratta di un errore di ortografia, correggere l'ortografia. Riavviare l'installazione.

---

**CIYBA0197E** Il componente {1} ha specificato un tipo di componente {1} non valido.

**Spiegazione:** È stato specificato un tipo di componente non valido per il componente.

**Risposta dell'utente:** Verificare che il file di specifica per il componente contenga il tipo di componente. I file di specifica componente si trovano nella sottodirectory *install\_home/spec/component* sul server di installazione.

---

**CIYBA0198E** La connessione {0} non è valida per il componente {1}

**Spiegazione:** La connessione definita non è valida per il componente.

**Risposta dell'utente:** Verificare l'ortografia della connessione del file di tipologia per il componente ed accertarsi che non sia errata.

---

**CIYBA0199E** Manca la connessione {0} dal componente {1}.

**Spiegazione:** Nessuna connessione è definita per il componente indicato.

**Risposta dell'utente:** Verificare il file di specifica del componente ed accertarsi che siano incluse le informazioni della connessione.

---

**CIYBA0200E** Le informazioni della connessione per {0} non esistono.

**Spiegazione:** Manca l'ID connessione per il componente indicato.

**Risposta dell'utente:** Verificare che l'ID connessione sia specificato nel file della topologia. Verificare che l'ID connessione sia scritto correttamente e faccia riferimento ad una stanza nel file della topologia che definisce il componente associato per l'ID connessione.

---

**CIYBA0201E** Impossibile connettersi al server remoto {0}.

**Spiegazione:** Il programma di installazione ha rilevato un problema di connettività al server indicato.

**Risposta dell'utente:** Verificare che non vi siano problemi di connessione tra i server. Eseguire il passo di verifica preliminare del programma di installazione e risolvere eventuali problemi di connettività.

---

**CIYBA0202E** Il nome utente o la password non è valido per il server {0}.

**Spiegazione:** Il programma di installazione ha rilevato credenziali non valide per il server indicato.

**Risposta dell'utente:** Verificare che le credenziali del server siano corrette nel file della topologia.

---

---

**CIYBA0203E** Il file {0} non esiste.

**Spiegazione:** Un tentativo di caricare il file delle proprietà ha restituito un errore.

**Risposta dell'utente:** Verificare che il percorso del file delle proprietà sia corretto e che il file esista.

---

**CIYBA0204E** Impossibile leggere/scrivere il file {0}.

**Spiegazione:** Il programma di installazione ha tentato di caricare il file delle proprietà ed è stato restituito un errore.

**Risposta dell'utente:** Verificare che il percorso del file delle proprietà sia corretto e che il file indicato esista.

---

**CIYBA0205E** Impossibile creare la directory {0} su {1}.

**Spiegazione:** Il programma di installazione non è riuscito a creare una directory sul server remoto.

**Risposta dell'utente:** Verificare che vi sia spazio a sufficienza sul server remoto e che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e delle autorizzazioni adeguate per creare una directory.

---

**CIYBA0206E** Impossibile caricare il file {0} nella directory remota {1} sul server {2}.

**Spiegazione:** Il programma di installazione non è riuscito a copiare i file nella directory indicata sul server remoto.

**Risposta dell'utente:** Verificare che vi sia spazio sufficiente sul server remoto e che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e dell'autorizzazione adeguata per scrivere file nel server remoto.

---

**CIYBA0207E** Nessuna immagine definita per {0}.

**Spiegazione:** Il programma di installazione non è riuscito a richiamare i dati dell'immagine per il file delle proprietà.

**Risposta dell'utente:** Verificare che il file delle proprietà contenga un campo immagine con il componente dati.

---

**CIYBA0208E** Impossibile caricare l'immagine del componente {0} per il server remoto {1}.

**Spiegazione:** Il programma di installazione non è riuscito a copiare i file immagine in una directory sul server remoto.

**Risposta dell'utente:** Verificare che vi sia spazio sufficiente sul server remoto e che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e dell'autorizzazione adeguata per scrivere nella directory sul server remoto. Verificare

inoltre che il nome della directory remota sia corretto.

---

**CIYBA0209I** Nome host: {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0210I** OSType={0},OSBit={1},CPUArch={2}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0211I** Percorso remoto: {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0212I** Percorso locale: {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0213E** Impossibile scaricare il file {0} dal server remoto {1}.

**Spiegazione:** Il programma di installazione non è riuscito a copiare i file immagine da una directory di server remoto sul server locale.

**Risposta dell'utente:** Verificare che vi sia spazio a sufficienza sul server locale e che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e delle autorizzazioni adeguate per scrivere nella directory. Inoltre verificare che i nomi delle directory locale e remota siano corretti.

---

**CIYBA0214E** Download del file {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0215I** Comando: {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0216I** Codice di uscita del comando: {0}.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA02171 Output del comando: {0}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0218E Il comando non è riuscito con codice di ritorno {0}.**

**Spiegazione:** Il comando non è stato completato correttamente.

**Risposta dell'utente:** Controllare i file di log per ulteriori dettagli.

---

**CIYBA0219I Caricamento del file {0}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0220I Directory immagine locale: {0}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0221I Directory immagine remota: {0}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0222E L'immagine remota {0} esiste già.**

**Spiegazione:** Il file esiste già sul server di destinazione. Il processo di installazione include il trasferimento del supporto sui server di destinazione. Questo messaggio indica che l'immagine richiesta è già stata trasferita.

**Risposta dell'utente:** Questo messaggio indica che esiste ancora il supporto di un'installazione precedente sui server di destinazione. Se l'utente intendeva avviare una nuova installazione, il supporto deve essere eliminato per poter essere caricato nuovamente.

---

**CIYBA0223E Impossibile avviare il comando sul server {0}.**

**Spiegazione:** Il programma di installazione non è riuscito ad eseguire il comando **IOC** dal server remoto sul server locale.

**Risposta dell'utente:** Verificare la connessione tra il server locale e il server remoto. Verificare che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e dell'autorizzazione adeguata per eseguire il comando.

---



---

**CIYBA0224E Acquisisci i file di backup dalla cartella {0} sul server {1}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0225E Impossibile richiamare i file di backup dalla cartella {0} sul server {1}.**

**Spiegazione:** Il programma di installazione non è riuscito a richiamare i file da una cartella di backup remota su una cartella locale.

**Risposta dell'utente:** Verificare la connessione tra il server locale e il server remoto. Verificare che l'ID utente utilizzato dal programma di installazione disponga di diritti di accesso sufficienti e dell'autorizzazione adeguata per accedere alle cartelle.

---

**CIYBA0226E Non esiste alcuna cartella {0} sul server {1}.**

**Spiegazione:** Il programma di installazione non è riuscito a richiamare i file da una cartella di backup remota su una cartella locale.

**Risposta dell'utente:** Verificare che la directory remota e la cartella esistano.

---

**CIYBA0227E È necessario fornire un valore per gli attributi id e path.**

**Spiegazione:** L'installazione non è riuscita ad identificare gli attributi ID e path del componente.

**Risposta dell'utente:** Verificare che gli argomenti ID e path del componente siano forniti all'interno degli argomenti dell'attività.

---

**CIYBA0228I Comando exec: {0}.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0229E Spazio su disco insufficiente nella directory di destinazione {0}.**

**Spiegazione:** Il programma di installazione non ha rilevato spazio sufficiente nella directory di destinazione.

**Risposta dell'utente:** Verificare che la directory indicata abbia sufficiente spazio assegnato e che possa essere acceduta dall'ID utente utilizzato dal programma di installazione.

---

---

**CIYBA0230I** Riga comandi IOC versione: {0}

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0231I** Topologia "{0}" importata correttamente

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0232E** Il nome della topologia "{0}" non è presente nella cartella ../topology

**Spiegazione:** Il programma di installazione non è riuscito a individuare la topologia indicata nella cartella ../topology.

**Risposta dell'utente:** Verificare che il file della topologia esista nella cartella ../topology e che sia in un formato XML valido.

---

**CIYBA0233I** La topologia corrente è "{0}".

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0234E** ANT\_HOME non impostata o impostata in modo errato. Impostare ANT\_HOME.

**Spiegazione:** Il programma di installazione ha riscontrato un problema nella variabile di ambiente ANT\_HOME.

**Risposta dell'utente:** Verificare che la variabile ANT\_HOME sia impostata su una versione ANT valida.

---

**CIYBA0237E** L'ID componente "{0}" non è valido.

**Spiegazione:** Il programma di installazione ha rilevato un ID componente non corretto nel file della topologia.

**Risposta dell'utente:** Verificare che l'ID componente esista e sia denominato correttamente nel file della topologia.

---

**CIYBA0238E** L'azione "{0}" per l'ID componente "{1}" non è valida.

**Spiegazione:** L'azione indicata non è corretta per il componente corrente nel file della topologia.

**Risposta dell'utente:** Controllare il file della topologia ed accertarsi che l'azione definita sia adatta al componente.

---



---

**CIYBA0239E** Se si desidera che i messaggi operativi siano più dettagliati, selezionare {0}.

**Spiegazione:** Il comando non è stato completato correttamente.

**Risposta dell'utente:** Controllare il file di log indicato da {0} per le azioni da intraprendere.

---

**CIYBA0240I** Comando terminato correttamente.

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0241E** Comando non riuscito:

**Spiegazione:** Il comando visualizzato non è riuscito.

**Risposta dell'utente:** L'azione da intraprendere dipenderà dal comando non riuscito. Riesaminare il comando e i log per determinare la causa dell'errore.

---

**CIYBA0242E** Rimuovere ".xml" dal parametro "{0}".

**Spiegazione:** Il parametro mostrato include l'estensione file .xml.

**Risposta dell'utente:** I parametri dei nomi file XML non devono includere l'estensione .xml. Rimuovere .xml dal parametro e riprovare il comando.

---

**CIYBA0243E** Le variabili di ambiente IOP\_CIPHER\_ALG o IOP\_CIPHER\_KEYSIZE sono impostate in modo errato. Impostarle con valori appropriati compatibili con JCE."

**Spiegazione:** Il programma di installazione non è riuscito a identificare un valore corretto per la cifratura utilizzata per la codifica.

**Risposta dell'utente:** Verificare che le variabili di ambiente CIPHER\_ALG e IOP\_CIPHER\_KEYSIZE siano impostate correttamente.

---

**CIYBA0244E** "{0}" non è un parametro valido.

**Spiegazione:** Il parametro indicato non è un parametro valido.

**Risposta dell'utente:** Rimuovere o correggere il parametro e riprovare il comando.

---

**CIYBA0245E** Parametro mancante "-{0}".

**Spiegazione:** Il parametro indicato è obbligatorio ma manca dal comando.

**Risposta dell'utente:** Rieseguire il comando con il parametro mancante.

---

---

**CIYBA0249I Preparare gli script dell'operazione.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0250I Operazione completata.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0251I Sequenza dell'operazione avviata.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0252I Sequenza dell'operazione terminata.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0253I Caricamento delle immagini del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0254I Installazione del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0255I Disinstallazione del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0256I Avvio del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0257I Arresto del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0258I Propagazione del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0259I OK**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0261I Sono in esecuzione {0} attività**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0262I Verranno eseguite le {0} attività totali**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0263I Backup del componente {{0}} sull'host {{1}}**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0264E Impossibile caricare il file di configurazione {0}.**

**Spiegazione:** La funzione di registrazione non riesce a trovare il file che contiene i parametri di registrazione della configurazione.

**Risposta dell'utente:** Verificare che il package di installazione sia stato estratto completamente e che si trovi su un file system accessibile all'ID utente che esegue il programma di installazione.

---

**CIYBA0265E Impossibile creare il gestore file per il log.**

**Spiegazione:** La funzione di registrazione ha tentato di aprire un file utilizzando un handle di file di sistema e non ci è riuscita.

---



**Risposta dell'utente:** Chiedere all'amministratore di sistema di verificare il numero di handle di file disponibili sul sistema. Assicurarsi che il file system su cui è stato estratto il package di installazione non sia danneggiato.

---

**CIYBA0266E Il RPM richiesto {0} non è installato sul server {1}.**

**Spiegazione:** Il package RPM indicato non è installato sul server.

**Risposta dell'utente:** Installare il package RPM supportato sul server.

---

**CIYBA0267E Il server {1} non dispone dello spazio su disco necessario. È richiesto {0} di spazio su disco.**

**Spiegazione:** Il server non dispone dello spazio su disco necessario o il server non soddisfa i requisiti di sistema per lo spazio su disco.

**Risposta dell'utente:** Eliminare dei file per liberare spazio sul server in modo da soddisfare i requisiti minimi di spazio.

---

**CIYBA0268E Il server {1} non dispone della memoria necessaria. Sono necessari {0} GB di memoria.**

**Spiegazione:** Non vi è RAM sufficiente sul server indicato. Il server non soddisfa i requisiti di sistema per la RAM minima.

**Risposta dell'utente:** Aggiungere RAM al server.

---

**CIYBA0269E Impossibile creare la directory {0} sul server {1}. La directory esiste già.**

**Spiegazione:** La directory specificata esiste già sul server.

**Risposta dell'utente:** Rimuovere la directory sul server.

---

**CIYBA0270E La porta tcp ip {0} è già in uso sul server {1}. Si tratta di una porta obbligatoria che deve essere disponibile prima dell'installazione.**

**Spiegazione:** Il programma o il processo è già configurato per utilizzare una porta TCP/IP obbligatoria sul server.

**Risposta dell'utente:** Riconfigurare il server in modo che la porta richiesta sia disponibile. Eseguire nuovamente l'installazione.

---

**CIYBA0271E Il server {1} non ha il nome host completo previsto. Il nome host completo previsto è {0}.**

**Spiegazione:** Il server non ha il nome host completo previsto.

**Risposta dell'utente:** Se si sta utilizzando l'installazione IBM Installation Manager, immettere il nome host completo per il server. Se si sta utilizzando l'installazione dettagliata, immettere il nome host completo nella sezione SERVERS del file delle proprietà della topologia. Correggere il server visualizzato nel messaggio di errore.

---

**CIYBA0272E La connessione di rete dal server {1} al server {0} è interrotta.**

**Spiegazione:** Non è presente connettività di rete tra i due server indicati.

**Risposta dell'utente:** Controllare la connettività tra i server. Se il problema persiste, contattare l'amministratore della rete di sistema.

---

**CIYBA0273E Il server {0} ha in esecuzione SELinux che non è supportato.**

**Spiegazione:** SELinux non è supportato da IBM Intelligent Operations Center.

**Risposta dell'utente:** Installare una versione Linux supportata.

---

**CIYBA0274E Sul server {0} è stato rilevato un firewall attivo. Prima dell'installazione è necessario disabilitare tutti i firewall.**

**Spiegazione:** Il server ha un firewall attivo.

**Risposta dell'utente:** Disabilitare il firewall sul server durante il processo di installazione.

---

**CIYBA0275E Impossibile trovare una voce DNS per il server {0}. La ricerca DNS in base all'IP o al nome host non è riuscita.**

**Spiegazione:** Il server non è stato configurato correttamente nel DNS o il DNS non sta funzionando correttamente. Il comando di ricerca DNS per indirizzo IP e per nome host non è riuscito per il server.

**Risposta dell'utente:** Contattare l'amministratore di rete del sistema per il server e correggere la voce DNS del DNS

---

**CIYBA0276E Il server {1} ha un'impostazione di sistema che non soddisfa i requisiti di installazione. Il numero massimo di file aperti [unlimit] è inferiore a {0}.**

**Spiegazione:** L'impostazione del sistema per il

numero massimo di file aperti non soddisfa i requisiti dell'installazione.

**Risposta dell'utente:** L'impostazione `ulimit` deve essere modificata nel valore indicato.

**CIYBA0277E** La richiesta Linux rilevata non soddisfa i requisiti di installazione. La release prevista è {0}.

**Spiegazione:** La versione Linux installata sul server indicato non è supportata.

**Risposta dell'utente:** Installare una versione Linux supportata.

**CIYBA0278E** La distribuzione Linux rilevata non soddisfa i requisiti. La distribuzione prevista è {0}

**Spiegazione:** La versione Linux installata non è supportata.

**Risposta dell'utente:** Installare una distribuzione Linux supportata.

**CIYBA0279E** Il profilo WebSphere Application Server {0} non è stato avviato o l'account o la password non sono validi sul server {4}.

**Spiegazione:** Il profilo WebSphere Application Server non è stato avviato o è stato effettuato un tentativo di avviarlo con credenziali non valide.

**Risposta dell'utente:** Avviare il profilo WebSphere Application Server utilizzando ID utente e password corretti.

**CIYBA0281E** Il server {0} non ha IPv6 abilitato. Abilitare IPv6 sul server prima dell'installazione.

**Spiegazione:** Il server indicato non ha IPv6 configurato.

**Risposta dell'utente:** Abilitare IPv6 sul server indicato.

**CIYBA0282E** Alcuni dei file ubicati nella directory {0} sul server dei supporti sono danneggiati.

**Spiegazione:** Tutti i file dell'installazione devono avere checksum MD5 che devono essere verificati prima dell'installazione. Il checksum MD5 su alcuni file ubicati nella directory indicata non hanno checksum MD5 validi.

**Risposta dell'utente:** Estrarre nuovamente il package di installazione o copiare di nuovo i file nella directory.

**CIYBA0283E** SSH sul server {0} non è configurato correttamente. L'autenticazione della password con SSH è necessaria ma non è configurata sul server.

**Spiegazione:** La configurazione SSH sul server indicato non è corretta.

**Risposta dell'utente:** Riconfigurare il file `/etc/ssh/sshd_config` nel modo seguente:

- Rimuovere tutte le istruzioni `AllowUsers`.
- Specificare `YES` per `PermitRootLogin`.
- Specificare `YES` per `Password Authentication`.

Queste modifiche consentiranno solo agli utenti `root` di accedere al server utilizzando SSH con l'autenticazione della password.

**CIYBA0284E** {0} è stato rilevato come un link [soft] simbolico. I link simbolici non sono consentiti.

**Spiegazione:** I link simbolici o soft a file o directory non sono supportati.

**Risposta dell'utente:** Rimuovere i link simbolici e fornire il percorso diretto o il nome file.

**CIYBA0285E** L'istanza Tivoli Directory Server {0} non è stata avviata sul server {1}.

**Spiegazione:** L'istanza Tivoli Directory Server indicata deve essere avviata.

**Risposta dell'utente:** Avviare l'istanza Tivoli Directory Server.

**CIYBA0286E** L'istanza IBM DB2 {0} non è stata avviata sul server {1}.

**Spiegazione:** L'istanza DB2 indicata non è stata avviata.

**Risposta dell'utente:** Avviare l'istanza DB2.

**CIYBA0287E** WebSphere Application Server {1} sul profilo {0} non è stato avviato sul server {2}.

**Spiegazione:** Il profilo WebSphere Application Server indicato non è stato avviato sul server indicato.

**Risposta dell'utente:** Avviare il profilo WebSphere Application Server.

**CIYBA0288E** Il server {0} non ha "localhost" associato a 127.0.0.1.

**Spiegazione:** Nel file `host` di ogni server la voce `localhost` deve essere associata a `127.0.0.1`.

**Risposta dell'utente:** Aggiornare il file `host` sul server



associando il valore localhost a 127.0.0.1.

---

**CIYBA0289E** Il server {0} non dispone di risorse CPU sufficienti. Il conteggio delle risorse CPU sul server è {1}

**Spiegazione:** Il server non dispone di risorse CPU sufficienti a soddisfare i requisiti.

**Risposta dell'utente:** Aggiungere risorse CPU al server indicato.

---

**CIYBA0301E** È stato premuto un pulsante per eseguire un test ma non sono state trovate proprietà nel file delle proprietà.

**Spiegazione:** Le proprietà per il test non sono state trovate nel file delle proprietà.

**Risposta dell'utente:** Fare clic su **Reimposta**. Questo farà sì che il programma legga il file delle proprietà corrente nel caso vengano apportate modifiche. Riprovare il test.

---

**CIYBA0302E** Ogni test deve avere determinate proprietà. class è una di queste. Parametri: {0}: nome classe {1}: nome metodo {2}: numero di sequenza

**Spiegazione:** Alla definizione del test manca la proprietà class.

**Risposta dell'utente:** Cercare il numero di sequenza nel file delle proprietà. Aggiungere una proprietà class per il test. Questo è il nome classe del test. In genere si tratta del nome classe dell'agent di esecuzione remoto (il codice che inoltra la richiesta di test a IopCatRemoteResponder per l'esecuzione.

Ad esempio:

```
0070.classname=com.ibm.top.cat.fw.remote.IopCatRemoter
```

---

**CIYBA0303E** Ogni test deve avere determinate proprietà. displaylabel è una di queste. Parametri: {0}: nome classe {1}: nome metodo {2}: numero di sequenza

**Spiegazione:** Alla definizione del test manca l'etichetta di visualizzazione.

**Risposta dell'utente:** Cercare il numero di sequenza nel file delle proprietà. Aggiungere una proprietà displaylabel per il test. Questo è il testo che verrà visualizzato sul pulsante.

---

**CIYBA0304E** È stato premuto un pulsante per eseguire un test ma non è stato trovato un test corrispondente nel file delle proprietà.

**Spiegazione:** Il file delle proprietà caricato attualmente non definisce il test richiesto.

**Risposta dell'utente:** Fare clic su **Reimposta**. Il file delle proprietà corrente verrà ricaricato.

---

**CIYBA0305E** È stato premuto un pulsante per eseguire un test, ma non è possibile trovare le informazioni di configurazione del test.

**Spiegazione:** Le informazioni di configurazione non sono disponibili per il test.

**Risposta dell'utente:** Fare clic su **Reimposta**. Il file delle proprietà corrente verrà ricaricato.

---

**CIYBA0306E** Non è stato possibile trovare il codice specificato dalla classe. Parametro:{0}: nome classe (non trovato)

**Spiegazione:** Il classname non è stato specificato correttamente nel file delle proprietà o il codice non è stato trovato.

**Risposta dell'utente:** Controllare le librerie condivise per l'applicazione IopCatRemoteResponder per vedere se una o più librerie condivise mancano o non sono specificate.

---

**CIYBA0307E** Le variabili comuni si applicano a tutti i test. Non è consentito impostare il nome, la classe o il debug utilizzando common. Parametri: {0}: nome classe {1}: nome metodo {2}: stringa chiave proprietà

**Spiegazione:** È stato utilizzato common per impostare name, class o debug.

**Risposta dell'utente:** Cercare la chiave e rimuovere la riga in errore. Ad esempio, common.name utilizzato per denominare tutti i test con lo stesso nome.

---

**CIYBA0308E** Si è verificata un'eccezione nella classe {0}, metodo {1}. Dettagli {2}

**Spiegazione:** Si è verificata un'eccezione.

**Risposta dell'utente:** Esaminare la stringa dell'eccezione per determinare perché il test non è riuscito. Potrebbe trattarsi di un normale errore di test. Ad esempio, "Connessione rifiutata" in genere significa che nessun programma era in ascolto su una determinata porta quindi il servizio non è in esecuzione.

---

**CIYBA0309E** {0},{1}() - Test[{2}] - Eccezione: {3}

**Spiegazione:** Si è verificata un'eccezione runtime nel test indicato.

**Risposta dell'utente:** Esaminare il messaggio di errore per i dettagli.

---

**CIYBA0310E** Durante l'esecuzione di questo test si è verificata un'eccezione imprevista.

**Spiegazione:** Si è verificata un'eccezione imprevista.

**Risposta dell'utente:** Esaminare le altre eccezioni per ulteriori dettagli.

---

**CIYBA0311I** La stringa restituita dal test echo di diagnostica interna. Parametro {0}: proprietà di input per il test.

**Spiegazione:** Visualizza le proprietà di input per il test.

**Risposta dell'utente:** Si tratta di un normale messaggio e non di un'indicazione di errore.

---

**CIYBA0312E** Il test Web ha ricevuto un codice risposta HTTP previsto (contenuto nei codici 200 o specificato dalla proprietà expectedRcode). Parametri: {0}: nome classe

**Spiegazione:** Indica che il test ha avuto esito positivo.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0313E** Il test Web non ha ricevuto il codice risposta HTTP previsto (contenuto nei codici 200 o specificato dalla proprietà expectedRcode). Parametri: {0}: nome classe {1}: codice risposta HTTP

**Spiegazione:** È stato ricevuto un codice di risposta HTTP imprevisto.

**Risposta dell'utente:** Controllare l'URL specificato dalla proprietà hosturl con un browser o tramite il comando `wget`.

---

**CIYBA0314E** La rappresentazione stringa della risposta del test. Parametri: {0}: codice risposta {1}: testo risposta {2}: ulteriore testo specifico del test

**Spiegazione:** Questo messaggio restituisce la risposta del test come stringa.

**Risposta dell'utente:** Non è richiesta alcuna azione.

---

**CIYBA0315E** Tutti i test devono avere proprietà. Non sono state trasmesse proprietà in questo test.

**Spiegazione:** Mancavano le proprietà dal richiamo del test.

**Risposta dell'utente:** Questo messaggio non dovrebbe verificarsi poiché le proprietà vengono trasmesse dal framework. Contattare il supporto software IBM.

---



---

**CIYBA0320E** Una stringa prevista non è stata trovata nelle proprietà del testo. Nome classe {0}, testo di output {1}

**Spiegazione:** I test SSH si collegano al server, eseguono i comandi e verificano la presenza di una stringa prevista nell'output proveniente dai comandi. Nelle proprietà di questo test non è stata specificata alcuna stringa prevista.

**Risposta dell'utente:** Verificare la chiave expected per il test. Aggiungere o modificare la proprietà specificando una stringa prevista da includere nell'output per i comandi specificati nella proprietà `commands`.

---

**CIYBA0322E** Stringa prevista non trovata nell'output. Nome classe {0}, testo di output {1}

**Spiegazione:** I test SSH si collegano al server, eseguono i comandi e verificano la presenza di una stringa prevista nell'output proveniente dai comandi. La stringa prevista non è stata trovata nell'output.

**Risposta dell'utente:** Verificare la chiave expected per il test e il testo dell'output. Potrebbe indicare che il test ha avuto esito negativo. Se il testo di output contiene "tastiera interattiva non consentita" potrebbe indicare che l'ID utente o la password utilizzati per collegarsi al server remoto non siano corretti. Verificare le proprietà `user`, `password` e `hostname` per il test. La password è un alias di una password nel keystore.

---

**CIYBA0323E** Eccezione non prevista nel nome classe {0}. Eccezione: {1}

**Spiegazione:** Si è verificata un'eccezione imprevista.

**Risposta dell'utente:** Se il testo di output contiene "tastiera interattiva non consentita" potrebbe indicare che l'ID utente o la password utilizzati per collegarsi al server remoto non siano corretti. Verificare le proprietà `user`, `password` e `hostname` per il test. La password è un alias di una password nel keystore.

---

**CIYBA0340E** L'agent di esecuzione del test (IopCatRemoteResponder) non è riuscito ad analizzare i dati di input JSON. Parametri: {0}: nome classe {1}: nome metodo {2}: dati post

**Spiegazione:** L'interfaccia utente e l'agent di esecuzione del test comunicano mediante JSON. Questo errore indica che l'agent di esecuzione del test (IopCatRemoteResponder) non è riuscito ad analizzare i dati di input JSON.

**Risposta dell'utente:** Esaminare i dati post per vedere se sono nel formato JSON corretto.

---

**CIYBA0341E** Si è verificata un'eccezione durante l'esecuzione del test. Parametri: {0}: nome classe {1}: nome metodo {2}: stringa eccezione

**Spiegazione:** Si è verificata un'eccezione durante l'esecuzione del test.

**Risposta dell'utente:** Controllare la stringa dell'eccezione per determinare perché il test non è riuscito. Potrebbe trattarsi di un normale errore di test. Ad esempio, "Connessione rifiutata" in genere significa che nessun programma era in ascolto sulla porta quindi il servizio non è in esecuzione.

**CIYBA0342E** L'agent di esecuzione del test (IopCatRemoteResponder) non è riuscito a inviare una risposta all'interfaccia utente. Parametri: {0}: nome classe {1}: nome metodo {2}: stringa eccezione

**Spiegazione:** L'interfaccia utente e l'agent di esecuzione del test comunicano mediante JSON. Questo errore indica che l'agent di esecuzione del test (IopCatRemoteResponder) non è riuscito ad inviare una risposta all'interfaccia utente.

**Risposta dell'utente:** Esaminare la stringa dell'eccezione per determinare perché non è stato possibile inviare la risposta. Questo potrebbe verificarsi se il test impiega troppo tempo e l'interfaccia utente non è più in attesa.

**CIYBA0343E** Manca un prefisso chiave previsto. Parametri: {0}: nome classe {1}: nome metodo {2}: stringa chiave proprietà

**Spiegazione:** Tutte le proprietà di un determinato test hanno come prefisso lo stesso numero. Ciò consente il raggruppamento, poiché i file delle proprietà non sono posizionali.

**Risposta dell'utente:** Cercare la chiave nel file delle proprietà ed aggiungere il prefisso delle proprietà. Ad esempio, quanto segue non è corretto:

```
classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl   = https://$!APP_HOSTNAME:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel = Internal Diagnostic (Echo REST remotd)
0050.comment    = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfo page = cct_echo_rest_remoted_test.html
```

Dovrebbe essere:

```
0050.classname  = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl   = https://$!APP_HOSTNAME:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel = Internal Diagnostic (Echo REST remotd)
0050.comment    = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfo page = cct_echo_rest_remoted_test.html
```

**CIYBA0345E** Chiave non valida - Il prefisso della chiave non è numerico. Parametri: {0}: nome classe {1}: nome metodo {2}: numero di sequenza CCT\_RESULTS\_INFO = {0}.{1}() - Classe: {2} Risultati - Codice risposta[{3}] Testo risposta[{4}]

**Spiegazione:** Ogni test deve avere un prefisso

numerico che raggruppa tutte le proprietà di un determinato test. Il prefisso fornito non è numerico.

**Risposta dell'utente:** Cercare il numero di sequenza nel file delle proprietà. Modificare il prefisso in modo che sia numerico e utilizzare lo stesso prefisso per il resto delle proprietà del test.

**CIYBA0347E** Si è verificata un'eccezione. Parametri: {0}: nome classe {1}: nome metodo {2}: stringa eccezione

**Spiegazione:** Si è verificata un'eccezione.

**Risposta dell'utente:** Esaminare la stringa dell'eccezione per determinare perché il test non è riuscito. Potrebbe trattarsi di un normale errore di test. Ad esempio, "Connessione rifiutata" in genere significa che nessun programma era in ascolto sulla porta quindi il servizio non è in esecuzione.

**CIYBA0348E** È stato premuto un pulsante per eseguire un test ma non sono state trovate proprietà nel file delle proprietà.

**Spiegazione:** Non sono state trovate proprietà per il test. Il file delle proprietà potrebbe essere stato modificato.

**Risposta dell'utente:** Fare clic su **Reimposta**. Il file delle proprietà corrente verrà ricaricato.

**CIYBA0349E** Non è stato possibile trovare il codice specificato dalla classe. Parametro:{0}: nome classe (non trovato)

**Spiegazione:** Il classname non è specificato correttamente nel file delle proprietà o il codice non è stato trovato.

**Risposta dell'utente:** Controllare nelle librerie condivise IopCatRemoteResponder per vedere se mancano una o più librerie condivise.

**CIYBA0401E** Il nome file template delle proprietà IOPMGMT non è stato specificato o non era corretto.

**Spiegazione:** Manca il parametro del file template delle proprietà IOPMGMT.

**Risposta dell'utente:** Immettere il nome corretto per il file delle proprietà IOPMGMT.

**CIYBA0402E** Il nome file delle proprietà della topologia non è stato specificato o non era corretto.

**Spiegazione:** Manca il parametro del file delle proprietà della topologia o non è corretto.

**Risposta dell'utente:** Immettere il nome corretto per il file delle proprietà della topologia.

---

**CIYBA0403E** Il nome file template delle proprietà IOPMGMT non è stato specificato o non era corretto.

**Spiegazione:** Manca il parametro che specifica il file template delle proprietà IOPMGMT.

**Risposta dell'utente:** Immettere il nome file corretto per il file delle proprietà della topologia.

---

**CIYBA0404E** Impossibile trovare il file delle proprietà della topologia.

**Spiegazione:** Impossibile trovare il file delle proprietà della topologia.

**Risposta dell'utente:** Verificare che il file delle proprietà della topologia si trovi nella directory *install\_home/topology* sul server di installazione.

---

**CIYBA0405E** Password mancante nel file della topologia per la proprietà:

**Spiegazione:** Non è stata trovata una password nel file delle proprietà della tipologia indicato.

**Risposta dell'utente:** È richiesta una password per il file della topologia. Immettere una password per la topologia.

---

**CIYBA0501E** Manca il parametro richiesto per il supporto Cyber Hygiene BA (Base Architecture).

**Spiegazione:** Manca il parametro richiesto per il supporto Cyber Hygiene di IBM Intelligent Operations Center.

**Risposta dell'utente:** Verificare che lo script Cyber Hygiene abbia il percorso corretto dell'ubicazione del supporto di installazione.

---

**CIYBA0502E** Manca il parametro richiesto per il file delle proprietà della topologia.

**Spiegazione:** Manca il parametro del nome file per il file delle proprietà della topologia.

**Risposta dell'utente:** Fornire il nome file corretto per il file delle proprietà della topologia.

---

**CIYBA0503E** Manca il parametro richiesto per la directory di destinazione Cyber Hygiene BA (Base Architecture).

**Spiegazione:** Manca il parametro richiesto per la directory di destinazione Cyber Hygiene.

**Risposta dell'utente:** Fornire la directory di destinazione corretta.

---



---

**CIYCC0002E** Correggere i seguenti errori di configurazione: {0}

**Spiegazione:** Si è verificato un errore nella pagina di configurazione Modifica sessioni condivise. L'errore è indicato da {0}.

**Risposta dell'utente:** Correggere l'errore e riprovare la richiesta.

---

**CIYCC0005E** L'evento non può essere inoltrato. Provare nuovamente ad inoltrare l'evento. Se il problema persiste contattare un amministratore o l'help desk.

**Spiegazione:** Si è verificato un errore di servlet publisher quando un utente ha provato ad aggiornare, elevare o annullare un evento.

**Risposta dell'utente:** Far risolvere l'errore di servlet publisher all'amministratore o all'help desk.

---

**CIYCC0006W** Il record è stato aggiornato da un altro utente. Aggiornare la pagina per recuperare il record aggiornato.

**Spiegazione:** Un aggiornamento richiesto dall'utente è in conflitto con un'altra modifica verificatasi sul server. Questo può accadere se due utenti provano a modificare lo stato di un'attività contemporaneamente.

**Risposta dell'utente:** Aggiornare la pagina. Verrà visualizzato l'aggiornamento effettuato dall'altro utente. Quindi apportare le eventuali modifiche richieste.

---

**CIYUI0001E** L'array JSON fornito contiene errori e non può essere analizzato.

**Spiegazione:** L'utente ha immesso una stringa JSON in una finestra in cui deve essere immesso lo script, ma la stringa contiene errori di sintassi e non può essere analizzata.

**Risposta dell'utente:** Correggere la stringa JSON.

---

**CIYUI0002E** Evento non trovato. Non è possibile visualizzare le proprietà dell'evento.

**Spiegazione:** La richiesta di visualizzare le proprietà dell'evento non è riuscita perché non sono state trovate le proprietà nel database.

**Risposta dell'utente:** Aggiornare la pagina e riprovare la richiesta.

---

**CIYUI0004E** Errore nell'inoltro dei dati del gestore mappa ubicazioni.

**Spiegazione:** Si è verificato un problema durante l'impostazione dei dati del gestore mappa ubicazioni.

---

**Risposta dell'utente:** Per ulteriori dettagli consultare i messaggi aggiuntivi.

Messaggi aggiuntivi della scheda Classificazione.

**Errore di inoltro dei dati**

La nuova classificazione non è stata immessa nel database.

Messaggi aggiuntivi della scheda Mappe ubicazioni.

**Errore di inoltro dei dati**

La nuova mappa ubicazioni non è stata immessa nel database.

Messaggi aggiuntivi della scheda Aree.

**L'identificativo dell'area immesso non è valido.**

**L'identificativo dell'area è già presente nella mappa.**

L'utente sta immettendo un'area nella mappa che esiste già sulla mappa.

**L'identificativo dell'area immesso non è valido.**

L'identificativo dell'area non è valido. È vuoto o l'ID area è uguale all'ID area principale.

**I dati dell'area immessi non sono validi.**

I dati dell'area non sono validi. Il cliente deve verificare di aver immesso tutti i campi obbligatori di ogni area.

**L'identificativo area principale non deve esistere come area sulla mappa corrente.**

L'ID area principale immesso esiste come area sulla mappa. Un'area non può avere un'area principale che è un'area sulla mappa. Deve essere su un'altra mappa.

**Sono presenti riferimenti circolari tra le aree e le rispettive aree principali. Rimuovere i riferimenti circolari.**

Rimuovere le relazioni circolari dell'area principale dal database the IBM Intelligent Operations Center.

**Errore nell'inoltro dei dati.**

La scheda delle nuove aree non è stata immessa nel database.

**CIYUI0003I Dati inoltrati correttamente.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo. Il messaggio indica che il database IBM Intelligent Operations Center, il portlet Gestore mappa ubicazioni ed il portlet Mappa ubicazioni sono stati aggiornati.

**Risposta dell'utente:** Non è richiesta alcuna azione.

**CIYUI0004I Inoltro correttamente.**

**Spiegazione:** Questo messaggio viene fornito solo a scopo informativo. Il messaggio indica che solo l'interfaccia utente del portlet Gestore mappa ubicazioni è aggiornata, le modifiche non sono memorizzate nel database IBM Intelligent Operations Center. Se si esce dal portlet Gestore mappa ubicazioni senza inoltrare le modifiche, l'aggiornamento viene annullato.

**Risposta dell'utente:** Fare clic su **Inoltra** per aggiornare il database IBM Intelligent Operations Center ed il portlet Mappa ubicazioni.

## Utilizzo di Knowledge base e del supporto IBM

Questa sezione contiene gli argomenti relativi all'utilizzo di Knowledge base, Fix Central e del supporto IBM per la ricerca delle informazioni relative alla risoluzione dei problemi.

### Ricerca nei knowledge base

Spesso è possibile trovare le soluzioni ai problemi effettuando ricerche nei knowledge base IBM. È possibile ottimizzare i risultati utilizzando le risorse disponibili, gli strumenti di supporto e i metodi di ricerca.

### Informazioni su questa attività

È possibile reperire informazioni utili cercando nel centro informazioni IBM Intelligent Operations Center, ma a volte è necessario guardare oltre il centro informazioni per rispondere alle domande o risolvere problemi.

### Procedura

Per cercare nei knowledge base le informazioni necessarie, utilizzare uno o più approcci tra i seguenti:

- Cercare contenuto utilizzando IBM Support Assistant Lite (ISA Lite).

ISA Lite è uno strumento software gratuito utile per rispondere alle domande e risolvere i problemi con i prodotti software IBM. Per istruzioni sul download e l'installazione di ISA Lite, vedere i link alla fine dell'argomento.



- Trovare il contenuto necessario utilizzando il portale del supporto IBM.  
Il portale del supporto IBM è una vista centralizzata unificata di tutti gli strumenti del supporto tecnico e delle informazioni per tutti i sistemi, il software ed i servizi IBM. Il portale del supporto IBM consente l'accesso al portfolio del supporto elettronico IBM da un unico posto. È possibile personalizzare le pagine concentrando l'attenzione sulle informazioni e sulle risorse necessarie per la prevenzione dei problemi e per una risoluzione dei problemi più rapida. Familiarizzare con il portale del supporto IBM visualizzando i video dimostrativi ([https://www.ibm.com/blogs/SPNA/entry/the\\_ibm\\_support\\_portal\\_videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos)) relativi a questo strumento. Questi video introducono l'utente al portale del supporto IBM, esplorano la risoluzione dei problemi ed altre risorse, e illustrano in che modo è possibile personalizzare la pagina spostando, aggiungendo ed eliminando portlet.
- Cercare contenuto relativo a IBM Intelligent Operations Center utilizzando una delle seguenti risorse tecniche aggiuntive:
  - Technote e APAR (report di problemi) di IBM Intelligent Operations Center
  - IBM Intelligent Operations Center Pagina portale di supporto
  - IBM Intelligent Operations Center Pagina Forum e community
  - IBM Smarter Cities Software Solutions Redbooks
- Cercare contenuto utilizzando la ricerca per titoli (masthead) IBM. È possibile utilizzare la ricerca per titoli (masthead) IBM immettendo la stringa di ricerca nel campo Cerca nella parte superiore di qualsiasi pagina ibm.com.
- Cercare contenuto utilizzando qualsiasi motore di ricerca esterno, ad esempio Google, Yahoo o Bing. Se si utilizza un motore di ricerca esterno, è probabile che i risultati includano informazioni esterne al dominio ibm.com. Tuttavia, a volte è possibile trovare informazioni utili per la risoluzione di un problema relativo a prodotti IBM in newsgroup, forum e blog che non sono in ibm.com.

**Suggerimento:** Includere nella ricerca "IBM" e il nome del prodotto se si stanno cercando informazioni su un prodotto IBM.

#### Concetti correlati:

"Informazioni" a pagina 195

Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.

"Installazione ed utilizzo di IBM Support Assistant Lite" a pagina 303

IBM Support Assistant Lite (ISA Lite) è uno strumento che raccoglie dati di diagnostica comuni utili per analizzare problemi generali.

#### Informazioni correlate:



Download di IBM Support Assistant Lite per IBM Intelligent Operations Center 1.5

## Ottenimento di fix da Fix Central

È possibile utilizzare Fix Central per individuare le fix consigliate dal supporto IBM per vari prodotti, incluso IBM Intelligent Operations Center. Con Fix Central, è possibile cercare, selezionare, ordinare e scaricare fix per il proprio sistema con una scelta di opzioni di distribuzione. Una fix del prodotto IBM Intelligent Operations Center potrebbe essere disponibile per risolvere un problema.

### Procedura

Per individuare e installare fix:

1. Ottenere gli strumenti richiesti per acquisire la fix. Se non è installato, ottenere il programma di installazione dell'aggiornamento del proprio prodotto. È possibile eseguire il download del programma di installazione da Fix Central. Questo sito fornisce istruzioni per il download, l'installazione e la configurazione del programma di installazione dell'aggiornamento.

2. Selezionare IBM Intelligent Operations Center come prodotto e selezionare una o più caselle di spunta pertinenti al problema che si desidera risolvere.
3. Identificare e selezionare la fix richiesta.
4. Scaricare la fix.
  - a. Aprire il documento di download e seguire il link nella sezione "Scarica pacchetto".
  - b. Quando si scarica il file, assicurarsi che il nome del file di manutenzione non sia cambiato. Questa modifica potrebbe essere intenzionale o potrebbe essere una modifica involontaria causata da determinati browser web o programma di utilità di download.
5. Per applicare la fix, seguire le istruzioni nella sezione "Istruzioni per l'installazione" del documento di download.
6. Opzionale: Effettuare la sottoscrizione per ricevere settimanalmente notifiche via email sulle fix ed altri aggiornamenti del supporto IBM.

#### Attività correlate:

"Sottoscrizione agli aggiornamenti del supporto" a pagina 325

Per rimanere informati su importanti informazioni relative ai prodotti IBM utilizzati, è possibile effettuare la sottoscrizione agli aggiornamenti.

#### Informazioni correlate:

 [Fix Central help](#)

## Contattare il supporto IBM

Il supporto IBM fornisce assistenza per i difetti dei prodotti, rispondendo alle FAQ ed eseguendo una nuova individuazione.

### Prima di iniziare

Dopo aver provato a individuare la risposta o la soluzione utilizzando altre opzioni di self-help come le note tecniche, è possibile contattare il supporto IBM. Prima di contattare il supporto IBM, la propria società deve avere una sottoscrizione attiva al software IBM e un contratto di supporto, ed è necessario essere autorizzati ad inoltrare problemi a IBM. Per informazioni sui tipi di supporto disponibili, consultare l'argomento Support portfolio in *Software Support Handbook*.

### Procedura

Completare la seguente procedura per contattare il supporto IBM con un problema:

1. Definire il problema, raccogliere le informazioni di background e determinare la gravità del problema. Per ulteriori informazioni, consultare l'argomento Getting IBM support in *Software Support Handbook*.
2. Raccogliere le informazioni diagnostiche. Per informazioni sull'utilizzo di IBM Support Assistant Lite per raccogliere i file di log di IBM Intelligent Operations Center, vedere i link alla fine dell'argomento.
3. Inoltrare il problema al supporto IBM in uno dei seguenti modi:
  - Utilizzando IBM Support Assistant Lite (ISA Lite). Vedere i link alla fine dell'argomento.
  - Online tramite la IBM Intelligent Operations Center Pagina portale di supporto: è possibile aprire, aggiornare e visualizzare tutte le richieste di servizio dal portlet Richiesta di servizio nella pagina Richiesta di servizio.
  - Per telefono: per il numero di telefono da chiamare nella propria regione, consultare la pagina Web Directory of worldwide contacts.

### Risultati

Se il problema inoltrato è un difetto software o per documentazione carente o inaccurata, il supporto IBM crea un APAR (Authorized Program Analysis Report). L'APAR descrive il problema in dettaglio. Quando possibile, il supporto IBM fornisce una soluzione temporanea che l'utente può implementare fino a



quando non viene risolto l'APAR e viene distribuita una fix. IBM pubblica giornalmente gli APAR risolti sul sito Web del supporto IBM, in modo che altri utenti che riscontrano lo stesso problema possano beneficiare della stessa soluzione.

## Operazioni successive

Prepararsi a collaborare con il rappresentante del supporto tecnico IBM utilizzando IBM Assist On-Site, che è un plug-in di assistenza remota che può essere scaricato sul computer. Il rappresentante del supporto tecnico IBM può utilizzare IBM Assist On-Site per visualizzare il desktop dell'utente e condividere il controllo del mouse e della tastiera. Questo strumento riduce il tempo impiegato per identificare il problema, raccoglie i dati necessari e risolve il problema. Per ulteriori informazioni, vedere IBM Assist On-Site.

### Concetti correlati:

“Informazioni” a pagina 195

Utilizzare il portlet Informazioni per visualizzare i dettagli della versione di IBM Intelligent Operations Center e di IBM Smarter Cities Software Solutions integrato, che sono stati installati. È possibile inoltre visualizzare i dettagli di tutti gli aggiornamenti applicati da quando è stata eseguita l'installazione.

“Installazione ed utilizzo di IBM Support Assistant Lite” a pagina 303

IBM Support Assistant Lite (ISA Lite) è uno strumento che raccoglie dati di diagnostica comuni utili per analizzare problemi generali.

### Informazioni correlate:



Download di IBM Support Assistant Lite per IBM Intelligent Operations Center 1.5

## Sottoscrizione agli aggiornamenti del supporto

Per rimanere informati su importanti informazioni relative ai prodotti IBM utilizzati, è possibile effettuare la sottoscrizione agli aggiornamenti.

### Informazioni su questa attività

Con la sottoscrizione per ricevere gli aggiornamenti, è possibile ricevere importanti informazioni tecniche ed aggiornamenti per strumenti e risorse specifici del supporto IBM. È possibile effettuare la sottoscrizione agli aggiornamenti utilizzando uno dei seguenti due approcci:

#### Feed RSS

Il seguente feed RSS è disponibile per IBM Intelligent Operations Center: *IBM Intelligent Operations Center*.

Per informazioni generali su RSS, inclusi i passi di introduzione e un elenco di pagine Web IBM abilitate a RSS, visitare il sito IBM Software Support RSS feeds.

#### My Notifications

Con My Notifications, è possibile effettuare la sottoscrizione agli aggiornamenti del supporto per qualsiasi prodotto IBM. (My Notifications sostituisce My Support, uno strumento simile che potrebbe essere stato utilizzato in passato). Con My Notifications è possibile specificare che si desidera ricevere annunci giornalieri o settimanali via email. È possibile semplificare quale tipo di informazioni si desidera ricevere (ad esempio pubblicazioni, suggerimenti, flash di prodotti (noti anche come avvisi), download e driver). My Notifications consente all'utente di personalizzare e classificare i prodotti sui quali si desidera essere informati e i metodi di distribuzione più adatti alle proprie esigenze.

## Procedura

Per effettuare la sottoscrizione agli aggiornamenti del supporto:

1. Per effettuare la sottoscrizione al feed RSS di *IBM Intelligent Operations Center*, utilizzare i seguenti passi secondari:

- a. Aprire il link IBM Intelligent Operations Center RSS feed.
- b. Nella finestra Subscribe with Live Bookmark, selezionare una cartella in cui salvare il segnalibro del feed RSS e fare clic su **Subscribe**.

Per ulteriori informazioni sulla sottoscrizione ai feed RSS, vedere il link IBM Software Support RSS feeds nella sezione Informazioni correlate alla fine dell'argomento.

2. Per effettuare la sottoscrizione a My Notifications, andare al portale del supporto IBM e fare clic su **My Notifications** nel portlet **Notifiche**.
3. Accedere utilizzando il proprio ID e la propria password IBM e fare clic su **Inoltra**.
4. Identificare quali aggiornamenti si desidera ricevere e quando.
  - a. Fare clic sulla scheda **Sottoscrivi**.
  - b. Selezionare IBM Intelligent Operations Center e fare clic su **Continua**.
  - c. Selezionare le proprie preferenze relative a come ricevere gli aggiornamenti, se tramite email, online in una cartella designata o come feed RSS o Atom.
  - d. Selezionare i tipi di aggiornamento della documentazione che si desidera ricevere, ad esempio, nuove informazioni sui download del prodotto e commenti dei gruppi di discussione.
  - e. Fare clic su **Inoltra**.

## Risultati





Fino a quando non si modificano le preferenze dei feed RSS e di My Notifications, si riceveranno le notifiche degli aggiornamenti richiesti. È possibile modificare le preferenze quando necessario (ad esempio, se si smette di utilizzare un prodotto e si inizia ad utilizzarne un altro).

### Attività correlate:

“Ottenimento di fix da Fix Central” a pagina 323

È possibile utilizzare Fix Central per individuare le fix consigliate dal supporto IBM per vari prodotti, incluso IBM Intelligent Operations Center. Con Fix Central, è possibile cercare, selezionare, ordinare e scaricare fix per il proprio sistema con una scelta di opzioni di distribuzione. Una fix del prodotto IBM Intelligent Operations Center potrebbe essere disponibile per risolvere un problema.

### Informazioni correlate

-  [IBM Software Support RSS feeds](#)
-  [Subscribe to My Notifications support content updates](#)
-  [My notifications for IBM technical support](#)
-  [My notifications for IBM technical support overview](#)

## Scambio di informazioni con IBM

Per diagnosticare o identificare un problema, potrebbe essere necessario fornire al supporto IBM i dati e le informazioni dal proprio sistema. In altri casi il supporto IBM potrebbe fornire all'utente gli strumenti o le utilità da utilizzare per la determinazione dei problemi.

### Concetti correlati:

“Abilitazione delle tracce e visualizzazione dei file di log” a pagina 295

Per risolvere un problema in IBM Intelligent Operations Center, potrebbe essere necessario analizzare i file di log in diversi sistemi. I seguenti argomenti forniscono una guida su come accedere ai file di log.

“Installazione ed utilizzo di IBM Support Assistant Lite” a pagina 303

IBM Support Assistant Lite (ISA Lite) è uno strumento che raccoglie dati di diagnostica comuni utili per analizzare problemi generali.

### Attività correlate:

“Esecuzione dello strumento "must gather" dell'installazione” a pagina 299

Durante l'installazione di IBM Intelligent Operations Center vengono generati dei file di log. Uno strumento è disponibile per raccogliere questi file di log per l'analisi.

### Informazioni correlate:



Download di IBM Support Assistant Lite per IBM Intelligent Operations Center 1.5

## Invio di informazioni al supporto IBM

Per ridurre il tempo necessario a risolvere un problema, è possibile inviare informazioni diagnostiche e la traccia al supporto IBM.

### Procedura

Per inoltrare le informazioni diagnostiche al supporto IBM:

1. Aprire un PMR (problem management record) utilizzando lo strumento di richiesta di servizio.
2. Raccogliere i dati diagnostici necessari. I dati diagnostici sono utili per ridurre il tempo necessario a risolvere il PMR. È possibile raccogliere i dati diagnostici automaticamente o manualmente:
  - Raccogliere i dati automaticamente utilizzando IBM Support Assistant Lite (ISA Lite). Vedere i link vicino all'inizio dell'argomento.
  - Raccogliere i dati manualmente. Per informazioni sui file di log di IBM Intelligent Operations Center vedere i link vicino all'inizio dell'argomento.
3. Comprimere i file utilizzando il formato ZIP o TAR.
4. Trasferire i file a IBM. È possibile utilizzare uno dei seguenti metodi per trasferire i file a IBM:
  - Strumento di richiesta di servizio
  - Metodi di caricamento dei dati standard: FTP, HTTP
  - Metodi di caricamento dei dati sicuri: FTPS, SFTP, HTTPS
  - Email

Tutti questi metodi di scambio di dati sono spiegati sul sito del supporto IBM.

## Ricezione di informazioni dal supporto IBM

Occasionalmente un rappresentante del supporto tecnico IBM potrebbe chiedere di scaricare strumenti diagnostici o altri file. È possibile utilizzare FTP per eseguire il download di tali file.

### Prima di iniziare

Accertarsi che il rappresentante del supporto tecnico IBM abbia fornito all'utente il server preferito da utilizzare per il download dei file e i nomi esatti dei file e della directory a cui accedere.

### Procedura

Per scaricare i file dal supporto IBM:

1. Utilizzare FTP per connettersi al sito fornito dal rappresentante del supporto tecnico IBM e collegarsi come anonimo. Utilizzare il proprio indirizzo email come password.
2. Andare alla directory appropriata:

- a. Andare alla directory `/fromibm`.  
`cd fromibm`
  - b. Andare alla directory fornita dal rappresentante del supporto tecnico IBM.  
`cd nomedirectory`
  3. Abilitare la modalità binaria per la sessione.  
`binary`
  4. Utilizzare il comando **get** per scaricare il file specificato dal rappresentante del supporto tecnico IBM.  
`get nomefile.estensione`
  5. Terminare la sessione FTP.  
`quit`
- 

## Problemi noti e soluzioni

Questa sezione contiene un elenco di problemi che si verificano comunemente e una soluzione per ciascun elemento.

### L'elaborazione di KPI (Key Performance Indicator) si interrompe dopo un periodo

In IBM Intelligent Operations Center, l'elaborazione di KPI (key performance indicator) a volte si arresta dopo un periodo, ad esempio, di notte. Per informazioni sulla risoluzione del problema, vedere il link alla fine dell'argomento per la technote di risoluzione dei problemi *Key performance indicator processing stops after a period of time*.

### I portlet non vengono popolati con i dati quando cambiano le impostazioni di sicurezza

Se i portlet non vengono popolati con dati KPI, di attività o di risorse come previsto, controllare le impostazioni della porta. Se si utilizza la tabella proprietà di sistema per modificare le impostazioni HTTPS e non si modificano di conseguenza le impostazioni della porta, si verificherà un problema con il popolamento dei portlet con i dati.

### Errore di connessione del report Cognos

Se si riceve un errore di connessione del report Cognos, aggiornare la pagina.

### I report Cognos non vengono visualizzati correttamente

Se i report Cognos non vengono visualizzati correttamente all'apertura della pagina Supervisore: Report o Operatore: Report, aggiornare la pagina.

Se, una volta aggiornata la pagina, i report Cognos continuano a non essere visualizzati correttamente, i cluster del server delle applicazioni Cognos potrebbero essere arrestati. Accedere alla console di gestione WebSphere Application Server e verificare lo stato dei cluster WebSphere Application Server. Se lo stato di un cluster visualizza una X rossa, selezionare tale cluster e premere **Avvia**.

### Dati non trovati per i report Cognos

Se i report Cognos non vengono visualizzati correttamente e viene visualizzato un messaggio Nessun dato trovato, i dati per i propri criteri di selezione potrebbero non esistere nel database. Definire nuovamente i criteri di selezione. Ad esempio, cancellare i dati dai campi **Dalla data** ed **Alla data** nel report personalizzato e fare clic su **Aggiorna**. Quindi, copiare l'URL del report ed incollarlo nel portlet Cognos.

## **Il report non viene visualizzato quando si copia l'URL del report utilizzando il pulsante URL report**

Come utente di esempio, se si copia l'URL del report utilizzando il pulsante **URL report** e si va direttamente alla pagina del portlet Report, il report non viene visualizzato. Per correggere questo problema, premere **F5** per effettuare l'aggiornamento, e il report viene visualizzato correttamente.

## **La risorsa modificata non viene visualizzata nel portlet Dettagli**

Se si modifica una risorsa in Tivoli Service Request Manager quando Tivoli Netcool/Impact non è disponibile, la risorsa potrebbe non essere visualizzata nel portlet Dettagli. Ad esempio, se si fa clic con il tasto destro del mouse su un evento nella scheda **Eventi e incidenti** e poi si fa clic su **Visualizza risorse vicine**, la risorsa modificata potrebbe non essere visualizzata. Per risolvere questo problema, modificare di nuovo la risorsa in Tivoli Service Request Manager.

## **Lo stato degli utenti scollegati non viene visualizzato correttamente nel portlet Contatti**

Lo stato degli utenti collegati viene visualizzato nel portlet Contatti. Se un utente collegato chiude la finestra del browser o si scollega da WebSphere Portal, il suo stato continua ad essere visualizzato come collegato finché non scade la sessione. Tuttavia, i messaggi inviati a tale utente, dopo che questo ha chiuso la finestra del browser o si è scollegato, non vengono recapitati. Di conseguenza, viene proposto un messaggio di errore all'utente che sta tentando di inviare il messaggio. Per assicurarsi che lo stato venga aggiornato immediatamente nel portlet Contatti, scollegarsi facendo clic su **File > Disconnetti**.

## **Selezione di Aggiorna più di una volta nella pagina Supervisore: Report**

Nella pagina Supervisore: Report nell'interfaccia utente di IBM Intelligent Operations Center, quando si seleziona **Aggiorna** senza apportare modifiche, i campi **Dalla data** e **Alla data** vengono popolati con la data odierna. Se si seleziona di nuovo **Aggiorna** senza apportare modifiche, viene visualizzato il messaggio Nessun dato trovato.

Questo comportamento si verifica perché i campi **Dalla data** e **Alla data** vengono popolati automaticamente.

## **I titoli lunghi rendono inutilizzabili i grafici dei report**

I titoli di evento che superano dai 20 ai 30 caratteri possono influire sulla visualizzazione del report grafico a torta **Tutti gli eventi, per titolo**, rendendo il grafico inutilizzabile. Poiché i titoli degli eventi etichettano le sezioni del grafico a torta e il grafico a torta si rimpicciolisce per contenere le etichette, l'immagine del grafico a torta diviene troppo piccola per poter distinguere le varie sezioni.

## **Risultati imprevisti nella conversione del fuso orario del browser**


Risultati imprevisti nella conversione del fuso orario del browser potrebbero essere causati da una codifica errata del fuso orario nell'evento CAP (Common Alerting Protocol). Per maggiori dettagli, vedere il link alla fine dell'argomento.

### Concetti correlati:

“Utilizzo CAP per eventi KPI” a pagina 96

Il WebSphere Message Broker, che è fornito come parte di IBM Intelligent Operations Center, accetta messaggi di evento CAP ed utilizza i dati nei calcoli KPI (Key performance indicator).

### Informazioni correlate:

 Technote di risoluzione dei problemi Key performance indicator processing stops after a period of time

## Gli errori di connessione quando si installa IBM Intelligent Operations Center

Come procedere quando si riceve un messaggio SOAPException durante l'installazione di IBM Intelligent Operations Center.

Quando si riceve un messaggio simile al seguente significa che la connessione al server non è attiva:

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

In tal caso è necessario arrestare e riavviare i server. Quindi riavviare il programma di installazione o immettere nuovamente il comando di installazione.

## La rete IPv6 non viene avviata

Se su un server non viene avviata la rete IPv6, è possibile che sia necessario apportare delle modifiche al file `/etc/modprobe.conf`.

### Informazioni su questa attività

Il problema si verifica quando si aggiorna VMWare alla release 5.

### Procedura

1. Modificare il file `/etc/modprobe.conf`.

2. Cambiare la seguente riga:

```
alias ipv6 off
```

in

```
# alias ipv6 off
```

3. Cambiare la seguente riga:

```
options ipv6 disable=1
```

in

```
# options ipv6 disable=1
```

4. Salvare il file.

5. Riavviare il server.

## Tivoli Service Request Manager non parte

Come procedere se Tivoli Service Request Manager non può essere avviato da Strumento di controllo della piattaforma mentre viene visualizzato come funzionante dallo strumento Controllo di verifica del sistema.

### Informazioni su questa attività

Per riavviare Tivoli Service Request Manager, procedere come segue.

## Procedura

1. Arrestare tutti i servizi utilizzando lo Strumento di controllo della piattaforma.
2. Arrestare e riavviare il server eventi.
3. Avviare tutti i servizi utilizzando lo Strumento di controllo della piattaforma.

## Impossibile creare una nuova pagina per l'interfaccia utente

Risolvere un problema che si verifica durante la creazione di una nuova pagina se si utilizza Microsoft Internet Explorer 9.

### Informazioni su questa attività

Questo problema può verificarsi durante il tentativo di creazione di una nuova pagina dalla pagina **Amministrazione** oppure da una delle pagine utente **Intera città**. La nuova pagina non viene caricata. Per eliminare il problema, attivare temporaneamente la **Visualizzazione Compatibilità** del browser. Assicurarsi di disattivare la **Visualizzazione Compatibilità** una volta creata la nuova pagina, perché IBM Intelligent Operations Center non supporta la Visualizzazione Compatibilità di Internet Explorer 8 o Internet Explorer 9.

## Procedura

1. Aprire Internet Explorer 9.
2. Accedere a IBM Intelligent Operations Center come amministratore.
3. Fare clic su **Amministrazione > Interfaccia utente del portale > Gestisci pagine**.
4. Nella barra degli strumenti superiore del browser, fare clic su **Strumenti**.
5. Dal menu, selezionare **Visualizzazione Compatibilità**.
6. Immettere **Intera città** nella casella di ricerca.
7. Una volta restituita la ricerca, fare clic su **Intera città**.
8. Fare clic su **Nuova pagina**.
9. Una volta caricata la nuova pagina, tornare alla barra degli strumenti del browser ed annullare la selezione di **Visualizzazione Compatibilità**.

### Concetti correlati:

“Browser supportati” a pagina 13

L'interfaccia delle soluzioni IBM Intelligent Operations Center supporta un certo numero di browser. Alcuni browser possono essere utilizzati con alcune limitazioni.

## Soluzioni temporanee per l'accesso facilitato per i portlet

Per i problemi di accesso facilitato relativi ad alcuni dei portlet IBM Intelligent Operations Center, sono disponibili soluzioni temporanee:

- Nel portlet **Dettagli** e nel portlet **Notifiche**, per accedere al menu a comparsa, utilizzare i seguenti controlli della tastiera:

### Windows

Premere il tasto del menu dedicato.

**Mac** Scegliere l'opzione appropriata a seconda che si disponga o meno di un tastierino numerico:

- Se si dispone di un tastierino numerico, assicurarsi che i tasti del mouse siano abilitati, e premere **Ctrl+5**.
  - Se non si dispone di un tastierino numerico, abilitare i tasti del mouse e premere **Ctrl+I**.
- Per aprire la finestra **Aggiungi evento**, nel portlet **Dettagli** fare clic sulla scheda **Eventi e incidenti** o premere il tasto di tabulazione; il lettore schermo legge i nomi delle schede. Quindi scegliere dall'elenco i controlli di tastiera appropriati.



**Mozilla Firefox**  
Ctrl+Alt+V

**Safari** fn+controllo+opzione+V

**Internet Explorer**  
Ctrl+Alt+V

- Nel portlet Dettagli, nella finestra Aggiungi evento, il lettore schermo non legge i seguenti valori:
  - Data di validità
  - Ora di validità
  - Data di inizio
  - Ora di inizio
  - Data di scadenza
  - Ora di scadenza

## Soluzione temporanea di accessibilità per la selezione di date nel portlet Report

Nel portlet Report, non è possibile selezionare le date dal calendario utilizzando la tastiera.

### Informazioni su questa attività

Nel portlet Report, per configurare un report predefinito è necessario immettere una data o un intervallo di date. Tuttavia, il selettore di data del calendario non è accessibile dalla tastiera. Il calendario viene visualizzato ma non è possibile selezionare una data dal calendario utilizzando la tastiera. La selezione delle date dal calendario funziona solo se si utilizza un mouse.

Per aggirare il problema, completare i seguenti passi per immettere le date manualmente utilizzando la tastiera.

### Procedura

1. Nel portlet Report, selezionare il report predefinito nella parte inferiore della pagina e fare clic su **Configura il report**.
2. Nel campo **Dalla data**, immettere la data per la quale si stanno visualizzando le informazioni. Se si sta immettendo un intervallo di date, questa è la data di inizio.
3. Nel campo **Alla data**, immettere la data di fine dell'intervallo di date per le informazioni del report.
4. Fare clic su **Visualizza il report**.

## I nuovi eventi non vengono visualizzati nel portlet Dettagli

Se i nuovi eventi non vengono visualizzati nel portlet Dettagli, è possibile eseguire alcuni passi per risolvere il problema.

### Informazioni su questa attività

Se il problema non viene risolto con il primo passo, procedere al passo successivo. Continuare con ciascun passo fino a quando il problema non viene risolto.

### Procedura

1. Verificare lo stato del probe XML di IBM Intelligent Operations Center
  - a. Accedere al server eventi come root ed immettere il comando:
    - `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
  - b. Verificare che nella parte inferiore del file sia visualizzata la stringa Connection status OK.

- c. Se viene visualizzato un messaggio Probe shutting down oppure se la data e l'ora non corrispondono all'ora del server corrente, completare i passi riportati di seguito:
- 1) Ridenominare il log corrente immettendo il comando riportato di seguito:
 

```
- mv /opt/IBM/netcool/omnibus/log/ioc_xml.log
/opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```
  - 2) Riavviare il probe immettendo il comando riportato di seguito:
 

```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/i
```
  - 3) Attendere circa 1 minuto, quindi immettere il comando:
 

```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Ricerca la stringa Connection Status OK. Se lo stato della connessione non è OK, ricercare gli errori nel file. I problemi di connessione possono indicare che il server di oggetti è inattivo. Consultare il passo 2.
2. Se il probe XML di IBM Intelligent Operations Center continua ad essere arrestato, completare i passi riportati di seguito per verificare lo stato del database Tivoli Netcool/OMNIBus. Se il probe XML di IBM Intelligent Operations Center non continua ad essere arrestato, continuare al passo 3.
- a. Accedere al server eventi come `ibmadmin` ed immettere il comando:
 

```
- /opt/IBM/netcool/omnibus/bin/nco_config &
```
  - b. Se viene richiesto di eseguire l'importazione da `omni.dat`, selezionare **Sì** e fare clic su **Fine**.
  - c. Ridurre al minimo la finestra dell'agent del processo e fare clic sul tasto destro del mouse su **NCOMS**.
 

Se l'opzione **Connect As** è disponibile, fare clic su di essa, effettuare la connessione come `root` ed utilizzare la password della topologia.

Se l'opzione **Connect As** non è visualizzata, chiudere `nco_config` e, come `ibmadmin`, immettere il comando riportato di seguito per avviare il server di oggetti NCOMS:

```
- /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

Se il server di oggetti NCOMS non viene avviato, aprire `/opt/IBM/netcool/omnibus/var`, individuare e rimuovere il file `NCOMS.pid` ed immettere il comando riportato di seguito:

```
/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```
- Nota:** Una volta avviato il server di oggetti NCOMS, è necessario riavviare il probe XML di IBM Intelligent Operations Center. Consultare il passo 1 a pagina 332.
3. Verificare lo stato di Tivoli Netcool/Impact.
- a. Accedere al server eventi all'indirizzo `http://EventsHost:9080/nci/login_main.jsp` come `admin`. Se non è possibile effettuare l'accesso, eseguire i comandi riportati di seguito sul server eventi:
 

```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```
  - b. Nella finestra **Stato servizio**, scorrere verso il basso e verificare che i seguenti servizi siano in esecuzione:
    - **EventProcessor**
    - **IOC\_CAP\_Event\_Reader**
    - **IOC\_Notification\_Reader**

**Nota:** Accanto ai servizi in esecuzione, è visualizzato un segno di spunta verde.
  - c. Nella finestra **Stato servizio**, fare clic sull'icona **Visualizza log** accanto a **PolicyLogger** e ricercare gli errori nel file di log.
 

Se nel log vengono rilevati degli errori, è possibile visualizzare i dettagli del file di log in `/opt/IBM/netcool/impact/log/`. Per ulteriori dettagli, fare clic su **PolicyLogger**, impostare **Highest log level** su **3** e selezionare le caselle di spunta rilevanti.
4. Verificare se gli eventi sono bloccati in una delle code WebSphere MQ.

- a. Utilizzare un client VNC per accedere al server eventi ed immettere i comandi riportati di seguito per aprire WebSphere MQ Explorer:

```
xhost +  
su - mqm  
strmqcfcfg &
```

**Nota:** Se viene visualizzata la pagina di benvenuto, chiuderla.

- b. Espandere **IBM WebSphere MQ > Gestori code > IOC.MC.QM > QueuesLocate** e selezionare la cartella **Code**.
  - c. Nella tabella **Code**, selezionare la casella **Profondità coda corrente** di tutte le code che iniziano con **IOC\_**. Ad esempio, **IOC\_KPI\_IN\_INTERNAL\_USE\_ONLY\_DO\_NOT\_MODIFY**.  
Una profondità della coda maggiore di 0 per un qualsiasi intervallo di tempo può indicare un problema.
5. Verificare che gli eventi CAP raggiungano il database IBM Intelligent Operations Center.
    - a. Utilizzare un client VNC per accedere al server di dati e immettere i seguenti comandi per aprire DB2 Control Center:

```
xhost +  
su - db2inst1  
Db2cc &
```
    - b. Fare clic su **Tabelle > IOCDDB**, fare clic con il tasto destro del mouse su **Evento** nello schema **IOC\_COMMON** e fare clic su **Apri**. Viene visualizzato un elenco di eventi inoltrati al sistema.
    - c. Verificare che gli eventi siano nel database.

**Nota:** Potrebbe essere necessario richiamare più righe, in base al numero di eventi presenti nel sistema.

6. Per impostare la traccia sul server portale, effettuare le operazioni riportate di seguito:
  - a. Accedere alla console di gestione all'indirizzo `http://app-host:9060/ibm/console`, dove `app-host` è il nome host completo del server delle applicazioni.
  - b. Fare clic su **Risoluzione dei problemi > Log e traccia**.
  - c. Fare clic su **WebSphere\_Portal > Modifica dettagli livello di log**.
  - d. Fare clic sulla scheda **Runtime**, incollare il seguente comando e fare clic su **OK**.

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```
  - e. Per visualizzare un log, immettere il comando riportato di seguito:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal  
tail -f trace.log
```

Per ulteriori informazioni relative alla visualizzazione dei log, consultare il link correlato alla fine dell'argomento.

#### Concetti correlati:

“Abilitazione delle tracce e visualizzazione dei file di log” a pagina 295

Per risolvere un problema in IBM Intelligent Operations Center, potrebbe essere necessario analizzare i file di log in diversi sistemi. I seguenti argomenti forniscono una guida su come accedere ai file di log.

## Meccanismo di autenticazione non disponibile

Se si riceve il messaggio di errore HPDIA0119W Meccanismo di autenticazione non disponibile dopo l'accesso a error message after you log on to the WebSphere Portal, controllare lo stato di Tivoli Directory Server e del proxy Tivoli Directory Server per il server delle applicazioni.

### Procedura

1. Accedere al server di gestione come `ibmadmin` ed immettere i seguenti comandi:

```
su - ibmadmin  
cd /opt/IBM/ISP/mgmt/scripts  
./iopmgmt.sh status tds password_topologia
```

Se il server è in esecuzione, verrà restituito un messaggio simile a quello riportato di seguito:

```
Esecuzione comando query.....completata.  
Comando IBM Tivoli Directory Server [ on ]  
completato correttamente.
```

2. Se il server non è in esecuzione, immettere `./iopmgmt.sh start tds password_topologia`
3. Se il server non è in esecuzione dopo aver completato i passi 1 a pagina 334 e 2, accedere al server di gestione come `ibmadmin` ed immettere i seguenti comandi:

```
su - ibmadmin  
cd /opt/IBM/ISP/mgmt/scripts  
./iopmgmt.sh status tdspxyapp password_topologia
```

Se il server è in esecuzione, verrà restituito un messaggio simile a quello riportato di seguito:

```
Esecuzione comando query.....completata.  
Comando IBM Tivoli Directory Server [ on ]  
completato correttamente.
```

4. Se il server non è in esecuzione, immettere `./iopmgmt.sh start tdspxyapp password_topologia`

## Un server di terze parti non risponde

Se si riceve il messaggio di errore Un server di terze parti non risponde dopo l'accesso al portale WebSphere Portal, controllare lo stato di WebSphere Portal.

### Procedura

1. Accedere al server di gestione come `ibmadmin` ed immettere il seguente comando:

```
su - ibmadmin  
cd /opt/IBM/ISP/mgmt/scripts  
./iopmgmt.sh status wpe password_topologia
```

Se il portale è in esecuzione, verrà restituito un messaggio simile a quello riportato di seguito:

```
Esecuzione comando query.....completata.  
Comando IBM WebSphere Portal Extend [ on ]  
completato correttamente.
```

2. Se il portale non è in esecuzione, immettere `./iopmgmt.sh start wpe password_topologia`.

## Nel portlet Attività personali non viene visualizzata alcuna attività

Se non è possibile visualizzare alcuna attività nel portlet Attività personali, le cause possibili sono descritte nelle sezioni riportate di seguito.

## Risoluzione dei problemi relativi ai dati di esempio

Utilizzare i dati di esempio per creare un evento ed utilizzare i risultati per ridurre il numero di cause possibili delle attività non visualizzate.

### Procedura

1. Accedere all'interfaccia di gestione IBM Intelligent Operations Center come `wpsadmin`.
2. Creare un evento "Avvicinamento uragano":
  - a. Nel portlet Mappa, fare clic con il tasto destro sulla mappa, quindi fare clic su **Aggiungi evento**.
  - b. Per **Tipo evento**, selezionare **Avvicinamento uragano**. Gli altri campi vengono popolati automaticamente.
  - c. Per **Urgenza**, selezionare **Previsto**.
  - d. Mantenere i valori predefiniti per gli altri parametri dell'evento e fare clic su **OK**.

I parametri per l'evento "Avvicinamento uragano" sono associati ad una procedura operativa standard di esempio nella matrice di selezione procedura operativa standard.

3. Dopo circa 5 minuti, verificare che nel portlet Attività personali sia visualizzata una nuova attività che corrisponde all'evento "Avvicinamento uragano".

## Risultati

- Se nel portlet Attività personali non è visualizzata un'attività che corrisponde all'evento "Avvicinamento uragano", il problema delle attività non visualizzate per un altro utente potrebbe essere causato da un problema relativo a Tivoli Service Request Manager.
- Se nel portlet Attività personali è visualizzata un'attività che corrisponde all'evento "Avvicinamento uragano", il problema delle attività non visualizzate per un altro utente potrebbe essere causato da uno dei motivi riportati di seguito:
  - Le autorizzazioni utente non sono configurate correttamente.
  - Una procedura operativa standard non è configurata correttamente.
  - La matrice di selezione procedura operativa standard non è configurata correttamente.

### Riferimenti correlati:

"Esempi e risorse procedure operative standard, flussi di lavoro" a pagina 138

Esempi e risorse procedure operative standard, flussi di lavoro sono forniti quando si installa IBM Intelligent Operations Center Versione 1.5.

## Verifica dello stato di Tivoli Service Request Manager

Se nel portlet Attività personali non viene visualizzata alcuna attività quando viene creato un evento utilizzando i dati di esempio, utilizzare la seguente procedura per la risoluzione dei problemi relativi a Tivoli Service Request Manager.

### Prima di iniziare

Verificare che la password di gestione di Tivoli Service Request Manager sia stata codificata correttamente. Per ulteriori informazioni, consultare il link alla fine della procedura.

### Informazioni su questa attività

Selezionare una delle opzioni riportate di seguito.

### Procedura

- Utilizzare lo Strumento di controllo della piattaforma per verificare lo stato di Tivoli Service Request Manager:
  1. Accedere al server eventi come `ibmadmin` con il comando `putty`.
  2. Passare alla directory `opt/IBM/ISP/mgmt/scripts`.
  3. Utilizzare lo Strumento di controllo della piattaforma per visualizzare lo stato di Tivoli Service Request Manager e per arrestare ed avviare Tivoli Service Request Manager. Per ulteriori informazioni relative all'esecuzione dello Strumento di controllo della piattaforma, consultare i link alla fine della procedura.
- In alternativa, per riavviare manualmente Tivoli Service Request Manager, effettuare le operazioni riportate di seguito:
  1. Accedere al server eventi come `ibmadmin` con il comando `putty`.
  2. Per arrestare Tivoli Service Request Manager, immettere i comandi riportati di seguito:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
./stopServer.sh MXServer1 -user waswebadmin -password password
./stopNode.sh -user waswebadmin -password password
../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password password
```

dove *password* è la password della topologia.
  3. Per avviare Tivoli Service Request Manager, immettere i comandi riportati di seguito:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
../../ctgDmgr01/bin/startManager.sh
./startNode.sh -user waswebadmin
./startServer.sh MXServer1
exit
```

#### **Attività correlate:**

“Query dello stato dei servizi” a pagina 202

Strumento di controllo della piattaforma è disponibile per determinare lo stato dei servizi IBM Intelligent Operations Center.

“Avvio dei servizi” a pagina 196

Strumento di controllo della piattaforma è disponibile per avviare i servizi in esecuzione nei server IBM Intelligent Operations Center.

“Arresto dei servizi” a pagina 199

Strumento di controllo della piattaforma è disponibile per arrestare i servizi IBM Intelligent Operations Center.

“Codifica della password di gestione di Tivoli Service Request Manager” a pagina 60

Utilizzare la seguente procedura per codificare la password di gestione di Tivoli Service Request Manager in Tivoli Netcool/Impact.

## **Verifica delle autorizzazioni utente**

Verificare che un utente disponga delle autorizzazioni per la visualizzazione delle attività associate ad una procedura operativa standard.

### **Procedura**

1. Per aprire il portlet SOP (Standard Operating Procedure), nell'interfaccia di gestione di WebSphere Portal, fare clic su **Intelligent Operations > Strumenti di personalizzazione > SOP (Standard Operating Procedure)**.
2. Per aprire l'applicazione Matrice di selezione SOP (Standard Operating Procedure), fare clic su **Matrice di selezione SOP (Standard Operating Procedures)**.
3. Nella colonna **Nome SOP**, individuare il nome di una procedura operativa standard di cui si desidera verificare le autorizzazioni utente.
4. Accanto al campo **Nome SOP**, fare clic sull'icona **Menu Dettagli**, quindi fare clic su **Passa a SOP (Standard Operating Procedure)**.
5. Accanto al campo **Gruppo proprietario**, fare clic sull'icona **Menu Dettagli** e fare clic su **Passa a Gruppi di persone**.
6. Verificare che l'utente sia membro del gruppo di persone.

### **Operazioni successive**

Se l'utente non è membro del gruppo di persone, effettuare una delle azioni riportate di seguito:

- Non assegnare le autorizzazioni utente per la visualizzazione di attività associate alla procedura operativa standard.
- Aggiungere l'utente al gruppo di persone, in modo che l'utente possa visualizzare tutte le attività assegnate al gruppo di persone.
- Aggiungere l'utente ad un altro gruppo di persone associato alla procedura operativa standard.

Per ulteriori informazioni relative alla configurazione degli utenti, consultare il link alla fine dell'attività.

#### **Attività correlate:**

“Configurazione di nuovi utenti in Tivoli Service Request Manager” a pagina 126  
Quando si aggiunge un utente in IBM Intelligent Operations Center, assegnare le autorizzazioni e i gruppi di persone per l'utente in Tivoli Service Request Manager.

## **Verifica dell'associazione di un flusso di lavoro ad una procedura operativa standard**

Creare un evento i cui parametri corrispondono ad una serie di criteri di selezione definiti nella matrice di selezione procedura operativa standard. Verificare che le attività del flusso di lavoro associato siano visualizzate nel portlet Attività personali.

### **Informazioni su questa attività**

Per ulteriori informazioni relative a ciascuno dei passi riportati di seguito, consultare i link alla fine della procedura.

### **Procedura**

1. Creare un flusso di lavoro.
2. Creare una procedura operativa standard ed associarla al flusso di lavoro creato al passo precedente.
3. Creare una voce per la procedura operativa standard nella matrice di selezione procedura operativa standard.
4. Nel portlet Mappa, creare un evento che corrisponda ai parametri definiti nella matrice di selezione procedura operativa standard.
5. Verificare che le attività del flusso di lavoro associato siano visualizzate nel portlet Attività personali.

### **Operazioni successive**

Se nel portlet Attività personali non è visualizzata alcuna attività, verificare che il flusso di lavoro, la procedura operativa standard, la matrice di selezione procedura operativa standard e l'evento siano stati configurati correttamente. Se la configurazione è corretta, verificare il file di log della politica Tivoli Netcool/OMNIBus ed i file di log di Tivoli Service Request Manager.

#### **Concetti correlati:**

“Mappa” a pagina 279

Utilizzare il portlet Mappa per visualizzare eventi e risorse presenti su una mappa.

“Attività personali” a pagina 284

Il portlet Attività personali visualizza un elenco dinamico di attività di proprietà del gruppo di cui l'utente collegato all'interfaccia è membro.

#### **Attività correlate:**

“Creazione di flussi di lavoro” a pagina 128

In Tivoli Service Request Manager, è possibile creare flussi di lavoro che è possibile includere come attività automatizzate nelle attività procedura operativa standard.

“Creazione di procedure operative standard” a pagina 129

Creare una procedura operativa standard ed assegnarla ad un gruppo proprietario. Gli utenti vengono assegnati ad un gruppo proprietario mediante la relativa appartenenza ad un gruppo di persone.

“Definizione dei parametri nella matrice di selezione procedura operativa standard” a pagina 131

Nella matrice di selezione procedura operativa standard, definire i parametri degli eventi che determinano se una procedura operativa standard è selezionata per un particolare evento.

## **Verifica dei file di log**

Verificare il file di log della politica Tivoli Netcool/OMNIBus ed i file di log di Tivoli Service Request Manager.



## Procedura

- Verificare il file di log della politica Tivoli Netcool/OMNIBus:
  1. Abilitare il file di log della politica Tivoli Netcool/OMNIBus. Per informazioni relative all'abilitazione ed all'utilizzo del file di log, consultare il link alla fine della procedura.
  2. Nel file di log della politica Tivoli Netcool/OMNIBus, per individuare un evento, ricercare CallMaximoEnterpriseServices. Il file di log della politica Tivoli Netcool/OMNIBus analizza gli eventi in base al parametro, ad esempio Categoria eGravità, ed elenca ciascun evento con il relativo ID ordine lavoro associato. È possibile associare gli eventi rispetto alla matrice di selezione procedura operativa standard. Se un evento non è elencato nel file di log della politica Tivoli Netcool/OMNIBus, il motivo probabile è che nessuna procedura operativa standard corrisponde ai parametri dell'evento.
  3. Ricercare server error 500, che indica un errore del server Tivoli Service Request Manager. Se viene visualizzato questo errore, verificare il file di log Tivoli Service Request Manager. Consultare il link alla fine della procedura.
- Verificare il file di log Tivoli Service Request Manager. Per informazioni relative all'abilitazione ed all'utilizzo del file di log, consultare il link alla fine della procedura.

### Attività correlate:

“Abilitazione e visualizzazione dei file di log Tivoli Netcool/Impact” a pagina 299

“Abilitazione della traccia e visualizzazione dei file di log per Tivoli Service Request Manager” a pagina 296

## I dati KPI non vengono visualizzati nei portlet Stato o Drill Down KPI (Key Performance Indicator)

Se i dati KPI non vengono visualizzati nei portlet Stato o Drill Down KPI (Key Performance Indicator), effettuare le operazioni riportate nella procedura per risolvere il problema.

## Procedura

1. Per verificare lo stato di IBM WebSphere Business Monitor, accedere alla console di gestione WebSphere Application Server. Per ulteriori informazioni relative all'accesso alle console di gestione, selezionare il link alla fine dell'argomento.
2. Se IBM WebSphere Business Monitor è arrestato, riavviarlo. Se IBM WebSphere Business Monitor non è arrestato, prima arrestarlo, quindi riavviarlo. Se il problema non viene risolto, continuare al passo 3.
3. Consultare i log di IBM WebSphere Business Monitor per esaminare e risolvere eventuali problemi relativi a IBM WebSphere Business Monitor. Per ulteriori informazioni relative al controllo dei log, selezionare il link alla fine dell'argomento.
4. Una volta risolti tutti i problemi relativi a IBM WebSphere Business Monitor, accedere alla console di gestione WebSphere Application Server per riavviare IBM WebSphere Business Monitor.

### Concetti correlati:

“File di log del Server delle applicazioni” a pagina 295

Utilizzare le seguenti procedure per abilitare le tracce e visualizzare i log per alcuni dei sistemi sul server delle applicazioni.

“Console di gestione” a pagina 203

Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.

## Gli eventi non vengono aggiornati nei portlet Stato o Drill Down KPI (Key Performance Indicator)

Se i dati evento KPI non vengono aggiornati nei portlet Stato o Drill Down KPI (Key Performance Indicator), effettuare le operazioni riportate nella procedura fino a quando il problema non viene risolto.

## Procedura

1. Per confermare che gli aggiornamenti degli eventi KPI raggiungano IBM Intelligent Operations Center, passare al link *I nuovi eventi non vengono visualizzati nel portlet Dettagli* alla fine dell'argomento e seguire i passi riportati.
2. Confermare che gli eventi raggiungano IBM WebSphere Business Monitor.
  - a. Accedere alla console di gestione WebSphere Application Server. Per ulteriori informazioni relative all'accesso alle console di gestione, selezionare il link alla fine dell'argomento.
  - b. Fare clic su **Risoluzione dei problemi > Modelli di monitoraggio > Sequenze di eventi non riusciti**. Eliminare gli eventi KPI visualizzati in questa pagina.
  - c. Riavviare IBM WebSphere Business Monitor.
  - d. Fare clic su **Applicazioni > Servizi di monitoraggio > Gestione eventi registrati > Abilita/Disabilita registrazione eventi** ed abilitare la registrazione eventi.
  - e. Fare clic su **Applicazioni > Servizi di monitoraggio > Gestione eventi registrati > Gestione eventi**. Verificare che in questa pagina siano presenti almeno due eventi creati per ciascun evento KPI inviato a IBM Intelligent Operations Center.
3. Confermare che gli aggiornamenti degli eventi KPI raggiungano il portlet KPI (Key Performance Indicators). Per ulteriori informazioni relative al portlet KPI (Key Performance Indicators), selezionare il link alla fine dell'argomento. Se i valori KPI vengono aggiornati nel portlet KPI (Key Performance Indicators), i valori sono aggiornati in IBM WebSphere Business Monitor.

### Concetti correlati:

“Console di gestione” a pagina 203

Utilizzare il portlet Console di gestione per gestire i servizi forniti dalla soluzione.

“KPI (Key Performance Indicators)” a pagina 168

Utilizzare il portlet KPI (Key Performance Indicators) per personalizzare i KPI (Key Performance Indicators) e la loro visualizzazione gerarchica in IBM Intelligent Operations Center.

### Attività correlate:

“I nuovi eventi non vengono visualizzati nel portlet Dettagli” a pagina 332

Se i nuovi eventi non vengono visualizzati nel portlet Dettagli, è possibile eseguire alcuni passi per risolvere il problema.

---

## Capitolo 10. Riferimento

Questi argomenti contengono ulteriori informazioni di riferimento utili per l'utente.

---

### Prodotti e componenti inclusi con IBM Intelligent Operations Center

La soluzione IBM Intelligent Operations Center installa una serie di prodotti e componenti software.

I prodotti ed i componenti software ed i server su cui sono installati vengono mostrati in Tabella 100.

*Tabella 100. Prodotti installati con IBM Intelligent Operations Center*

Prodotto	Server delle applicazioni	Server di dati	Server eventi	Server di gestione
IBM WebSphere Business Monitor 7.5	installato	non installato	non installato	non installato
IBM Cognos Business Intelligence 10.1.1	installato	non installato	non installato	non installato
DB2 Enterprise Server Edition con DB2 Spatial Extender 9.7.0.5	non installato	installato	non installato	installato
Servizi di modelli semantici	non installato	non installato	non installato	installato
IBM ILOG CPLEX Optimization Studio 12.4	installato	non installato	non installato	non installato
Jazz Foundation Server (per Servizi di modelli semantici) 3.0.1	non installato	non installato	non installato	installato
Lotus Domino 8.5.3.1	non installato	non installato	installato	non installato
Lotus Sametime Standard 8.5.2 + IFR1	non installato	non installato	installato	non installato
Tivoli Access Manager for e-Business 6.1.1.4	non installato	non installato	non installato	installato
Tivoli Composite Application Manager 7.1	non installato	non installato	non installato	installato
Tivoli Directory Integrator 7.1.0.5	non installato	non installato	non installato	installato
Tivoli Directory Server 6.3.0.8	non installato	installato	non installato	non installato
Tivoli Identity Manager 5.1	non installato	non installato	non installato	installato
Tivoli Monitoring 6.2.2.1	non installato	non installato	non installato	installato

Tabella 100. Prodotti installati con IBM Intelligent Operations Center (Continua)

Prodotto	Server delle applicazioni	Server di dati	Server eventi	Server di gestione
Tivoli Netcool/Impact 5.1.1.1 + IF003	non installato	non installato	installato	non installato
Tivoli Netcool/OMNIBus 7.3.1.2 e probe XML	non installato	non installato	installato	non installato
Tivoli Service Request Manager 7.2.1.2	non installato	non installato	installato	non installato
WebSphere Application Server 1.1.0.0 Feature Pack for Web 2.0 and Mobile	installato	non installato	non installato	non installato
WebSphere Application Server Network Deployment 7.0.0.21	installato	non installato	non installato	installato
WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager	non installato	non installato	installato	non installato
WebSphere Message Broker 8.0	non installato	non installato	installato	non installato
WebSphere MQ 7.0.1.7	non installato	non installato	installato	non installato
WebSphere Operational Decision Management 7.5.1 (Rules Engine)	installato	non installato	non installato	non installato
WebSphere Portal Enable 7.0.0.2	installato	non installato	non installato	non installato

## Processi in esecuzione con l'account root

Dopo l'esecuzione di Cyber Hygiene, alcuni processi devono ancora essere eseguiti con l'account root.

I processi in esecuzione con l'account root possono essere vulnerabili se un utente o processo è in grado di ottenere i privilegi root mediante un aumento di privilegi. Normalmente questo è solo un problema per i servizi che elaborano le richieste originate da un utente. Le richieste originate dall'utente possono contenere dati di input configurati in modo dannoso che possono compromettere la funzionalità del server. I servizi che elaborano le richieste dell'utente sono sistemi che forniscono interfacce utente o API (Application Programming Interface) accessibili.

I daemon Linux non sono generalmente a rischio dal momento che avviano, arrestano o rispondono soltanto agli eventi di sistema correttamente definiti. In molti casi, questi daemon devono essere eseguiti con account root in modo che possano controllare altri processi o rispondere a eventi di sistema critici. Fino a quando un server accessibile all'utente stesso non è in esecuzione come root, i daemon in esecuzione con l'account root non presentano come grave un rischio.

Con l'eccezione di Tivoli Netcool/OMNIBus, tutti i server di prodotti in IBM Intelligent Operations Center sono configurati con ID che non dispongono di privilegi di sistema. Tivoli Netcool/OMNIBus fornisce servizi di monitoraggio e di gestione su tutti i server e gli host IBM Intelligent Operations Center.

Tabella 101 elenca i processi che continuano l'esecuzione come account root dopo l'esecuzione di Cyber Hygiene.

Tabella 101. Processi dell'ambiente IBM Intelligent Operations Center in esecuzione come root

Server	Prodotto	Nome processo	Spiegazione
server di dati e server di gestione	DB2	db2wdog	Questo processo daemon riceve gli eventi di sistema e li trasmette a più processi child. Il processo db2wdog gestisce i processi db2sync e richiede una gestione a livello root.
server di dati e server di gestione	DB2	db2chkpwd	Questo daemon autentica l'ID e la password dell'utente o l'applicazione che si connette ad un database. Il processo db2chkpwd deve leggere il file della password /etc/shadow.
server di dati e server di gestione	DB2	/opt/IBM/DB2/bin/db2fmcd	Questo daemon viene utilizzato come coordinatore di monitoraggio degli errori. Deve essere eseguito come root per monitorare tutte le istanze DB2.
server di dati e server di gestione	DB2	/usr/sbin/rcst/bin/rmcd e /usr/sbin/rcst/bin/IBM.ConfigRMd	Questi comandi gestiscono la soluzione ad alta disponibilità per DB2. Necessitano dell'accesso a tutti i database sui server configurati per l'alta disponibilità.
server eventi	Agent IBM Tivoli Monitoring per Lotus Domino	kgbagent, kgbclient, kslagent	Tali agenti di monitoraggio devono essere eseguiti come root per tenere traccia dell'attività del server Lotus Domino.
server delle applicazioni, server eventi e server di gestione	IBM HTTP Server	httpd -d, http -f	Linux richiede l'accesso root per restare in ascolto sulle porte inferiori a 1024. Le porte HTTP standard vanno da 80 a 443. IBM Intelligent Operations Center utilizza la porta 82. I processi httpd -d e http -f devono essere eseguiti come root. Qualsiasi configurazione alternativa è responsabile dell'installazione come parte della rete globale e della configurazione e politica di protezione.
server di dati	Agenti di IBM Tivoli Monitoring	klzagent, kcawd	Si tratta di processi agenti di gestione e di monitoraggio. Questi processi monitorano il sistema operativo e le risorse e i processi di applicazioni.
server delle applicazioni	Agenti di IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent	Si tratta di processi agenti di gestione e di monitoraggio. Questi processi monitorano il sistema operativo e le risorse e i processi di applicazioni.
server eventi	Agenti di IBM Tivoli Monitoring	klzagent, kcawd, khtagent, kynagent, kmcrca, kgbagent, kgbstart.sh, kgbclient, kslagent, kmqagent, /opt/IBM/ITM/JRE/1x8266/bin/java	Si tratta di processi agenti di gestione e di monitoraggio. Questi processi monitorano il sistema operativo e le risorse e i processi di applicazioni.
server di gestione	Agenti di IBM Tivoli Monitoring	cms, kdsmain, KfwServices, klzagent, kcawd, kynagent, /opt/IBM/ITM/1i6263/iw/java/jre/bin/java, /opt/IBM/ITM/1i6263/iw/java/bin/java	Si tratta di processi agenti di gestione e di monitoraggio. Questi processi monitorano il sistema operativo e le risorse e i processi di applicazioni.
server eventi	Tivoli Netcool/OMNIBus	/usr/ibm/common/acsi/jre/bin/java, /opt/IBM/netcool/omnibus/platform/linux2x26/bin/nco_pad	Il processo nco_pad è il daemon dell'agent del processo che monitora tutti gli agent del processo. Il daemon richiede l'accesso alle risorse di sistema. Il daemon dell'agent del processo non dispone di un'interfaccia utente. Esso gestisce solo altri processi.

## Eccezioni Cyber hygiene

Una volta eseguito cyber hygiene, rimangono eccezioni note alla configurazione di sicurezza preferita.

La configurazione ideale non ha eccezioni rispetto alle pratiche consigliate. Tuttavia la maggior parte dei sistemi hanno eccezioni. Tali eccezioni non presentano un rischio significativo, ma potrebbero essere problematiche se non comprese. Ad esempio, alcuni programmi potrebbero dover essere eseguiti con il bit **suid** impostato.

Gli amministratori della sicurezza devono comprendere le eccezioni in modo da verificare se il sistema è stato compromesso. Durante il controllo possono distinguere tra le eccezioni previste e quello non desiderate.

Tabella 102. Eccezioni Cyber hygiene alla configurazione di sicurezza preferita.

Vulnerabilità	Server	Istanza	Spiegazione
GEN000360: GID impostato ad un valore nell'intervallo di sistema per Linux (0-499).	server di dati	dasadm1	L'ID gruppo dasadm1 (GID) è impostato su 102. Questo è il gruppo di gestione degli ID dell'istanza runtime di DB2. Questo gruppo viene creato automaticamente quando si installa DB2 .

## Le autorizzazioni file che richiedono la convalida dell'amministratore di sistema

Cyber hygiene non apporta modifiche alle vulnerabilità nelle autorizzazioni e nel proprietario del file. Alcune di queste devono essere valutate e corrette dagli amministratori di sistema poiché le modifiche automatizzate potrebbero rendere alcune funzioni di sistema inutilizzabili.

Gli script cyber hygiene registrano informazioni relative alle risorse potenzialmente influenzate. Gli amministratori di sistema possono esaminare questi rilevamento e apportare le modifiche al sistema necessarie.

I file dei rilevamenti si trovano nella directory `/var/BA15/CH/results` di ciascun server IBM Intelligent Operations Center. Il file si chiama `scanrem-combined-log-date-time.log`. La data/ora indica quando è stato eseguito cyber hygiene.

Tabella 103 elenca le vulnerabilità che necessitano di un controllo e le azioni consigliate.

Tabella 103. Vulnerabilità che richiedono la valutazione da parte dell'amministratore di sistema

STIGID	Descrizione	Gravità	Suggerimento
GEN001220	I file, le applicazioni e le directory nelle directory di sistema devono essere posseduti da un account di sistema o da un account applicazione.	II	Controllare la proprietà della risorsa e modificare manualmente o documentare come richiesto.
GEN001240	I file, le applicazioni e le directory nelle directory di sistema devono essere posseduti da un gruppo di sistema o da un gruppo applicazione.	II	Controllare la proprietà del gruppo della risorsa e modificare manualmente o documentare come richiesto.
GEN001500	La directory home, elencata per un utente nel file <code>/etc/passwd</code> , deve essere posseduta da un utente.	II	Controllare la proprietà della directory home e modificare manualmente la proprietà, o documentare il perché non può essere modificata.
GEN001520	La directory home, elencata per un utente nel file <code>/etc/passwd</code> , deve essere posseduta dal gruppo primario dell'utente.	II	Controllare la proprietà del gruppo della directory home e modificare manualmente la proprietà del gruppo, o documentare il perché non può essere modificata.
GEN001560	I file nella home directory, tranne i file di avvio, devono avere autorizzazioni non superiori a 750.	III	Modificare le autorizzazioni se le eccezioni non sono state già documentate.

Tabella 103. Vulnerabilità che richiedono la valutazione da parte dell'amministratore di sistema (Continua)

STIGID	Descrizione	Gravità	Suggerimento
GEN002520	Le directory pubbliche devono essere di proprietà dell'account root o di un ID utente dell'applicazione.	II	Controllare la proprietà ed assegnarla in modo appropriato.
GEN002540	Le directory pubbliche deve essere di proprietà di root, sys, bin, o di un gruppo applicazioni.	II	Controllare la proprietà del gruppo ed assegnarla in modo appropriato.

## Certificazione della sicurezza del prodotto e dei componenti

Alcuni dei prodotti e dei componenti inclusi come parte della soluzione IBM Intelligent Operations Center hanno certificati di sicurezza.

Tabella 104. Certificazioni di sicurezza dei prodotti installati con IBM Intelligent Operations Center

Prodotto	Criteri comuni		FIPS 140-2		IPV6
	Release	Livello	Release	Certificato?	
IBM WebSphere Business Monitor	Nessuna	Nessuna	7.5	Sì	Sì
IBM Cognos Business Intelligence	10.1.1	Nessuna	Nessuna	Nessuna	Sì
DB2 Enterprise Server Edition con DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	Sì	Sì
IBM HTTP Server	7.0.0.19		7.0	Sì	Sì
Lotus Domino	Nessuna	Nessuna	8.0.1	Sì	Sì
Lotus Sametime Standard	Nessuna	Nessuna	8.5	Sì	Sì
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	Sì	Sì
Tivoli Composite Application Manager	Nessuna	Nessuna	Nessuna	Nessuna	Sì
Tivoli Directory Integrator	Nessuna	Nessuna	7.0	Sì	Sì
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	Sì	Sì
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	Nessuna	Nessuna	Sì
Tivoli Monitoring	Nessuna	Nessuna	6.2.0.1	Sì	Sì
Tivoli Netcool/Impact	Nessuna	Nessuna	5.1	Sì	Sì
Tivoli Netcool/OMNIBUS e probe XML	7.1	EAL2	Tutto	Sì	Sì
Tivoli Service Request Manager	Nessuna	Nessuna	Tutto	Sì	Sì
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	Tutto	Sì	Sì
WebSphere Application Server for Tivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	Tutto	Sì	Sì
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	Sì	Sì
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	Tutto	Sì	Sì
WebSphere Operational Decision Management (Rules Engine)	Nessuna	Nessuna	Nessuna	Nessuna	Sì
WebSphere Portal Enable	5.0	EAL2	Tutto	Sì	Sì

I prodotti con la certificazione 104-2 FIP sono solitamente destinati all'utilizzo con IBM Crypto per i moduli C e Java. I numeri dei certificati per questi prodotti sono mostrati in Tabella 105.

Tabella 105. Certificati FIPS 140-2

Modulo	Numero certificato
IBM Crypto for C (V8.0.0)	1433



Tabella 105. Certificati FIPS 140-2 (Continua)

Modulo	Numero certificato
IBM CryptoLite for Java (V4.2)	910
IBM CryptoLite for C (V4.5)	899
IBM Java JCE 140-2 Cryptographic Module	497
IBM Java JSSE FIPS 140-2 Cryptographic Module	409
IBM SSL Lite for Java	406

#### Informazioni correlate:

 Criteri comuni: <http://www.commoncriteriaportal.org/>

 Valutazioni di sicurezza per i prodotti IBM

---

## Libreria di PDF

Questo argomento fornisce i link per il contenuto del centro informazioni in formato PDF.

Il contenuto del centro informazioni è disponibile nel seguente PDF per convenienza di stampa:

- IBM Intelligent Operations Center Centro informazioni

---

## Glossario

Questo glossario contiene termini e definizioni per IBM Intelligent Operations Center.

In questo glossario vengono utilizzati i seguenti riferimenti incrociati:

- Vedere rinvia l'utente da un termine ad un sinonimo preferito o da un acronimo o abbreviazione alla definizione completa.
- Vedere anche conduce a un termine correlato o contrario.

Per visualizzare i glossari di altri prodotti IBM, andare a [www.ibm.com/software/globalization/terminology](http://www.ibm.com/software/globalization/terminology) (si apre in una nuova finestra).

"A" "B" a pagina 347 "C" a pagina 347 "D" a pagina 348 "E" a pagina 348 "F" a pagina 349 "G" a pagina 349 "H" a pagina 349 "I" a pagina 350 "J" a pagina 350 "K" a pagina 350 "L" a pagina 351 "M" a pagina 352 "N" a pagina 352 "O" a pagina 352 "P" a pagina 352 "R" a pagina 352 "S" a pagina 353 "T" a pagina 354 "U" a pagina 354 "V" a pagina 355 "W" a pagina 355 "X" a pagina 356

## A

### Abstract Syntax Notation One (ASN.1)

Lo standard internazionale per definire la sintassi dei dati di informazioni. Definisce un numero di tipi di dati semplici e specifica una notazione per fare riferimento a tali tipi e per la specifica dei valori di tali tipi. Le notazioni ASN.1 possono essere applicate ogniqualvolta è necessario definire la sintassi astratta di informazioni senza limitare in alcun modo il modo in cui le informazioni sono codificate per la trasmissione.

### elenco di controllo accessi (o ACL, access control list)

Nella sicurezza dei computer, un elenco associato a un oggetto che identifica tutti gli utenti che possono accedere all'oggetto e i relativi diritti di accesso.

**ACL** Vedere elenco controllo accessi.

**autorizzazione amministratore**

L'autorizzazione, concessa ad un amministratore, a fornire accesso per creare, configurare ed eliminare utenti o risorse del portale. Questa autorizzazione viene concessa dall'appartenenza ad un gruppo di ruoli utente.

**KPI di aggregazione**

Un valore KPI che viene calcolato da una metrica che utilizza una funzione di aggregazione.

**avviso** Un messaggio che segnala un evento o il cambiamento di stato di un indicatore di prestazioni chiave (o KPI - key performance indicator).

**trigger avviso**

La modifica di un valore indicatore di prestazioni chiave (o KPI - key performance indicator) predefinito che causa l'invio di una notifica di avviso al portlet Coordinatore - Avvisi.

**APAR** Vedere report di analisi programma autorizzata.

**ASN.1** Vedere Abstract Syntax Notation One.

**asincrono**

Relativo ad eventi che non sono sincronizzati nel tempo o che non si verificano ad intervalli di tempo regolari o prevedibili.

**attributo**

Caratteristica o tratto di un'entità che la descrive, ad esempio, il numero di telefono di un dipendente è uno degli attributi del dipendente.

**utente del portale autenticato**

Un utente che è membro di un gruppo generale all'interno di WebSphere Portal autenticato con un profilo contenente una password e un ID utente.

**autenticazione**

Servizio di sicurezza che fornisce una prova che l'utente di un sistema di computer è realmente la persona che dichiara di essere. Tra i meccanismi più comuni per l'implementazione di questo servizio vi sono le password e le firme digitali.

**autorizzazione**

Il processo con cui si concede a un utente, a un sistema o a un processo l'accesso completo o limitato a un oggetto, una risorsa o una funzione.

**permesso autorizzazione**

Accesso a un portale, risorsa o dati associato all'appartenenza di un gruppo.

**report di analisi programma autorizzata (o APAR - authorized program analysis report)**

Una richiesta di correzione di un difetto in una release supportata di un programma fornito da IBM.

**B****mapa di base**

Una mappa che rappresenta informazioni di riferimento di background, ad esempio morfologia, strade, punti di riferimento e confini politici, in cui sono inserite altre informazioni tematiche.

Una mappa di base viene utilizzata come riferimento posizionale e spesso include una rete di controllo geodetico come parte della sua struttura.

**C**

**cache** Memoria utilizzata per migliorare i tempi di accesso alle istruzioni, ai dati o a entrambi. I dati che risiedono nella memoria cache sono generalmente una copia di dati che si trovano altrove, in memorizzazioni meno costose e più lente, ad esempio su un disco o su un altro nodo di rete.

**CAP** Vedere Common Alerting Protocol.

### **applicazione cloud**

Un'applicazione che viene estesa per essere accessibile tramite Internet. Le applicazioni cloud utilizzano centri di dati di vaste dimensioni e potenti server che ospitano applicazioni e servizi Web.

### **CAP (Common Alerting Protocol)**

Un formato semplice ma generale per lo scambio di allarmi di pericolo e avvisi pubblici su tutti i tipi di reti.

### **widget comune**

Un widget fornito da IBM che non è associato a un prodotto particolare. Vedere anche widget.

### **configurazione**

1. Il modo in cui l'hardware e il software di un sistema, sottosistema o rete sono organizzati e interconnessi.
2. Il processo con cui vengono descritti a un sistema le unità, le caratteristiche opzionali e i prodotti software che sono stati installati, in modo che possano essere utilizzati. Vedere anche personalizzazione.

### **file CSV**

Un file di testo che contiene valori separati da virgole. Un file CSV viene comunemente utilizzato per scambiare file tra applicazioni e sistemi di database che utilizzano formati differenti.

### **personalizzazione**

1. Modifica della pagina di un portale o di un portlet da parte dell'utente. WebSphere Portal consente agli utenti di personalizzare una pagina di portale, modificando il layout della pagina e selezionando quale portlet visualizzare per unità. Vedere anche personalizzare.
2. Il processo per cui vengono descritte modifiche facoltative ai valori predefiniti di un programma software già installato sul sistema e configurato in modo da poter essere usato. Vedere anche configurazione.

## **D**

### **dashboard**

1. Pagina Web che può contenere uno o più widget per la rappresentazione grafica dei dati aziendali.
2. Un'interfaccia che integra i dati da un'ampia gamma di origini e fornisce una visualizzazione unificata di informazioni rilevanti e interne al contesto.

### **autorizzazione accesso dati**

Accesso ai dati in una particolare categoria, ad esempio, dati medici e sulla salute pubblica, o i dati ambientali. Questo accesso è associato ad un gruppo di categorie di dati.

### **gruppo di categorie di dati**

Un gruppo i cui membri hanno accesso a una categoria specifica di dati, ad esempio, dati medici e sulla salute pubblica, o i dati ambientali. L'appartenenza a un gruppo di categorie di dati viene assegnata per fornire all'utente il livello appropriato di accesso ai dati. Ogni utente viene aggiunto come membro del gruppo o dei gruppi appropriati.

### **dominio**

Un reparto singolo in un gruppo operativo più ampio, che generalmente corrisponde alla struttura dell'organizzazione e alle competenze delle persone coinvolte. Ad esempio, un'autorità cittadina è suddivisa in reparti che si occupano di trasporti, sistema idrico e sicurezza pubblica.

## **E**

**EAR** Vedere enterprise archive.

**EJB** Vedere Enterprise JavaBeans.

**EAR (enterprise archive)**

Tipo specifico di file JAR, definito dallo standard Java EE, utilizzato per distribuire applicazioni Java EE a server di applicazioni Java EE. Un file EAR contiene componenti EJB, un descrittore di distribuzione e file WAR (web archive) per le singole applicazioni web. Vedere anche Java archive.

**Enterprise JavaBeans (EJB)**

Architettura di componenti definita da Sun Microsystems per lo sviluppo e la distribuzione di applicazioni di livello enterprise, distribuite, orientate agli oggetti (Java EE).

**evento**

Una ricorrenza significativa che avviene in un dato luogo e momento. Vedere anche incidente.

**correlazione eventi**

Il processo di analisi dei dati evento per identificare modelli, cause comuni e cause principali. La correlazione eventi analizza gli eventi in entrata per gli stati predefiniti, utilizzando regole predefinite e rispetto a relazioni predefinite.

**espressione KPI**

Un KPI che ha il suo valore calcolato dai valori di altri KPI.

**Extensible Markup Language (XML)**

Un metalinguaggio standard per la definizione dei linguaggi di markup basati su SGML (Standard Generalized Markup Language).

**F****modulo di filtro**

Un modulo che può essere utilizzato per selezionare il contenuto da visualizzare sulla mappa e sull'elenco.

**G****GDDM**

Vedere Graphical Data Display Manager.

**GIS (geographical information system)**

Un insieme di oggetti, dati e applicazioni che viene utilizzato per creare e analizzare informazioni spaziali relative alle caratteristiche geografiche.

**geospaziale**

Relativo alle caratteristiche geografiche della terra.

**GIS** Vedere geographical information system.

**Graphical Data Display Manager (GDDM)**

Un sistema computer-graphics IBM che definisce e visualizza il testo e le immagini per l'emissione su un terminale video o stampante.

**gruppo**

Insieme di utenti che possono condividere autorizzazioni di accesso a risorse protette.

**H**

**heap** Nella programmazione Java, blocco di memoria che la JVM (Java Virtual Machine) utilizza al runtime per memorizzare oggetti Java. La memoria heap Java viene gestita da un programma di raccolta dati obsoleti, che dealloca automaticamente gli oggetti Java non più utilizzati.

**guida a comparsa**

Testo esplicativo che può essere visualizzato passando il cursore su un elemento della GUI (graphical user interface) come un'icona, un campo o una stringa di testo. La guida a comparsa può contenere testo rtf (rich text format) e link.

## I

### **incidente**

Evento che non fa parte delle operazioni standard di un servizio e causa o può causare una interruzione dei servizi o una riduzione della loro qualità e della produttività del cliente. Vedere anche evento.

### **integrazione**

Attività di sviluppo di software in cui dei componenti software separati vengono combinati in un unico corpo eseguibile.

### **modello ISO**

Serie di regole per la comunicazione dati, sancite da ISO (International Organization for Standardization). I protocolli ISO abilitano i sistemi di fornitori differenti a connettersi e comunicare. Sono la base degli standard OSI (open systems interconnection).

## J

**J2EE** Vedere Java Platform, Enterprise Edition.

**JAR** Vedere Java archive.

### **Java archive (JAR)**

Formato di file compresso per l'archiviazione di tutte le risorse richieste per installare ed eseguire un programma Java in un singolo file. Vedere anche enterprise archive.

### **Java EE**

Vedere Java Platform, Enterprise Edition.

### **Java Naming and Directory Interface (JNDI)**

Estensione della piattaforma Java che fornisce un'interfaccia standard per servizi di directory e denominazione eterogenei.

### **Java Platform, Enterprise Edition (J2EE, Java EE)**

Ambiente per lo sviluppo e la distribuzione di applicazioni enterprise, definito da Oracle. La piattaforma Java EE è costituita da una serie di servizi, API (application programming interface) e protocolli che forniscono la funzionalità per lo sviluppo di applicazioni a più livelli basate sul web. (Sun)

### **JavaScript Object Notation (JSON)**

Formato di interscambio di dati leggero, basato sulla notazione object-literal di JavaScript. JSON è indipendente dal linguaggio di programmazione ma utilizza convenzioni di linguaggi che includono C, C++, C#, Java, JavaScript, Perl e Python.

### **Java virtual machine (JVM)**

Implementazione software di un processore che esegue codice Java compilato (applet e applicazioni).

**JNDI** Vedere Java Naming and Directory Interface.

**JSON** Vedere JavaScript Object Notation.

**JVM** Vedere Java virtual machine.

## K

### **keyhole markup language (KML)**

Grammatica XML e formato file per il modeling e l'archiviazione di funzioni geografiche come punti, linee, immagini e poligoni.

### **key performance indicator (KPI)**

Misura quantificabile concepita per tracciare uno dei fattori critici di successo di un processo aziendale.

**KML** Vedere keyhole markup language.

**KPI** Vedere key performance indicator.

### **Modello KPI**

Parte del modello di monitoraggio che contiene i contesti KPI, che a loro volta contengono i KPI e i relativi eventi e trigger.

### **politica KPI**

Politica che determina se un evento in entrata è un aggiornamento di evento KPI, e quindi lo invia per l'elaborazione per generare un aggiornamento KPI o un avviso a seconda dei parametri.

## **L**

### **latitudine**

La distanza angolare di un luogo a nord o a sud dell'equatore, di solito espressa in gradi e minuti.

**livello** Sovrapposizione che può essere posizionata sulla mappa per fornire ulteriori informazioni geospaziali.

**LDAP** Vedere Lightweight Directory Access Protocol.

### **LDAP Directory Interchange Format (LDIF)**

Formato file utilizzato per descrivere le informazioni delle directory e le modifiche che devono essere applicate a una directory, come ad esempio le informazioni della directory che possono essere scambiate tra server delle directory che utilizzano LDAP.

**LDIF** Vedere LDAP Directory Interchange Format.

### **LOS (level of service)**

Una misura qualitativa utilizzata nell'industria dei trasporti dagli ingegneri del traffico per determinare l'efficacia degli elementi di una infrastruttura dei trasporti. Questa misura descrive le condizioni operative del traffico così come definito nella pubblicazione Highway Capacity Manual.

### **LDAP (Lightweight Directory Access Protocol)**

Protocollo aperto che utilizza TCP/IP per fornire accesso a directory che supportano un modello X.500 e che non richiedono i requisiti più complessi di X.500 DAP (Directory Access Protocol). Ad esempio, LDAP può essere utilizzato per individuare persone, organizzazioni e altre risorse in una directory di Internet o intranet.

### **riferimento lineare**

Un indicatore di posizione di riferimento lungo una carreggiata, generalmente sul bordo strada, che indica la propria posizione lungo un percorso. Un esempio di indicatore è una pietra miliare.

### **mappa ubicazione**

Mappa o piano contenente le aree interattive definite in IBM Intelligent Operations Center. Gli eventi possono essere associati a una o più di queste aree. Ad esempio, un diagramma di aree dei posti a sedere in uno stadio in cui si pratica uno sport importante può essere definito in modo che gli eventi che vi si sono verificati possono essere associati all'area appropriata.

### **zona logica**

Un raggruppamento logico di asset o eventi in un'area geografica.

### **longitudine**

La distanza angolare di un luogo a est o a ovest del meridiano di Greenwich, Inghilterra, di solito espressa in gradi e minuti.

**LOS** Consultare livello di servizio.

## M

### **istanza del contesto di monitoraggio**

Le informazioni in IBM WebSphere Business Monitor raccolte in un punto specifico nel tempo all'interno di un contesto di monitoraggio.

### **modello monitor**

Modello che descrive gli aspetti di gestione delle prestazioni di un modello di business, inclusi eventi, metrica di business, e KPI (Key Performance Indicator) richiesti per il monitoraggio di business in tempo reale.

## N

### **KPI nidificato**

KPI definito come elemento secondario di un KPI principale.

## O

### **ontologia**

Specifica formale esplicita della rappresentazione di oggetti, concetti e altre entità presenti in determinate aree di interesse con le relative relazioni.

### **vista Operazioni**

Pagina web che contiene portlet che possono cooperare per facilitare la fornitura delle informazioni e l'interazione globale a livello di operazioni, per il monitoraggio eventi correnti e la pianificazione di eventi futuri.

**OWL** Vedere web ontology language.

## P

### **pagina**

Nell'ambiente del portale, l'elemento dell'interfaccia che contiene uno o più portlet.

### **personalizzare**

Processo che consente alle informazioni di essere destinate a specifici utenti in base a regole di business e alle informazioni del profilo utente. Vedere anche personalizzazione.

### **plug-in**

Modulo software installabile separatamente che aggiunge funzioni a un programma, un'applicazione o un'interfaccia esistenti.

**PMR** Vedere problem management record.

### **poligono**

Nella funzione GDDM, una sequenza di linee rette contigue che contengono un'area.

### **portale**

Singolo punto di accesso, personalizzabile e sicuro, a informazioni, applicazioni e utenti.

### **portlet**

Componente riutilizzabile che fa parte di un'applicazione Web che fornisce informazioni o servizi specifici da presentare nel contesto del portale.

### **problem management record (PMR)**

Il numero nel meccanismo di supporto IBM che rappresenta un incidente di servizio con un cliente.

## R

**RDF** Vedere Resource Description Framework.



**RSS (Really Simple Syndication)**

Formato di file XML per i contenuti Web di tipo syndicated basato sulla specifica RSS (Really Simple Syndication) 2.0. I formati di file XML RSS vengono utilizzati dagli utenti di Internet per la sottoscrizione ai siti web che forniscono feed RSS.

**Representational State Transfer (REST)**

Stile di architettura software per sistemi ipermediali distribuiti come il World Wide Web. Il termine viene spesso utilizzato anche per descrivere qualsiasi interfaccia semplice che utilizzi XML (o YAML, JSON, testo semplice) su HTTP senza un ulteriore livello di messaggistica, come SOAP.

**bundle di risorse**

1. Classe contenente il testo per le pagine di archivio. La creazione e l'accesso ai file del bundle avviene secondo l'API Java PropertyResourceBundle.
2. Una raccolta strutturata di dati che fornisce un'associazione chiave-valore per i dati (risorse) utilizzati nell'individuazione di un programma. I valori sono comunemente stringhe, ma possono essere essi stessi dati strutturati.

**Resource Description Framework (RDF)**

Framework per rappresentare le informazioni sul web.

**REST** Vedere Representational State Transfer.

**RSS** Vedere Really Simple Syndication.

**S****Secure Sockets Layer (SSL)**

Protocollo di sicurezza che fornisce privacy nelle comunicazioni. Con SSL, le applicazioni client/server possono comunicare in una modalità concepita per evitare intercettazioni, manomissione di dati e falsificazione di messaggi.

**SGML**

Vedere Standard Generalized Markup Language.

**File shape**

Un formato di file digitale per software GIS (geographic information system).

**single sign-on (SSO)**

Processo di autenticazione in cui un utente può accedere a più di un sistema o applicazione inserendo un singolo ID utente e una password.

**skin** Elemento di una GUI (Graphical User Interface) che può essere modificato per cambiare la visualizzazione dell'interfaccia senza comprometterne le funzionalità.

**SOAP** Protocollo leggero basato su XML per lo scambio di informazioni in un ambiente distribuito decentralizzato. SOAP può essere utilizzato per eseguire query, restituire informazioni e richiamare servizi in Internet. Vedere anche servizio Web.

**soluzione**

Una combinazione di prodotti che affronta un particolare problema o progetto del cliente.

**SPARQL**

Linguaggio di query per RDF che viene utilizzato per esprimere query attraverso origini dati diverse. La specifica W3 definisce la sintassi e la semantica del linguaggio di query SPARQL.

**SSL** Vedere Secure Sockets Layer.

**SSO** Vedere single sign-on.

**Standard Generalized Markup Language (SGML)**

Metalinguaggio standard per la definizione dei linguaggi di markup basato sullo standard ISO

8879. SGML si basa sulla struttura delle informazioni invece che sulla loro presentazione; esso separa la struttura e il contenuto dalla presentazione. Inoltre facilita lo scambio di documenti su un supporto elettronico.

### **SOP (Standard Operating Procedure)**

Procedura che definisce una sequenza di attività che vengono attivate in risposta a un evento i cui parametri soddisfano determinate condizioni predefinite.

### **Matrice di selezione SOP (Standard Operating Procedure)**

Una matrice contenente serie univoche di parametri di eventi che determinano se una SOP (Standard Operating Procedure) viene avviata per un particolare evento.

### **tabella delle proprietà del sistema**

Tabella che memorizza i dati di configurazione dell'intero sistema per IBM Intelligent Operations Center.

## **T**

**TAI** Vedere trust association interceptor.

### **TCP/IP**

Vedere Transmission Control Protocol/Internet Protocol.

**tema** Elemento di stile che fornisce a un luogo un aspetto particolare. Il portale fornisce alcuni temi, simili a wallpaper virtuali, che possono essere scelti durante la creazione di un luogo.

### **TCP/IP (Transmission Control Protocol/Internet Protocol)**

Serie di protocolli di comunicazione non proprietari, standard di settore, che forniscono connessioni end-to-end affidabili tra reti interconnesse di diverso tipo.

### **trigger**

Meccanismo che rileva una ricorrenza e in risposta ne determina l'elaborazione aggiuntiva.

### **trust association interceptor (TAI)**

Il meccanismo con cui viene convalidata l'affidabilità nell'ambiente del prodotto per ogni richiesta ricevuta dal server proxy. Il metodo di convalida viene concordato dal server proxy e dall'interceptor.

## **U**

### **Uniform Resource Identifier (URI)**

1. Indirizzo univoco utilizzato per identificare contenuti sul Web, ad esempio una pagina di testo, un file video o audio, un'immagine fissa o in movimento, o un programma. Il formato URI più comune è costituito dall'indirizzo della pagina web, che è un formato particolare o un sottoinsieme URI chiamato URL (Uniform Resource Locator). Generalmente, un URI descrive come accedere a una risorsa, il computer che contiene la risorsa e il nome della risorsa (nome del file) sul computer.
2. Stringa compatta di caratteri per l'identificazione di una risorsa fisica o astratta.

### **Uniform Resource Locator (URL)**

Indirizzo univoco di una risorsa di informazioni accessibile in una rete come Internet. L'URL include il nome abbreviato del protocollo utilizzato per accedere alla risorsa di informazioni e le informazioni utilizzate dal protocollo per individuare tale risorsa.

**URI** Vedere Uniform Resource Identifier.

**URL** Vedere Uniform Resource Locator.

### **amministratore utente**

Persona che aggiunge nuovi utenti e garantisce la sicurezza fornendo agli utenti l'appartenenza a gruppi di autorizzazioni basate sul ruolo con i permessi appropriati.

**autorizzazione utente**

Autorizzazione concessa a un utente per fornire accesso alla visualizzazione e all'utilizzo delle risorse del portale. Questa autorizzazione viene concessa dall'appartenenza ad un gruppo di ruoli utente.

**profilo utente**

Descrizione di un utente che include informazioni come l'ID e il nome utente, la password, l'autorizzazione di accesso ed altri attributi che si ottengono quando l'utente si collega.

**gruppo ruoli utente**

Gruppo che assegna l'appartenenza per dare a un nuovo utente il livello di accesso appropriato alla soluzione. Ogni nuovo utente viene aggiunto come membro del gruppo ruoli appropriato. Ci sono diversi livelli di autorizzazione associati a ciascun gruppo di ruoli.

**V****Virtual Network Computing (VNC)**

Sistema di condivisione desktop grafico che utilizza il protocollo RFB (remote frame buffer) per controllare da remoto un altro computer. Trasmette gli eventi della tastiera e del mouse da un computer a un altro, comunicando gli aggiornamenti grafici dello schermo di nuovo nell'altra direzione, su una rete.

VNC Vedere Virtual Network Computing.

**W****Web Map Service (WMS)**

Protocollo standard per fornire immagini mappa con riferimento geografico su Internet che vengono generate da un server di mappe utilizzando i dati da un database GIS. La specifica è stata sviluppata e pubblicata per la prima volta da Open Geospatial Consortium nel 1999.

**web ontology language (OWL)**

Linguaggio utilizzato per rappresentare in modo esplicito il significato dei termini dei vocabolari e le rispettive relazioni. OWL è progettato per essere utilizzato quando le informazioni contenute nei documenti devono essere elaborate da applicazioni, diversamente da situazioni in cui il contenuto deve solo essere presentato agli utenti.

**servizio Web**

Applicazione modulare autonoma e autodescrittiva che può essere pubblicata, rilevata e richiamata in rete utilizzando protocolli di rete standard. Normalmente, XML viene utilizzato per contrassegnare i dati, SOAP per trasferire i dati, WSDL per descrivere i servizi disponibili e UDDI per elencare i servizi disponibili. Vedere anche SOAP, Web Service Definition Language.

**Web Service Definition Language (WSDL)**

Specifica basata su XML per la descrizione dei servizi di rete come insieme di endpoint che agiscono sui messaggi contenenti informazioni orientate ai documenti oppure alle procedure. Vedere anche servizio Web.

**widget**

Componente dell'interfaccia utente riutilizzabile come un pulsante, una barra di scorrimento, un'area di controllo o un'area di modifica testo che può ricevere l'immissione dalla tastiera o dal mouse e che può comunicare con un'applicazione o con un altro widget. Vedere anche widget comune.

WMS Vedere Web Map Service.

WO Vedere ordine di lavoro.

**flusso di lavoro**

Serie specifica di azioni appropriate per una serie particolare di circostanze. La soluzione può essere personalizzata per attivare flussi di lavoro appropriati, ad esempio creando una connessione a sistemi di risposta alle emergenze.

**ordine di lavoro (WO - Work Order)**

Record che contiene informazioni sul lavoro che deve essere eseguito.

**WSDL**

Vedere Web Service Definition Language.

**X**

**XML** Vedere Extensible Markup Language.

**schema XML**

Meccanismo per descrivere e vincolare il contenuto di file XML, indicando quali elementi sono consentiti e in che combinazione. Gli schemi XML sono un'alternativa a DTD (Document Type Definition) e possono essere utilizzati per estendere le funzionalità in aree come presentazione, eredità e immissione dati.

---

**Ulteriori informazioni sul prodotto**

Le seguenti ulteriori risorse sono disponibili online.

**WebSphere Portal**

- Pagina di supporto del prodotto WebSphere Portal: [http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere\\_Portal](http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal)
- Libreria di informazioni di WebSphere Portal: <http://www.ibm.com/software/genservers/portal/library/>
- Wiki di WebSphere Portal: <http://www.lotus.com/ldd/portalwiki.nsf>

**WebSphere Application Server**

- Pagina di supporto del prodotto WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/support/>
- Libreria di informazioni di WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/library/index.html>
- Centro informazioni di WebSphere Application Server 7.0.x: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

**Centri informazioni**

- Centro informazioni di Cognos Business Intelligence: <http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp>
- Centro informazioni di DB2: <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp>
- Centro informazioni di IBM ILOG CPLEX Optimization Studio: <http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp>
- Centro informazioni di Lotus Domino: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Centro informazioni di Lotus Notes: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Centro informazioni di Lotus Sametime Standard: <http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp>
- Centro informazioni di Rational Application Developer: [http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex\\_rad.html](http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html)

- Centro informazioni di Tivoli Access Manager: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro informazioni di Tivoli Composite Application Manager: <http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp>
- Centro informazioni di Tivoli Directory Integrator: [http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc\\_7.1/welcome.htm](http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc_7.1/welcome.htm)
- Centro informazioni di Tivoli Directory Server: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro informazioni di Tivoli Identity Manager : <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Centro informazioni di Tivoli Netcool/Impact: <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html>
- Centro informazioni di Tivoli Netcool/OMNIBus: [http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool\\_OMNIBus.doc\\_7.3.1/omnibus/wip/welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm)
- Centro informazioni di Tivoli Service Request Manager: [http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm\\_welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm)
- Centro informazioni di IBM WebSphere Business Monitor: <http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html>
- Centro informazioni di WebSphere Message Broker: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp>
- Centro informazioni di WebSphere MQ: <http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp>
- Centro informazioni di WebSphere Operational Decision Management: <http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp>

## Redbook

- Dominio Redbooks: <http://www.redbooks.ibm.com/>

## Altre risorse web

- Formazione e certificazione Tivoli: <http://www.ibm.com/software/tivoli/education/>
- OASIS CAP (Common Alerting Protocol) Versione 1.2 <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- Sito web di Red Hat: <http://www.redhat.com/>

### Concetti correlati:

“Destinatari previsti” a pagina 1

Questo centro informazioni è rivolto alle persone che utilizzano, installano, gestiscono e amministrano IBM Intelligent Operations Center. Contiene inoltre la documentazione di implementazione per personalizzare la soluzione e integrare i sistemi esterni sottostanti richiesti da IBM Intelligent Operations Center.

---

## Avviso sul copyright e marchi

### Avviso sul copyright

© Copyright IBM Corporation 2011, 2012. Tutti i diritti riservati. Può essere utilizzato unicamente a seguito di un accordo di licenza software IBM. Nessuna parte di questa pubblicazione può essere riprodotta, trasmessa, trascritta, memorizzata in un sistema di recupero o tradotta in qualsiasi linguaggio di computer, in qualsiasi formato o con qualunque mezzo (elettronico, meccanico, magnetico, ottico, chimico, manuale o altro), senza un consenso scritto di IBM Corporation. IBM Corporation concede un'autorizzazione limitata a effettuare copie cartacee o altre riproduzioni di qualsiasi documentazione leggibile da macchina per utilizzo proprio, a patto che ogni riproduzione riporti l'avviso di copyright di

IBM Corporation. Nessuna altro diritto con copyright viene concesso senza previa autorizzazione scritta di IBM Corporation. Il documento non è inteso per la produzione e viene fornito “nello stato in cui si trova” senza garanzie di alcun tipo. **Tutte le garanzie di questo documento vengono pertanto negate, inclusa la garanzia di non violazione e incluse le garanzie implicite di commerciabilità e idoneità per uno scopo particolare.**

Limitazioni previste per gli utenti del Governo degli Stati Uniti – L'utilizzo, la duplicazione o la divulgazione sono limitati dal GSA ADP Schedule Contract con IBM Corporation.

---

## Marchi

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities e Redbooks sono marchi di IBM Corporation negli Stati Uniti e/o negli altri paesi.

Microsoft, Internet Explorer, Windows e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Pentium è un marchio registrato di Intel Corporation o consociate negli Stati Uniti e in altri paesi

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Adobe, Acrobat, Portable Document Format (PDF) e PostScript sono marchi registrati o marchi di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Oracle, Javascript e Java sono marchi registrati di Oracle e/o consociate.

ArcGIS, EDN, StreetMap, @esri.com e www.esri.com sono marchi, marchi registrati o marchi di servizio di Esri negli Stati Uniti, nella Comunità Europea o in altre determinate giurisdizioni.

Altri nomi possono essere marchi dei rispettivi proprietari. Altri nomi di società, prodotti e servizi possono essere marchi o marchi di servizio di altri.

---

## Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

È possibile che IBM non offra in altri paesi i prodotti, i servizi o le funzioni illustrati in questa documentazione. Consultare il rappresentante IBM locale per informazioni sui prodotti e sui servizi disponibili nel proprio paese. Qualunque riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti dall'IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino la violazione dei diritti di proprietà intellettuale o di altri diritti di IBM. È tuttavia responsabilità dell'utente valutare e verificare il funzionamento di eventuali prodotti, programmi o servizi non IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente documentazione. La fornitura del presente documento non implica la concessione di alcuna licenza su tali brevetti. Chi desiderasse ricevere informazioni relative alle licenze può rivolgersi per iscritto a:

Director of Commercial Relations  
IBM Europe  
Schoenaicher Str. 220  
71032 Boeblingen  
Deutschland

Per domande su licenze relative a informazioni double-byte (DBCS), rivolgersi al dipartimento della proprietà intellettuale IBM del proprio paese oppure inviare le domande a:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

Il seguente paragrafo non è valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute: L'INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE NELLO STATO IN CUI SI TROVA SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIALIZZABILITÀ ED IDONEITÀ AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, pertanto la presente dichiarazione potrebbe non essere sempre applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche verranno incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non IBM contenuti in questo documento sono forniti solo per consultazione e non servono in alcun modo da approvazione di tali siti Web. I materiali presenti in tali siti Web non sono parte dei materiali di questo prodotto IBM e il loro utilizzo è a rischio dell'utente.

IBM può utilizzare o divulgare le informazioni ricevute dagli utenti secondo le modalità ritenute appropriate, senza alcun obbligo nei loro confronti.



Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, devono contattare:

IBM Corporation  
Department T81B F6/Building 503  
4205 S. Miami Boulevard  
Durham NC 27709-9990  
U.S.A.

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un corrispettivo.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti da IBM nel rispetto dei termini dell'IBM Customer Agreement, IBM International Program License Agreement o di ogni altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questa pubblicazione sono stati determinati in ambiente controllato. Pertanto, i risultati ottenuti in ambienti operativi diversi possono variare in modo significativo. È possibile che alcune misurazioni siano state effettuate su sistemi a livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni potrebbero essere state stimate tramite estrapolazione. I risultati effettivi possono quindi variare. Gli utenti di questa documentazione devono verificare i dati applicabili per i propri ambienti specifici.

Le informazioni relative a prodotti non IBM sono state ottenute dai fornitori di tali prodotti, dagli annunci pubblicati e da altre fonti disponibili pubblicamente. IBM non ha verificato tali prodotti e non può garantirne l'accuratezza delle prestazioni, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Eventuali domande relative alle funzioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Queste informazioni contengono esempi di dati e di report utilizzati quotidianamente nelle operazioni aziendali. Per meglio illustrarli, tali esempi contengono nomi di persone, società, marchi e prodotti. Tutti questi nomi sono fittizi e ogni riferimento a nomi ed indirizzi reali è puramente casuale.

#### LICENZA SOGGETTA ALLE LEGGI SUL DIRITTO D'AUTORE:

Queste informazioni contengono esempi di programmi applicativi in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi esempi di programmi sotto qualsiasi forma senza alcun pagamento a IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (Application Programming Interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi. I programmi di esempio vengono forniti "NELLO STATO IN CUI SI TROVANO" e senza alcun tipo di garanzia. IBM declina ogni responsabilità per eventuali danni derivanti dall'uso degli stessi.

---

## Marchi

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities e Redbooks sono marchi di IBM Corporation negli Stati Uniti e/o negli altri paesi.

Microsoft, Internet Explorer, Windows e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Pentium è un marchio registrato di Intel Corporation o consociate negli Stati Uniti e in altri paesi

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Adobe, Acrobat, Portable Document Format (PDF) e PostScript sono marchi registrati o marchi di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Oracle, Javascript e Java sono marchi registrati di Oracle e/o consociate.

ArcGIS, EDN, StreetMap, @esri.com e www.esri.com sono marchi, marchi registrati o marchi di servizio di Esri negli Stati Uniti, nella Comunità Europea o in altre determinate giurisdizioni.

Altri nomi possono essere marchi dei rispettivi proprietari. Altri nomi di società, prodotti e servizi possono essere marchi o marchi di servizio di altri.



---

## Indice analitico

### A

avvisi 357

### G

glossario 346

### M

marchi 357

### N

nuove funzioni  
panoramica 8



---

## Riservato ai commenti del lettore

IBM Intelligent Operations Center  
IBM Intelligent Operations Center  
Documentazione del prodotto  
Versione 1 Release 5

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla. Sono graditi commenti pertinenti alle informazioni contenute in questo manuale ed al modo in cui esse sono presentate. Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo.

Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni e/o per richiedere informazioni di carattere generale.

Per tali esigenze si consiglia di rivolgersi al punto di vendita autorizzato o alla filiale IBM della propria zona oppure di chiamare il "Supporto Clienti" IBM al numero verde 800-017001.

I suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Sistemi Informativi e diventeranno proprietà esclusiva delle stesse.

Commenti:

Si ringrazia per la collaborazione.

Per inviare i commenti è possibile utilizzare uno dei seguenti modi.

- Spedire questo modulo all'indirizzo indicato sul retro.
- Inviare un fax al numero: 1-800-227-5088 (US e Canada)

Se è gradita una risposta dalla Sistemi Informativi, si prega di fornire le informazioni che seguono:

Nome

Indirizzo

Società

Numero di telefono

Indirizzo e-mail

Indicandoci i Suoi dati, Lei avrà l'opportunità di ottenere dal responsabile del Servizio di Translation Assurance della Sistemi Informativi S.p.A. le risposte ai quesiti o alle richieste di informazioni che vorrà sottoporci. I Suoi dati saranno trattati nel rispetto di quanto stabilito dalla legge 31 dicembre 1996, n.675 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali". I Suoi dati non saranno oggetto di comunicazione o di diffusione a terzi; essi saranno utilizzati "una tantum" e saranno conservati per il tempo strettamente necessario al loro utilizzo.

IBM  
Information Development Dipartimento DLUA  
P.O. Casella 12195  
Research Triangle Park, NC  
USA







Stampato in Italia