

CA Identity Manager™

Guida per l'amministratore

12.6.5



La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da CA in qualsiasi momento. Questa Documentazione è di proprietà di CA non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata, per intero o in parte, senza la preventiva autorizzazione scritta di CA.

Fermo restando quanto enunciato sopra, se l'utente dispone di una licenza per l'utilizzo dei software a cui fa riferimento la Documentazione avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di CA.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a CA per iscritto che tutte le copie anche parziali del prodotto sono state restituite a CA o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, LA DOCUMENTAZIONE VIENE FORNITA "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO CA SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLIFICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DEL GOODWILL O DI DATI, ANCHE NEL CASO IN CUI CA VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è CA.

Questa Documentazione è fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

Copyright © 2015 CA. Tutti i diritti riservati. Tutti i marchi, i nomi commerciali, i marchi di servizio e i loghi citati nel presente documento sono di proprietà delle rispettive società.

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA CloudMinder™ Identity Management
- Directory CA
- CA Identity Manager™
- CA Identity Governance (precedentemente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo <http://www.ca.com/worldwide>.

Sommario

Capitolo 1: Pianificazione dei ruoli 17

Ruoli per la gestione di identità o accessi	18
Caratteristiche dei ruoli	18
Profilo di ruolo	19
Attività relative al ruolo	19
Modelli di account	19
Regole per membri, amministratori e titolari	20
Regole di ambito	21
Valutazione degli operatori	24
Mancanza di distinzione tra maiuscole e minuscole nelle regole	24
Azioni di aggiunta e rimozione	25
Criteri membri	26
Criteri di amministrazione	26
Elenco di controllo di pianificazione del ruolo	27

Capitolo 2: Ruoli di amministrazione 29

Ruoli di amministrazione e attività di amministrazione	29
Ruoli di amministrazione e ambienti Identity Manager	29
Ruoli di amministrazione e console utente	30
Creazione di un ruolo di amministrazione	30
Procedura preliminare di creazione del ruolo di amministrazione	31
Definizione del profilo del ruolo di amministrazione	31
Selezione delle attività di amministrazione per il ruolo	32
Definizione dei criteri membri per un ruolo di amministrazione	33
Definizione dei criteri di amministrazione per il ruolo di amministrazione	34
Definizione delle regole proprietari per un ruolo di amministrazione	35
Verifica di un ruolo di amministrazione	35
Assegnazione dei ruoli a se stessi	35

Capitolo 3: Attività di amministrazione 37

Pianificazione delle attività di amministrazione	37
Esempio di attività di amministrazione	39
Opzioni di utilizzo delle attività di amministrazione	41
Attività di amministrazione predefinite	42
Procedura di creazione di un'attività di amministrazione personalizzata	43
Definizione del profilo dell'attività	44

Scheda Profilo attività di amministrazione	45
Proprietà di configurazione dell'attività.....	48
Definizione dell'ambito dell'attività	49
configurazione dello schermo di ricerca	50
Selezione delle schede per l'attività	60
Schede Account.....	61
Scheda Pianificazione.....	63
Visualizzazione di campi nell'attività	64
Visualizzazione utilizzo ruolo.....	64
Assegnazione di processi del flusso di lavoro per gli eventi.....	64
Gestione di un archivio utenti di Active Directory	65
Attributo sAMAccountName.....	65
Tipo di gruppo e ambito.....	65
Attività esterne per le funzioni dell'applicazione	67
Scheda esterna.....	67
Scheda URL esterno	68
Componenti di attività avanzati	69
Creazione di gestori delle attività di logica aziendale	69
Eventi ed attività di amministrazione.....	71
Eventi primari e secondari	71
Visualizzazione degli eventi di un'attività	72
Eventi generati per i profili non modificati	72
Elaborazione dell'attività di amministrazione	73
Elaborazione della fase sincrona.....	74
Elaborazione della fase asincrona.....	75
Immagini per Attività di amministratore.....	77

Capitolo 4: Amministratori e utenti 79

Creazione di amministratori	79
Ruoli per la gestione di identità o accessi	80
Amministrazione delegata	80
Designazione di un amministratore di ruolo	81
Procedura di delega	82
Esempio di delega	83
Creazione di utenti	83
Creazione di un profilo utente	85
Assegnazione di un gruppo a un utente.....	86
Assegnazione di un ruolo a un utente.....	86
Assegnazione diretta di un servizio a un utente	87
Procedura per consentire agli utenti la registrazione automatica	88
Attività self-service.....	90

Accesso alle attività di self-service	91
Integrazione di un collegamento self-service nel sito Web aziendale	91
Configurazione di più attività di self-service	93
Limitazione dell'accesso al ruolo Gestione automatica	95

Capitolo 5: Gestione delle password 97

Gestione delle password in Identity Manager	97
Panoramica dei criteri di password	98
Creazione di un criterio di password	99
Abilitazione dei criteri di password aggiuntivi	99
Applicazione di un criterio di password ad un gruppo di utenti	100
Configurazione della scadenza della password	102
Configurazione della composizione della password	105
Specifica di espressioni regolari	107
Impostazione delle restrizioni di password	109
Configurazione delle opzioni avanzate di password	113
Gestione criteri di password	114
Criteri di password e database relazionali	114
CA Identity Manager e l'integrazione con i criteri di password di SiteMinder	114
Reimpostazione della password o sblocco dell'account	115
Installazione del Provider di credenziali	115
Configurazione del Provider di credenziali	115
Impostazioni del registro di sistema per il Provider di credenziali	117
Impostazioni di registro del browser Cube	119
Personalizzazione del messaggio Powered by	121
Ripristino di una password per un accesso Windows	121
Installazione invisibile all'utente del provider di credenziali	122
Password di sincronizzazione sugli endpoint	124
Sincronizzazione password su Windows	124
Sincronizzazione password su UNIX e Linux	133
Sincronizzazione password su OS400	148

Capitolo 6: Gruppi 155

Creazione di un gruppo statico	155
Creazione di un gruppo dinamico	156
Parametri di Query gruppo dinamico	157
Creazione di un gruppo nidificato	159
Esempio di gruppi statici, dinamici e nidificati	161
Amministratori gruppo	162

Capitolo 7: Account endpoint gestiti

165

Integrazione di endpoint gestiti	166
Importazione del file di definizione dei ruoli	167
Creazione di regole di correlazione.....	167
Aggiunta dell'endpoint all'ambiente	170
Creazione di una definizione di esplorazione e correlazione	170
Esplorazione e correlazione dell'endpoint	172
Sincronizzazione di utenti, account e ruoli.....	173
Sincronizzazione utente con ruoli	175
Sincronizzazione utente con modelli account.....	175
Sincronizzazione account endpoint con modelli di account	177
Sincronizzazione inversa con gli account endpoint.....	180
Funzionamento della sincronizzazione inversa	181
Mapping degli attributi endpoint.....	182
Criteri per la sincronizzazione inversa.....	184
Creazione di un'attività di approvazione per la sincronizzazione inversa	188
Esecuzione della sincronizzazione inversa	190
Estensione degli attributi personalizzati agli endpoint	191
Attività degli account	193
Visualizzazione o modifica di account di endpoint	193
Creazione di un account fornito.....	194
Creazione di un account di eccezione	195
Assegnazione di account orfani	195
Assegnazione di account di sistema	196
Schermata attività Sposta account	196
Eliminazione di un account di un endpoint.....	197
Modifica della password di un account di un endpoint	197
Esecuzione di azioni su più account	198
Operazioni di account avanzate	198
Modificare l'utente globale per un account.....	199
Funzionamento dell'esplorazione automatica	199
Eliminare gli account	200
Utilizzare l'opzione In attesa di eliminazione	201
Ricreare gli account eliminati.....	201

Capitolo 8: Ruoli di fornitura

203

Ruoli di fornitura e modelli di account.....	203
Creazione di ruoli per assegnare account	204
Creazione di un modello di account.....	206
Creazione di un ruolo di provisioning	207
Attività relative a ruoli e modelli.....	208

Importazione di un ruolo di provisioning	208
Assegnazione di nuovi titolari ai ruoli di provisioning.....	209
Password per gli account creati dai ruoli di provisioning.....	209
Ordine di elaborazione degli eventi dei ruoli di provisioning	210
Abilitazione di ruoli nidificati in un ambiente	212
Inclusione di un ruolo in un ruolo di provisioning.....	212
Attributi nei modelli di account	212
Attributi di compatibilità e attributi iniziali.....	213
Stringhe di regola nei modelli di account.....	214
Valori per gli attributi.....	216
Espressioni delle regole avanzate	216
Combinazione di stringhe e valori delle regole	217
Sottostringhe delle regole.....	217
Espressioni delle regole con più valori.....	218
Regole esplicite dell'Attributo utente globale	220
Funzioni delle regole incorporate	221
Prestazioni dei ruoli di provisioning	223
Cache oggetto JIAM	223
Pooling di sessione	224
Attività di fornitura per ambienti esistenti	225

Capitolo 9: Servizi gestiti (richieste di accesso di base) 227

Creazione di un servizio.....	228
Introduzione alla creazione dei servizi	230
Fasi iniziali nella creazione del servizio	231
Definizione del profilo del servizio	231
Definizione dei criteri di amministrazione per il servizio	233
Definizione delle regole di titolarità per il servizio	234
Definizione dei prerequisiti per il servizio	234
Configurazione delle notifiche di posta elettronica per il rinnovo del servizio.....	235
Comprensione delle azioni di esecuzione e revoca.....	236
Definizione delle azioni di esecuzione e revoca per il servizio.....	236
Assegnazione diretta di un servizio a un utente	238
Conferma dell'assegnazione del servizio	239
Procedura per rendere i servizi disponibili agli utenti	239
Assegnazione diretta di un servizio a un utente	241
Conferma dell'assegnazione del servizio	242
Modifica di un servizio	242
Aggiunta di una ricerca all'accesso e visualizzazione dell'accesso	244
Eliminazione di un servizio	245
Verifica e rimozione dei membri di un servizio	246

Eliminazione di un servizio	246
Rinnovo dell'accesso a un servizio	247

Capitolo 10: Sincronizzazione 249

Sincronizzazione utente tra server	249
Sincronizzazione in entrata	249
Failover della sincronizzazione in entrata	249
Sincronizzazione in uscita	249
Abilitare la sincronizzazione di password	251
Sincronizzare gli utenti nelle attività di creazione o modifica utente	252
Attività di sincronizzazione	253
Perché gli utenti perdono la sincronizzazione	255
Sincronizzazione utente	255
Sincronizzazione dei modelli di account	258
Sincronizzazione account	262

Capitolo 11: Flusso di lavoro 263

Panoramica del flusso di lavoro	263
Diagramma del processo di WorkPoint	264
Flusso di lavoro e notifiche via posta elettronica	264
Documentazione di WorkPoint	265
Metodi per il controllo del flusso di lavoro	265
Utilizza il controllo del flusso di lavoro - metodo basato su modelli	266
Prerequisito: Attiva flusso di lavoro	267
Colloca le attività di amministrazione sotto il controllo del flusso di lavoro - metodo basato su modelli	268
Flusso di lavoro basato sull'evento o sull'attività	269
Tipi di modelli di processi	275
Tipi di resolver partecipanti	279
Impostazione di un criterio di posta elettronica per un processo del flusso di lavoro	284
Esempio di flusso di lavoro: creazione di utenti	284
Utilizzo del metodo WorkPoint	286
Configurazione degli strumenti di amministrazione di WorkPoint	288
Processi WorkPoint	293
Attività del flusso di lavoro	298
Resolver partecipanti: metodo WorkPoint	300
Processi in WorkPoint Designer	311
Processi ed istanze di processi	314
Esecuzione delle attività del flusso di lavoro	316
Completamento dell'attività da parte del server del flusso di lavoro	317
Visualizzazione di processi Workpoint	318
Aggiunta della scheda Visualizza processo alle schede di approvazione esistenti	319

Flusso di lavoro basato su criterio.....	319
Oggetti delle regole.....	321
Valutazione regola	322
Ordine criterio	324
Descrizione criterio	326
Criteri di approvazione e attributi multivalore	327
Attributi evidenziati come modificati nelle schermate di approvazione del flusso di lavoro	328
Esempi di criteri	328
Configurazione di un flusso di lavoro basato su criterio per gli eventi	331
Configurazione di un flusso di lavoro basato su criterio per le attività.....	333
Modalità di configurazione di un criterio di approvazione	334
Stato del flusso di lavoro di basato su criterio	335
Mapping globale di eventi a processi del flusso di lavoro basato su criterio.....	336
Richieste in linea	338
Attività associate alle richieste in linea	338
Processo della richiesta in linea	340
Cronologia delle richieste in linea.....	341
Utilizzo delle richieste in linea.....	341
Comandi operazione del flusso di lavoro	342
Pulsanti del flusso di lavoro nelle attività di approvazione.....	343
Configurazione dei pulsanti in CA Identity Manager	343
Aggiunta di comandi operazione del flusso di lavoro	344
Elenchi ed elementi di lavoro.....	347
Visualizzazione di un elenco lavori.....	348
Attivazione della schermata di ricerca Elenco di lavoro	349
Riserva di elementi di lavoro.....	349
Delega di elementi di lavoro	351
Riassegnazione degli elementi di lavoro	356
Operazioni in blocco su elementi di lavoro	359

Capitolo 12: Notifiche di posta elettronica 361

Notifiche di posta elettronica in CA Identity Manager.....	362
Selezione di un metodo di notifica di posta elettronica.....	363
Configurazione delle impostazioni SMTP	364
Configurazione delle impostazioni SMTP su JBoss.....	365
Configurazione delle impostazioni SMTP su WebLogic.....	366
Configurazione delle impostazioni SMTP su WebSphere	366
Configurazione di un indirizzo di posta elettronica di amministrazione univoco per ciascun ambiente.....	367
Creazione di criteri della notifica di posta elettronica	368
Scheda Profilo delle notifiche di posta elettronica	369
Scheda Invia messaggi con stato.....	370

Scheda Destinatari	372
Contenuto	374
Modifica di criteri della notifica di posta elettronica	376
Disattivazione di criteri della notifica di posta elettronica	376
Use Case: invio di un messaggio di posta elettronica di benvenuto	377
Utilizzo dei modelli di messaggio di posta elettronica	378
Abilitazione delle notifiche di posta elettronica	379
Configurare un messaggio di posta elettronica per un evento o attività da inviare	379
Contenuto dei messaggi di posta elettronica	381
Modelli di messaggio di posta elettronica	382
Creazione di modelli di messaggio di posta elettronica	385
Modelli di messaggio di posta elettronica personalizzati	385
Distribuzione del modello di messaggio di posta elettronica	405

Capitolo 13: Rapporti 409

Panoramica di configurazione	409
Processo dei rapporti	411
Esecuzione di rapporti di snapshot	412
Configurazione della connessione del server di rapporto	415
Creazione di una connessione al database snapshot	416
Creazione di una definizione di snapshot	417
Esempio: creare una definizione snapshot per i dati dei diritti dell'utente	419
Gestione delle istantanee	420
Acquisizione dei dati di snapshot	420
Associazione di una definizione snapshot a un'attività rapporto	422
Sincronizzazione account endpoint con modelli di account	423
Esempio di attività di amministrazione	424
Richiesta di un rapporto	426
Visualizzazione del rapporto	428
Esecuzione di rapporti non di snapshot	429
Configurazione della connessione del server di rapporto	430
Creazione di una connessione per il rapporto	431
Associazione di una connessione a un'attività di rapporto	431
Richiesta di un rapporto	432
Visualizzazione del rapporto	434
Imposta opzioni di segnalazione	435
Creazione ed esecuzione di un rapporto di snapshot personalizzato	436
Creazione di un rapporto in Crystal Reports	438
Creazione del file XML del parametro di rapporto	438
Caricamento del rapporto e del file XML del parametro di rapporto	442
Creazione dell'attività di rapporto	444

Richiesta di un rapporto.....	447
Visualizzazione del rapporto	449
Sincronizzazione di utenti, account e ruoli.....	450
Sincronizzazione utente con ruoli	452
Sincronizzazione utente con modelli account.....	452
Sincronizzazione account endpoint con modelli di account	453
Risoluzione dei problemi	457
La visualizzazione di un rapporto ridirige alla pagina di accesso di Infoview	457
Generazione di account utente per oltre 20.000 record	458

Capitolo 14: Criteri di identità **459**

Criteri di identità	459
Pianificazione del set di criteri di identità	460
Creazione di un set di criteri di identità	461
Gestione di un set di criteri di identità.....	472
Modalità di sincronizzazione di utenti e criteri di identità	472
Set di criteri di identità in un ambiente Identity Manager.....	477
Criteri di identità preventivi	482
Azioni per le violazioni dei criteri di identità preventivi.....	483
Funzionamento dei criteri di identità preventivi	484
Note importanti sui criteri di identità preventivi	485
Creazione di un criterio di identità preventivo	486
Use Case: Impedire i conflitti di ruoli per gli utenti	487
Flusso di lavoro e criteri di identità preventivi.....	488
Combinazione di criteri di identità e criteri di identità preventivi	492

Capitolo 15: Policy XPress **495**

Panoramica di Policy Xpress	495
Creazione di un criterio	496
Profilo.....	497
Eventi	501
Elementi dati	502
Regole di ingresso	505
Regole azione	506
Avanzate.....	511

Capitolo 16: Applicazione mobile CA Identity Manager **513**

L'architettura dell'applicazione mobile di CA Identity Manager	514
Funzionamento del processo di implementazione	517
Funzionamento della configurazione dell'applicazione	518

Funzionamento della registrazione utenti	519
Configurazione di CA Identity Manager per il supporto dell'applicazione mobile	519
Configurazione degli attributi obbligatori	520
Importazione delle attività di amministrazione	523
Creazione di una configurazione dei servizi Web	525
Modifica del messaggio di posta elettronica di registrazione	527
Configurazione di SiteMinder per il supporto dell'applicazione mobile	528
Configurazione di un'applicazione mobile	529
Configurare delle proprietà aggiuntive	532
Download dell'applicazione mobile	534
Risoluzione dei problemi delle applicazioni mobili	535

Capitolo 17: CA User Activity Reporting **537**

Funzionalità di CA Enterprise Log Manager	537
Componenti di CA Enterprise Log Manager	537
Limiti di integrazione	538
Integrazione di CA Enterprise Log Manager con CA Identity Manager	538
Integrare i rapporti o le query aggiuntive di CA Enterprise Log Manager con CA Identity Manager	548
Configurazione della scheda di visualizzazione Enterprise Log Manager	549

Capitolo 18: Ruoli di accesso **553**

Gestione dei diritti mediante i ruoli di accesso	554
Esempio: Modifica indiretta dell'attributo di profilo	554
Creazione di un ruolo di accesso	555
Inizio della procedura di creazione del ruolo di accesso	555
Definizione del profilo di un ruolo di accesso	555
Definizione dei criteri membri per un ruolo di accesso	556
Definizione dei criteri di amministrazione per un ruolo di accesso	556
Definizione delle regole proprietari per un ruolo di accesso	557

Capitolo 19: Attività di sistema **559**

Attività di sistema predefinite	559
Aggiunta di utenti mediante il file alimentatore	560
Considerazioni sull'Utilità di caricamento in blocco	561
Creazione di un file alimentatore	563
Scheda Dettagli record dell'Utilità di caricamento	565
Scheda Mappatura azioni dell'Utilità di caricamento	565
Scheda Dettagli di notifica dell'utilità di caricamento	566
Conferma delle modifiche all'attività dell'Utilità di caricamento in blocco	567
Configurazione delle notifiche di posta elettronica per le attività in blocco	568

Pianificazione di un'attività dell'Utilità di caricamento in blocco	568
Modifica del file analizzatore per l'Utilità di caricamento in blocco	569
Supporto dei servizi Web per l'Utilità di caricamento in blocco	569
Gestione connessione JDBC	570
Creazione di una connessione JDBC.....	570
Gestori attributi logici	570
Creazione di un gestore attributo logico.....	571
Copia di un gestore attributo logico	572
Creazione di un gestore attributo logico ForgottenPasswordHandler	572
Eliminazione di un gestore attributo logico	573
Modifica di un gestore attributo logico	573
Visualizzazione di un gestore attributo logico	573
Dati casella di selezione	574
Schermata di attività Configura attributi di correlazione.....	574
Schermata attività Configurare il flusso di lavoro basato sul criterio globale per Eventi	575
Stato delle attività in CA Identity Manager	576
Determinazione dello stato delle attività con CA Identity Manager.....	577
Visualizzazione delle attività inoltrate	578
Scheda Cronologia utente.....	588
Pulitura delle attività inoltrate	593
Scheda Ricorrenza.....	594
Scheda Attività di pulizia inoltrate.....	597
Eliminazione di attività ricorrenti	598
Configurazione della connessione Enterprise Log Manager	599
Eliminazione della connessione Enterprise Log Manager	600
Gestione delle chiavi segrete	600

Capitolo 20: Persistenza delle attività 601

Pulitura ed archiviazione automatizzata della persistenza delle attività	601
Scheda Ricorrenza	602
Scheda Attività di pulizia inoltrate	603
Esecuzione immediata di un processo	604
Pianificazione di un nuovo processo	604
Modifica di un processo esistente.....	605
Eliminazione di un'attività ricorrente.....	605
Migrazione del database di persistenza delle attività.....	606
Aggiornare il file tpmigration125.properties	607
Impostazione della variabile JAVA_HOME	607
Esecuzione dello strumento runmigration.....	608

Capitolo 1: Pianificazione dei ruoli

Per pianificare i vari ruoli, occorre stabilire quali ruoli sono necessari per la propria azienda o organizzazione e come saranno delegati la gestione degli utenti e il loro accesso alle applicazioni. In base a queste decisioni, si determinano le caratteristiche di ciascun ruolo.

Per utilizzare i ruoli in modo efficace, prendere in considerazione le seguenti domande sulle esigenze degli utenti e le responsabilità degli amministratori:

- Quali dipartimenti e organizzazioni dispongono di utenti da gestire?
- Di quali account aggiuntivi negli endpoint gestiti gli utenti avranno bisogno?
- Quali utenti dovrebbero essere amministratori di altri utenti?
- Chi dovrebbe gestire gli amministratori?
- Quali attività di amministrazione e di accesso sono necessarie in ciascun ruolo?
- Chi dovrebbe creare ruoli e attività?
- Come è possibile utilizzare i ruoli per delegare il lavoro?

L'ultima domanda riguarda la condivisione delle attività di gestione degli utenti e di concessione dell'accesso alle applicazioni. Ulteriori informazioni sul modello di delega sono disponibili in Amministrazione delegata.

In base alle risposte a queste domande, è possibile decidere quanti e quali tipi di ruoli sono necessari.

Questa sezione contiene i seguenti argomenti:

[Ruoli per la gestione di identità o accessi](#) (a pagina 18)

[Caratteristiche dei ruoli](#) (a pagina 18)

[Profilo di ruolo](#) (a pagina 19)

[Attività relative al ruolo](#) (a pagina 19)

[Modelli di account](#) (a pagina 19)

[Regole per membri, amministratori e titolari](#) (a pagina 20)

[Elenco di controllo di pianificazione del ruolo](#) (a pagina 27)

Ruoli per la gestione di identità o accessi

Per abilitare la gestione delle identità degli utenti e il loro accesso ad altri account, CA CloudMinder fornisce due tipi di ruoli:

Tipo di ruolo	Scopo
Ruolo di amministrazione	Contiene le attività di amministrazione eseguite dall'utente a cui è stato concesso questo ruolo in CA CloudMinder, ad esempio le attività di modifica della password utente o dell'appartenenza a un gruppo. I ruoli di amministrazione possono comprendere, tra le altre, qualsiasi attività visualizzata nella console utente.
Ruolo di provisioning	Contiene modelli di account che definiscono gli account presenti negli endpoint gestiti, come un sistema di posta elettronica. I modelli di account definiscono inoltre le modalità di mapping degli attributi utente su questi account.
Ruolo di accesso	I ruoli di accesso rappresentano un ulteriore modo per concedere diritti in CA Identity Manager o in un'altra applicazione. Ad esempio, è possibile utilizzare i ruoli di accesso per completare le seguenti operazioni: ■ Fornire accesso indiretto a un attributo utente. ■ Creare espressioni complesse. ■ Impostare un attributo di profilo che un'altra applicazione può utilizzare per determinare i diritti.

Caratteristiche dei ruoli

Quando si crea un ruolo, si definiscono le caratteristiche illustrate nella tabella seguente:

Caratteristiche	Definizione
Profilo di ruolo	Caratteristiche generali del ruolo.
Attività	Attività per un ruolo di amministrazione.
Modelli di account	Modelli che definiscono account in endpoint gestiti per un ruolo di provisioning.

Caratteristiche	Definizione
Regole membri, Criteri membri	Una regola membri definisce le condizioni affinché un utente sia membro di un ruolo di accesso o di amministrazione. Un criterio membri associa una regola membri con regole di ambito. Nota: i ruoli di provisioning non hanno regole e criteri membri. Per rendere membro un utente, si utilizza l'opzione Modifica membri/amministratori del ruolo di provisioning.
Regole di amministrazione, Criteri di amministrazione	■ Una regola di amministrazione definisce le condizioni affinché un utente sia un amministratore di ruolo. ■ Un criterio di amministrazione associa una regola di amministrazione con una regola di ambito e i privilegi di amministratore per l'assegnazione di un ruolo.
Regole di titolarità	Definisce le condizioni affinché un utente sia titolare di un ruolo.
Regole di ambito	Limiti in base ai quali è possibile gestire gli oggetti dal ruolo.
Aggiungi azioni, Rimuovi azioni	Modifiche a un profilo utente quando un utente viene aggiunto o rimosso come membro del ruolo o amministratore.

Profilo di ruolo

Il profilo di ruolo corrisponde al nome e alla descrizione del ruolo e indica se il ruolo è abilitato. Se abilitato, il ruolo è disponibile per l'uso non appena viene creato.

Attività relative al ruolo

Per un ruolo di amministrazione, è possibile scegliere una o più attività di amministrazione, incluse le attività esterne, da una o più categorie.

Modelli di account

Ciascun ruolo di provisioning contiene dei modelli di account. Questi definiscono gli account presenti negli endpoint gestiti. Ad esempio, un endpoint di un account Exchange potrebbe definire la dimensione della casella di posta elettronica. I modelli di account definiscono anche le modalità di mapping degli attributi utente sugli account.

È possibile scegliere uno o più endpoint per ciascun tipo di endpoint. Un utente a cui viene assegnato il ruolo riceve un account nell'endpoint.

Regole per membri, amministratori e titolari

Ogni ruolo include regole per la definizione dei membri, degli amministratori o dei titolari del ruolo stesso. Di conseguenza, un utente può essere membro di uno o più ruoli, oppure di nessuno.

Le regole per membri, amministratori e titolari utilizzano le condizioni riportate nella tabella seguente:

Condizione regola	Esempio	Sintassi regola
L'utente deve corrispondere a un valore attributo.	Utenti in cui titolo inizia con senior	dove <filtro utente>
L'utente deve corrispondere a più valori attributo.	Utenti dove titolo=responsabile e località=est	dove <filtro utente>
L'utente deve appartenere alle organizzazioni indicate.	Utenti nell'organizzazione Vendite e inferiori	in <regola organizzazione>
L'utente deve appartenere a organizzazioni che soddisfano una condizione specificata dagli attributi dell'organizzazione.	Utenti in organizzazioni in cui Tipo attività=oro o platino	in organizzazioni in cui <filtro organizzazione>
L'utente deve appartenere a organizzazioni specifiche e soddisfare attributi utente specifici.	Utenti dove titolo=responsabile e località=est e che sono nell'organizzazione vendite o marketing	dove <filtro utente> e che sono in <regola organizzazione>
L'utente deve appartenere a uno specifico gruppo.	Utenti membri di gruppo 401K	membri di gruppo <gruppo>
L'utente deve essere un membro di un ruolo.	Utenti membri di ruolo Assistenza tecnica	membri di <regola di ruolo>
L'utente deve essere un amministratore di un ruolo.	Utenti amministratori di ruolo Responsabile vendite	amministratori di <regola di ruolo>
L'utente deve essere titolare di un ruolo.	Utenti titolari di ruolo Manager utente	titolari di <regola di ruolo>
L'utente deve appartenere a un gruppo che soddisfa una condizione specificata dagli attributi del gruppo.	Gli utenti che sono membri di gruppi in cui titolare=CIO	membri di gruppo <filtro gruppo>

Condizione regola	Esempio	Sintassi regola
L'utente deve soddisfare una condizione basata su una query LDAP.	(Utilizzare una directory LDAP per situazioni in cui non sia sufficiente una query creata nella console Identity Manager)	utente restituito dalla query ldap_query

Alcune regole possono comportare il confronto di un valore con un attributo multivalore. Perché la regola sia applicabile, deve essere soddisfatta da almeno un valore nell'attributo multivalore. Ad esempio, se la regola è Attributo A è uguale a 1, e il valore dell'attributo A è 1, 2, 3 per Utente X, Utente X soddisfa i criteri.

È possibile che l'utente che crea un ruolo non sia in grado di modificarlo. Per poter modificare il ruolo, l'utente deve soddisfare le condizioni nelle regole di titolarità.

Nota: nelle implementazioni di grandi dimensioni, la valutazione delle regole relative a membri, amministratori e titolari può richiedere molto tempo. Per ridurre il tempo necessario alla valutazione delle regole che includono attributi utente, è possibile attivare l'opzione di valutazione in memoria. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Regole di ambito

Le regole per membri e amministrazione si associano alle regole di ambito. Le *regole di ambito* limitano gli oggetti su cui è possibile utilizzare il ruolo.

- Per un membro del ruolo, le regole di ambito controllano quali oggetti è possibile gestire con il ruolo.
- Per un amministratore di ruolo, le regole di ambito controllano quali utenti possono diventare membri e amministratori di ruolo.

L'ambito si applica all'oggetto primario dell'attività. Ad esempio, l'utente è l'oggetto primario dell'attività Crea utente. Tuttavia, l'ambito non si applica ai gruppi dell'utente, poiché un gruppo è un oggetto secondario.

Per la maggior parte dei tipi di oggetto, è possibile specificare i tipi di regole di ambito nella tabella seguente.

Condizione regola	Esempio	Sintassi regola
Tutto	I membri del ruolo possono gestire tutti gli oggetti	Tutto
L'oggetto deve soddisfare uno o più valori dell'attributo.	Utenti in cui title inizia per senior	in cui <filtro>

Quando si seleziona l'opzione di filtro, CA Identity Manager visualizza due tipi di filtri:

<attributo> <comparatore><valore>

Un attributo nel profilo dell'oggetto deve corrispondere a un valore specifico.

<attributo> <comparatore> <attributo utente> dell'amministratore

Un attributo nel profilo dell'oggetto deve corrispondere a un attributo nel profilo dell'amministratore. Ad esempio: utenti dove manager = ID utente dell'amministratore.

Sono disponibili ulteriori opzioni, descritte nelle tabelle seguenti, per utente, gruppo e oggetti dell'organizzazione.

Nota: Le regole di ambito utente seguenti sono esempi. È possibile creare altre regole per gestire relazioni diverse tra l'amministratore e gli utenti che possono essere gestiti dall'amministratore.

Condizione regola	Esempio	Sintassi regola
L'utente deve corrispondere a un valore attributo.	Utenti dove il membro del gruppo Vendite o il telefono cellulare è diverso da null	dove <filtro utente>
L'utente deve corrispondere a più valori attributo.	Utenti dove titolo=manager e località=USA	dove <filtro utente>
L'utente deve appartenere alle organizzazioni indicate.	Utenti in organizzazione Australia o Nuova Zelanda Nota: La regola di ambito dell'organizzazione si applica alle organizzazioni secondarie della stessa che soddisfano la regola. Ad esempio, se la regola dell'organizzazione è "in Organization1", la regola di ambito si applica a Organization1.1 e Organization1.2, ma non a Organization1.	in <regola organizzazione>
L'utente deve appartenere a organizzazioni che soddisfano una condizione specificata dagli attributi dell'organizzazione.	Utenti in organizzazioni in cui Tipo attività=oro o platino	in organizzazioni in cui <filtro organizzazione>
L'utente deve appartenere a organizzazioni specifiche e soddisfare attributi utente specifici.	Utenti dove titolo=manager e località=est e che sono in reparto vendite o marketing dell'organizzazione	dove <filtro utente> e che sono in <regola organizzazione>

Condizione regola	Esempio	Sintassi regola
L'attributo sul profilo di un utente deve corrispondere a un attributo sul profilo dell'amministratore.	Utenti dove manager = ID utente dell'amministratore	dove <attributo utente> <comparatore> <attributo utente> dell'amministratore Nota: Utilizzare il criterio di confronto Diverso da con un attributo multivalore.
L'utente è nella stessa organizzazione dell'amministratore.	Utenti nell'organizzazione in cui Jeff (l'amministratore) è un membro	organizzazione dell'amministratore
L'utente è in un'organizzazione elencata nell'attributo dell'amministratore.	Utenti nel gruppo vendite o marketing	organizzazione che è un valore in <attributo amministrazione> dell'amministratore

Nota: Le seguenti regole di ambito del gruppo sono solo degli esempi. È possibile creare altre regole per gestire relazioni diverse tra l'amministratore e i gruppi che possono essere gestiti dall'amministratore.

Condizione regola	Esempio	Sintassi regola
Il gruppo deve corrispondere a un valore di attributo.	Nome gruppo in cui Nome gruppo = 401K	in cui <filtro gruppo>
I gruppi devono appartenere alle organizzazioni indicate.	Gruppi in contabilità e livelli inferiori dell'organizzazione	in <regola organizzazione>
Il gruppo deve corrispondere a un valore di attributo e appartenere alle organizzazioni indicate.	Gruppi in cui BusinessType = finanza e che sono in vendite e livelli inferiori dell'organizzazione	in cui <filtro gruppo> e che sono in <regola organizzazione>
Il gruppo deve essere elencato in un attributo dell'amministratore.	Gruppi in cui Descrizione = Engineering	in cui <attributo gruppo> <comparatore> <attributo utente> dell'amministratore Nota: Utilizzare il criterio di confronto Diverso da con un attributo multivalore.

Nota: Le seguenti regole di ambito dell'organizzazione sono solo degli esempi. È possibile creare altre regole per gestire relazioni diverse tra l'amministratore e le organizzazioni che può gestire.

Condizione regola	Esempio	Sintassi regola
L'organizzazione deve corrispondere a un valore di attributo.	organizzazioni in cui Nome organizzazione=finanza	in cui <filtro organizzazione>
L'organizzazione deve appartenere all'organizzazione indicata.	organizzazioni in finanza e livelli inferiori	in <regola organizzazione>
L'organizzazione deve corrispondere a un valore di attributo e appartenere all'organizzazione indicata.	organizzazioni in cui Nome organizzazione=finanza e sono in finanza e livelli inferiori	in cui <filtro organizzazione> e sono in <filtro organizzazione>

Valutazione degli operatori

Durante la creazione di regole per un ruolo, è possibile includere gli operatori >=, <=, <, e >. In ogni caso, questi operatori vengono valutati come stringhe dalla directory LDAP o dal database relazionale. La maggior parte degli archivi utenti confronta le stringhe in base all'alfabeto. Di conseguenza, confrontando 500 con 1100, l'archivio utenti può determinare che 500 è maggiore perché 5 è maggiore di 1.

È possibile modificare il modo in cui le stringhe vengono confrontate nell'archivio utenti. Consultare la documentazione del servizio della directory LDAP o del software del database relazionale.

Mancanza di distinzione tra maiuscole e minuscole nelle regole

Quando si creano ruoli di amministrazione o di accesso, le regole create possono essere valutate con o senza la distinzione tra maiuscole e minuscole, a seconda dell'archivio utenti.

Tuttavia, alla fine di un'operazione di creazione o di modifica, le regole vengono valutate internamente senza distinzione tra maiuscole e minuscole prima di confermare le modifiche all'archivio utenti. Ad esempio, se una regola presenta una condizione in cui title=manager, la regola corrisponde all'oggetto dell'archivio utenti sia nel caso che abbia come valore di titolo manager o Manager.

Azioni di aggiunta e rimozione

È necessario specificare un'impostazione di Aggiungi azione e Rimuovi azione per consentire a Identity Manager di gestire correttamente l'appartenenza quando un ruolo viene assegnato o revocato da un amministratore.

- Aggiungi azione deve far sì che l'utente soddisfi i criteri in una delle regole membri del ruolo. Ad esempio, se la regola membri del ruolo di Manager utente dichiara che i membri del ruolo hanno Manager utente come valore del loro attributo Ruoli di amministrazione, l'impostazione Aggiungi azione deve aggiungere Manager utente all'attributo Ruoli di amministrazione.
- L'impostazione Rimuovi azione deve modificare il profilo di un utente in modo che l'utente non soddisfi più la regola membri quando questa viene revocata.

Ciascun ruolo può avere due *azioni di aggiunta* e due *azioni di rimozione*.

Se gli amministratori possono aggiungere e rimuovere membri del ruolo, è possibile definire le azioni di aggiunta e rimozione. In caso contrario, l'utente dispone del ruolo soddisfacendo la regola membri, ad esempio se appartiene al gruppo RoleAdmins. Ad esempio:

- Il ruolo A può essere assegnato da un amministratore, in modo che vengano definite le azioni di aggiunta o di rimozione.
- Il ruolo B ha una regola in base alla quale tutti i membri del gruppo "amministrazione" dispongono del ruolo. Poiché non è possibile assegnare questo ruolo, esso non dispone di azioni di aggiunta o rimozione.

Quando si definiscono le azioni di aggiunta o rimozione, si consiglia di utilizzare l'attributo Ruolo di amministrazione, che Identity Manager può utilizzare per archiviare un elenco di ruoli dell'utente. Ad esempio, è possibile configurare un'azione di aggiunta che aggiunge Dipendente all'attributo Ruolo di amministrazione di un utente quando questo utente viene aggiunto come membro del ruolo Dipendente. Quando un amministratore assegna il ruolo di Dipendente a un manager che ha già il ruolo di Amministratore automatico e quello di Manager utenti, l'attributo Ruolo di amministrazione del manager conterrà i valori seguenti: Self Administrator, User Manager, Employee.

Per utilizzare l'attributo Ruolo di amministrazione, è necessario eseguire il mapping dell'attributo %ADMIN_ROLE_CONSTRAINT% conosciuto a un attributo multivalore nei profili utente. Per ulteriori informazioni, consultare la *Guida alla configurazione di CA Identity Manager*.

Importante. Quando si definisce un'azione Aggiungi, non impostare una regola che faccia riferimento al ruolo in corso di definizione. Ad esempio, non definire un'azione Aggiungi per impostare membro del ruolo A come membro del ruolo A. In questo caso si genera un errore ricorsivo che causerà il riavvio del Policy Server.

Criteri membri

Un *criterio membri* indica che se un utente soddisfa la regola membri, quell'utente ha l'ambito definito in quel criterio. Nella figura seguente viene mostrato un ruolo con due criteri membri.

- Il primo criterio indica che se un membro del ruolo ha come manager Jones, quel membro può utilizzare il ruolo sugli utenti dell'Ufficio vendite e gestirli come membri del gruppo 401k.
- Il secondo criterio indica che se un membro del ruolo si trova nella città di Bend, tale membro del ruolo può usare il ruolo sugli utenti che si trovano nello stato dell'Oregon e gestirli come membri dei gruppi che hanno Smith come Amministratore del gruppo.

Member Policies

	Member Rule	User Scope Rule	Group Scope Rule
▶	where (Manager = "Jones")	where (Office = "Sales")	where (Group Name = "401K")
▶	where (City = "Bend")	where (State = "OR")	where (Group Admin = "Smith")

Criteri di amministrazione

Un *criterio di amministrazione* indica che se un utente soddisfa la regola di amministrazione, quell'utente ha l'ambito utente e i privilegi di amministratore definiti in quel criterio. L'ambito utente definisce dove il ruolo viene utilizzato. I privilegi di amministratore determinano se l'amministratore di ruolo può gestire membri o gestire amministratori di ruolo.

Nella figura seguente viene mostrato un ruolo con due criteri di amministrazione, definiti come segue:

- Per il primo criterio, un amministratore IT può aggiungere e rimuovere membri e amministratori del ruolo dagli utenti nella città di Boston.
- Per il secondo criterio, un amministratore delle vendite può aggiungere e rimuovere membri nello stato dell'Ohio.

Admin Policies

	Admin Rule	User Scope Rule	Manage Members	Manage Administrators	
▶	where (Employee Type = "IT Admin")	where (City = "Boston")	☒	☒	⊖
▶	where (Office = "Sales")	where (State = "Ohio")	☒	☒	⊖

Elenco di controllo di pianificazione del ruolo

Prima di creare un ruolo, utilizzare questo elenco di controllo delle caratteristiche di ruolo.

Caratteristica del ruolo	Dettagli
Profilo di ruolo	Definire un nome e una descrizione per il ruolo e impostare lo stato su Attivo.
Attività	Includere le attività di amministrazione o di accesso.
Modelli di account	Includere i modelli di account che definiscono gli account presenti negli endpoint (solo per i ruoli di provisioning).
Criteri membri	Per ciascun criterio membri, definire: ■ Regole membri: chi può utilizzare il ruolo ■ Regole di ambito: quali oggetti un membro del ruolo può gestire ■ Aggiungi azione: cosa succede al profilo di un utente che diventa un membro ■ Rimuovi azione: cosa succede al profilo di un utente che viene rimosso come membro
Criteri di amministrazione	Per ciascun criterio di amministrazione: ■ Regole di amministrazione: chi può gestire gli utenti come membri o amministratori ■ Regole di ambito: quali utenti l'amministratore può gestire come membri o amministratori ■ Aggiungi azione: cosa succede al profilo di un utente che diventa un amministratore ■ Rimuovi azione: cosa succede al profilo di un utente che viene rimosso come amministratore
Regole di titolarità	Definire chi può modificare il ruolo.

Capitolo 2: Ruoli di amministrazione

Questa sezione contiene i seguenti argomenti:

[Ruoli di amministrazione e attività di amministrazione](#) (a pagina 29)

[Creazione di un ruolo di amministrazione](#) (a pagina 30)

[Verifica di un ruolo di amministrazione](#) (a pagina 35)

[Assegnazione dei ruoli a se stessi](#) (a pagina 35)

Ruoli di amministrazione e attività di amministrazione

È possibile creare ruoli contenenti attività finalizzate alla gestione di oggetti in base alle singole esigenze aziendali. Ad esempio, si creano ruoli con attività di gestione utenti e altri ruoli con attività di gestione dei ruoli creati.

In alternativa, si creano ruoli distinti contenenti:

- Attività destinate agli amministratori e finalizzate alla gestione degli utenti
- Attività finalizzate alla gestione degli amministratori
- Attività finalizzate alla gestione dei ruoli di amministrazione
- Attività finalizzate alla gestione dei ruoli di accesso

Nota: È inoltre possibile utilizzare i ruoli di amministrazione predefiniti disponibili in CA Identity Manager. Tali ruoli includono attività raggruppate in categorie simili all'elenco precedentemente descritto.

Ruoli di amministrazione e ambienti Identity Manager

Quando si effettua l'accesso ad un ambiente Identity Manager specifico, l'account utente utilizzato per l'accesso è associato ad uno o più ruoli di amministrazione. Ogni ruolo di amministrazione include attività, ad esempio Crea utente, che possono essere utilizzate nell'ambiente Identity Manager corrente.

Ad esempio, nell'ambiente Identity Manager *centrale* il ruolo di amministrazione *Help desk* include attività finalizzate al ripristino delle password. Il ruolo è associato ad una regola membro in base alla quale l'utente corrispondente deve essere un addetto del settore IT. Quando gli utenti IT accedono all'ambiente Identity Manager *centrale*, essi disporranno del ruolo *Help desk* e saranno in grado di ripristinare le password degli utenti contenuti in tale ambiente Identity Manager.

Ruoli di amministrazione e console utente

L'ambiente Identity Manager viene visualizzato all'interno della console utente. I ruoli di amministrazione assegnati determinano gli elementi disponibili in tale console, come illustrato nella seguente tabella.

Ruoli assegnati	Formato della console utente
Ruolo Gestore sistema	Elenco delle categorie relativo a tutti gli oggetti e tutte le attività di amministrazione predefinite per la gestione di tali oggetti
Ruoli per la gestione di più tipi di oggetti	Elenco delle categorie contenente un elemento per ogni tipo di oggetto che è possibile gestire
Ruoli per la gestione di un tipo di oggetto, ad esempio Utenti	Attività associate a tale oggetto, ad esempio Modifica utente, <i>senza</i> un elenco di categorie
Ruolo di approvazione	Schermo Elenco di lavoro Schermata visualizzata se l'amministratore è associato ad attività con approvazione in sospeso, ad esempio la registrazione automatica degli utenti richiede l'approvazione

In caso di gestione di più oggetti, l'elenco delle categorie include gli oggetti che è possibile modificare, ad esempio Utenti e Gruppi, sotto forma di schede disponibili lungo la parte superiore della schermata. Selezionare una scheda per visualizzare le attività disponibili nei ruoli assegnati.

Nota: se il browser Internet non supporta i fogli di stile CSS (Cascading Style Sheets), il formato della console utente sarà diverso. Per la gestione di tale formato, vedere la *Guida alla configurazione*.

Creazione di un ruolo di amministrazione

È possibile creare un ruolo di amministrazione dopo aver analizzato i requisiti del ruolo specifico. Tali requisiti fanno riferimento agli utenti che utilizzeranno il ruolo, agli oggetti gestiti dal ruolo ed all'ambiente contenente gli oggetti da gestire.

Procedura preliminare di creazione del ruolo di amministrazione

Per creare un ruolo di amministrazione, utilizzare la console utente.

Per creare un ruolo di amministrazione:

1. Accedere a CA Identity Manager utilizzando un account con un ruolo associato ad attività finalizzate alla creazione di ruoli di amministrazione.

Ad esempio, il primo utente di un ambiente è associato al ruolo Gestore sistema, che dispone dell'attività Crea ruolo di amministrazione.

2. Selezionare Ruoli e attività, Ruoli di amministrazione, quindi Crea ruolo di amministrazione.

3. Specificare se si desidera creare o copiare un ruolo.

Verrà visualizzata la scheda Profilo, dove sarà possibile iniziare a definire il ruolo di amministrazione.

4. Definire il profilo del ruolo di amministrazione.

Definizione del profilo del ruolo di amministrazione

Nella scheda Profilo è possibile definire le caratteristiche di base del ruolo.

Per definire il profilo

1. Immettere un nome e una descrizione, quindi impostare gli attributi personalizzati desiderati definiti per il ruolo specifico.

Nota: nella scheda Profilo è possibile definire attributi personalizzati con i quali specificare informazioni aggiuntive sui ruoli di amministrazione. Tali informazioni aggiuntive sono utili per facilitare le ricerche di ruoli in ambienti che presentano un numero elevato di ruoli.

2. Selezionare Attivato per rendere disponibile il ruolo subito dopo la creazione.
3. [Selezionare le attività di amministrazione per il ruolo](#) (a pagina 32).

Selezione delle attività di amministrazione per il ruolo

Nella scheda Attività è possibile selezionare le attività di amministrazione da includere nel ruolo. È possibile includere attività appartenenti a categorie diverse oppure copiare le attività utilizzate in un altro ruolo.

Per selezionare le attività di amministrazione

1. Selezionare la categoria nel campo Filtra per categoria.
Per visualizzare l'elenco delle categorie di attività disponibili, fare clic sulla freccia rivolta verso il basso.
2. Selezionare l'attività da includere nel ruolo nel campo Aggiungi attività.
L'attività verrà aggiunta all'elenco di attività nel ruolo.
3. Per aggiungere altre attività, ripetere i passaggi 1 e 2.
4. Per rimuovere un'attività dal ruolo, fare clic sul segno meno () per tale attività.
5. [Definire i criteri membri per un ruolo di amministrazione](#) (a pagina 33).

Definizione dei criteri membri per un ruolo di amministrazione

Nella scheda Membri è possibile creare i criteri membri per definire gli utenti che potranno essere membri di un ruolo specifico.

Per definire i criteri membri

1. Fare clic su **Aggiungi** per definire i criteri membri. Un criterio membri contiene le regole descritte di seguito.

- Una regola membri che definisce i requisiti in base ai quali un utente può essere membro di un ruolo.

Nota: gli operatori riportati di seguito consentono di gestire i numeri come caratteri all'interno delle regole membro:

- Minore di (<)
- Minore di o uguale a (<=)
- Maggiore di (>)
- Maggiore di o uguale a (>=)

Ad esempio, '10' sarà maggiore di (dopo) '1' ma minore di (prima) '2'.

- Regole di ambito, che consentono di limitare gli oggetti primari e secondari disponibili per le attività incluse nel ruolo.

Ad esempio, se un ruolo contiene un'attività che modifica gli utenti mediante la loro assegnazione a gruppi, la regola di ambito utente consente di limitare gli utenti (oggetto primario) che possono essere individuati, mentre la regola di ambito gruppo consente di limitare i gruppi (oggetto secondario) che è possibile assegnare.

Nota: accertarsi di immettere una risposta almeno per una domanda relativa all'ambito. Le regole di ambito consentono di limitare gli oggetti primari e secondari disponibili per le attività incluse nel ruolo. Ad esempio, se un ruolo contiene un'attività che modifica gli utenti mediante la loro assegnazione a gruppi, la regola di ambito utente consente di limitare gli utenti (oggetto primario) che possono essere individuati, mentre la regola di ambito gruppo consente di limitare i gruppi (oggetto secondario) che è possibile assegnare.

2. Verificare che il criterio membri sia visualizzato nella scheda Membri.
 - Per modificare un criterio, fare clic sulla freccia a destra disponibile a sinistra.
 - Per rimuovere il criterio, fare clic sull'icona raffigurante il segno meno.
3. Nella scheda Membri selezionare la casella di controllo "Gli amministratori possono aggiungere o rimuovere i membri di questo ruolo" a meno che non si desideri che gli utenti diventino membri solo quando risultano conformi ad una regola membri.

Dopo aver attivato questa caratteristica, la schermata verrà ingrandita.

4. Nell'area espansa definire l'azione di aggiunta e l'azione di rimozione da utilizzare quando un utente viene aggiunto o rimosso come membro del ruolo.

Importante. Quando si definisce un'azione di aggiunta, evitare di impostare una regola che faccia riferimento al ruolo in fase di definizione. Ad esempio, non definire un'azione di aggiunta che preveda l'aggiunta di un membro del Ruolo A in virtù della sua appartenenza al Ruolo A. Ciò potrebbe generare errori.

5. [Definire i criteri di amministrazione per il ruolo di amministrazione](#) (a pagina 34).

Definizione dei criteri di amministrazione per il ruolo di amministrazione

Nella scheda Amministratori definire gli utenti che possono aggiungere o rimuovere membri ed amministratori di questo ruolo.

Per definire i criteri di amministrazione

1. Per rendere disponibile l'opzione Gestione amministratori, selezionare la casella di controllo "Gli amministratori possono aggiungere o rimuovere gli amministratori di questo ruolo".

Dopo aver attivato questa caratteristica, la schermata verrà ingrandita.

2. Nell'area espansa definire l'azione di aggiunta e l'azione di rimozione da utilizzare quando un utente viene aggiunto o rimosso come amministratore del ruolo.
3. Definire i criteri di amministrazione impostando le regole di amministrazione, le regole di ambito ed almeno un privilegio di amministrazione (Gestisci membri o Gestione amministratori).

Nota: è possibile aggiungere più criteri di amministrazione con regole e privilegi diversi per gli amministratori che soddisfano la regola.

4. Per modificare un criterio, fare clic sulla freccia disponibile a sinistra. Per rimuovere il criterio, fare clic sull'icona raffigurante il segno meno.
5. [Definire le regole proprietari per un ruolo di amministrazione](#) (a pagina 35).

Definizione delle regole proprietari per un ruolo di amministrazione

Nella scheda Proprietari definire le regole che determinano chi può essere il proprietario del ruolo, ovvero l'utente che può modificare il ruolo stesso.

Per definire le regole proprietari

1. Definire le regole proprietari che determinano gli utenti che possono modificare il ruolo.
2. Fare clic su Inoltra.

Viene visualizzato un messaggio indicante che l'attività è stata inoltrata. Prima di poter utilizzare il ruolo definito, potrebbe essere necessario attendere alcuni minuti.

Se è stata selezionata l'opzione Attivato durante la creazione del ruolo, il ruolo risulterà disponibile per l'utilizzo. Se un utente soddisfa i requisiti definiti nella regola membri potrà effettuare l'accesso all'ambiente Identity Manager ed utilizzare le attività disponibili in tale ruolo.

Verifica di un ruolo di amministrazione

Per verificare la creazione del ruolo, scegliere Ruoli di amministrazione, Visualizza ruolo di amministrazione, quindi selezionare il nome del ruolo desiderato.

In alternativa, è possibile scegliere Sistema, Visualizza attività inoltrate per verificare se l'attività di creazione del ruolo è stata completata.

Assegnazione dei ruoli a se stessi

Gli utenti possono assegnare certi ruoli a se stessi. Ad esempio, è possibile consentire agli utenti di assegnare a se stessi il ruolo Gestore delega in modo da poter delegare gli elementi di lavoro di un utente ad un utente diverso.

Per definire i ruoli che gli utenti possono assegnare a se stessi, configurare i criteri nell'attività Gestione automatica ruoli.

Procedere come descritto di seguito:

1. Modificare l'attività Gestione automatica ruoli come indicato di seguito:
 - a. Selezionare Ruoli e attività, Modifica attività di amministrazione, quindi cercare l'attività Gestione automatica ruoli.
 - b. Selezionare la scheda Schede.

CA Identity Manager mostra l'elenco delle schede disponibili per l'attività.

- c. Selezionare la freccia rivolta verso destra accanto alla scheda Gestione automatica ruoli per modificarla.
- d. Completare i seguenti campi:

Mostra solo ruoli di amministrazione che rispettano le regole seguenti

Consente di specificare i criteri che verranno utilizzati in CA Identity Manager per determinare i ruoli che gli utenti possono assegnare a se stessi.

Per aggiungere ulteriori regole, fare clic sull'icona con il segno più (+).

Utente usato come amministratore di un ruolo di amministrazione

Consente di specificare l'amministratore per ruoli che gli utenti possono assegnare a se stessi.

Per ruoli che gli utenti possono assegnare a se stessi, l'utente selezionato in questo campo deve essere definito come amministratore e devono essere soddisfatti i criteri specificati nel campo Mostra solo ruoli di amministrazione che rispettano le regole seguenti.

Schermata elenco

Consente di specificare le colonne e il formato dell'elenco di ruoli che un utente può selezionare per assegnarli a se stesso.

- e. Fare clic su OK, quindi su Inoltra.
- 2. Aggiungere l'attività Gestione automatica ruoli ad un ruolo, quindi assegnare tale ruolo agli utenti appropriati.

Capitolo 3: Attività di amministrazione

Questa sezione contiene i seguenti argomenti:

[Pianificazione delle attività di amministrazione](#) (a pagina 37)
[Opzioni di utilizzo delle attività di amministrazione](#) (a pagina 41)
[Attività di amministrazione predefinite](#) (a pagina 42)
[Procedura di creazione di un'attività di amministrazione personalizzata](#) (a pagina 43)
[Definizione del profilo dell'attività](#) (a pagina 44)
[Definizione dell'ambito dell'attività](#) (a pagina 49)
[Selezione delle schede per l'attività](#) (a pagina 60)
[Visualizzazione di campi nell'attività](#) (a pagina 64)
[Visualizzazione utilizzo ruolo](#) (a pagina 64)
[Assegnazione di processi del flusso di lavoro per gli eventi](#) (a pagina 64)
[Gestione di un archivio utenti di Active Directory](#) (a pagina 65)
[Attività esterne per le funzioni dell'applicazione](#) (a pagina 67)
[Componenti di attività avanzati](#) (a pagina 69)
[Eventi ed attività di amministrazione](#) (a pagina 71)
[Elaborazione dell'attività di amministrazione](#) (a pagina 73)
[Immagini per Attività di amministratore](#) (a pagina 77)

Pianificazione delle attività di amministrazione

I ruoli di amministrazione sono composti da attività di amministrazione, che rappresentano le capacità granulari di gestione degli oggetti. Ad esempio, è possibile gestire un oggetto utente mediante l'utilizzo delle seguenti attività di amministrazione:

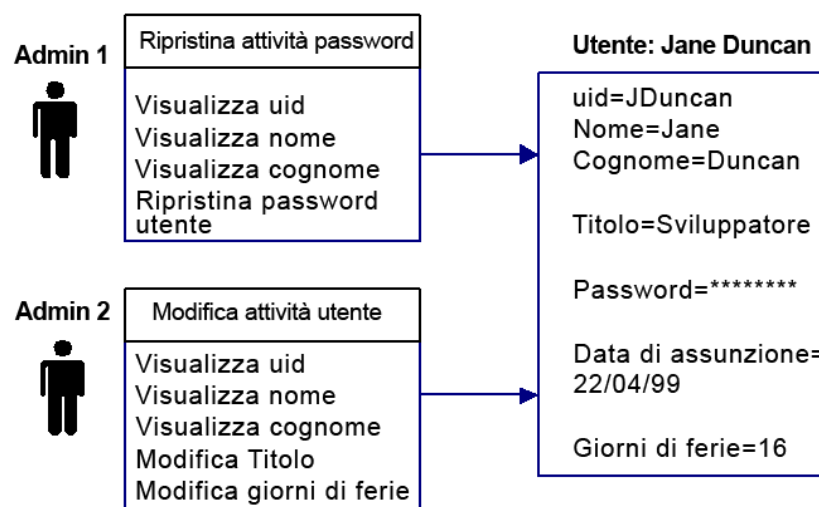
- Crea utente
- Visualizza utente
- Modifica utente
- Reimposta password utente

È possibile creare o modificare ciascun attività in base alle specifiche esigenze. È inoltre possibile combinare attività di amministrazione specifiche in ruoli di amministrazione che verranno assegnati agli amministratori. Grazie a tali ruoli, gli amministratori dispongono di tutti i privilegi necessari per la gestione degli oggetti.

Per pianificare la creazione di un'attività di amministrazione, individuare gli oggetti da gestire (Utente, Gruppo, Organizzazione, Ruolo o Attività) e gli amministratori che utilizzeranno tali attività. Ad esempio:

- Per gestire gli utenti, gli amministratori con ruolo Help desk devono disporre di attività finalizzate alla gestione degli attributi utente, ad esempio l'ID utente o il titolo.
- Per gestire l'accesso degli utenti alle applicazioni, altri amministratori devono disporre di attività che consentono di definire gli utenti come membri di ruoli di accesso.
- Per gestire i ruoli utilizzati dagli amministratori con ruolo Help desk, gli amministratori di livello superiore devono disporre di attività che supportano la gestione dei ruoli di amministrazione.

Per un tipo di oggetto, ad esempio Utenti, è possibile creare attività in modo tale che amministratori diversi possono gestire attributi distinti. Ad esempio, la seguente figura fa riferimento ad un utente gestito da due amministratori.



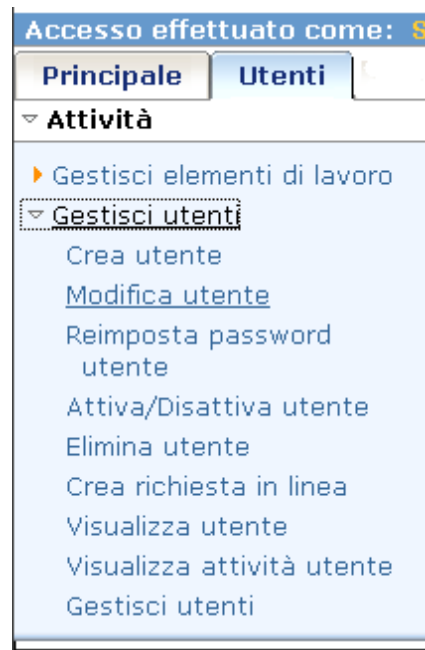
- Il primo amministratore (Admin 1) è associato all'attività Reimposta password utente, ovvero può visualizzare l'ID utente e il nome del dipendente, nonché reimpostare la relativa password.
- Il secondo amministratore (Admin 2) è associato all'attività Modifica utente, ovvero può visualizzare l'ID utente e il nome del dipendente, nonché modificare il relativo titolo e i periodi di ferie.

Esempio di attività di amministrazione

Durante la creazione di un'attività di amministrazione vengono definiti i contenuti e il layout degli schermi associati all'attività, fra cui:

- Il nome dell'attività;
- La categoria in cui l'attività sarà visualizzata;
- Le schede e i campi da utilizzare nell'attività e le proprietà di visualizzazione dei campi;
- I campi che un amministratore può utilizzare in una query di ricerca, nonché i campi visualizzati nei risultati delle ricerche.

Per comprendere meglio gli elementi che costituiscono un'attività, si consideri l'attività Modifica utente. In questo caso, Utenti corrisponde alla categoria, Gestisci utenti a una sottocategoria e Modifica utente è l'attività. Quando si crea un'attività, vengono creati i nomi della categoria e dell'attività.



Quando si sceglie Modifica utente, viene visualizzato una schermata di ricerca. In una schermata *di ricerca* sono disponibili le opzioni per la ricerca dell'oggetto da visualizzare o modificare. Ogni opzione viene definita *filtro* e consente di specificare un limite per gli oggetti individuati dalla ricerca.

Dopo aver impostato tutti i campi disponibili nella schermata di ricerca, viene visualizzato una schermata contenente schede. Nella figura seguente sono illustrate le schede disponibili per l'attività Modifica utente. Nella scheda Profilo sono visualizzati gli attributi dell'utente, mentre nelle altre schede sono visualizzati i privilegi a livello di ruolo e di gruppo per l'utente specifico.

Per l'attività creata è necessario definire le schede da includere, nonché il relativo ordine e i contenuti.

Modifica utente: liang

Profilo	Ruoli di accesso	Ruoli di amministrazione	Gruppi	Delega elementi di lavoro

• = Obbligatorio

Organizzazione

ID utente

Attivato ☒

• **Nome**

• **Cognome**

• **Nome completo**

Posta elettronica

Ad esempio, utilizzando l'attività Modifica utente come modello è possibile creare un'attività Modifica appaltatore, per la quale sono state apportate modifiche:

- Ai campi della scheda Profilo;
- Alle schede da includere nell'attività e ai contenuti corrispondenti;
- Alla categoria in cui l'attività sarà visualizzata.

È possibile creare questa attività all'interno della nuova categoria Appaltatore.

Accesso effettuato come: SuperAdmin	
Principale	Contraente
Utenti	
▼ Attività	
▶ Gestisci Contraenti Modifica Contraente	

Nell'attività Modifica appaltatore sono disponibili alcuni campi della scheda Profilo dell'attività Modifica utente, oltre ad altri campi, ad esempio la data di inizio del contratto e la società dell'appaltatore. Gli amministratori potranno cercare un appaltatore in base al nome dell'appaltatore, alla società e alla data di inizio del contratto.

Modify Contractor: *jhansen*

Profile	Groups	Contractor Roles
User ID jhansen		
Enabled ☒		
• First Name	Julia	
• Last Name	Hansen	
Email	jhansen@wxyz.com	
Start Date	10/19/2007	
Company		

La nuova attività include anche una scheda Ruoli appaltatore, che consente di aggiungere ruoli per gli appaltatori.

Opzioni di utilizzo delle attività di amministrazione

In Identity Manager sono disponibili due modalità di utilizzo delle attività di amministrazione:

- **Selezione dell'attività**

Vengono innanzitutto selezionate una categoria e un'attività, quindi viene eseguita la ricerca dell'oggetto a cui si applica l'attività.

Ad esempio, per modificare un profilo utente, selezionare la categoria Utenti, quindi scegliere l'attività Modifica utente. A questo punto, cercare l'utente da modificare.

■ Selezione dell'oggetto

Per cercare un oggetto è possibile utilizzare attività di gestione quali Gestisci utenti o Gestisci gruppi. Dopo aver selezionato l'oggetto, è possibile visualizzare l'elenco delle attività che possono essere utilizzate per gestirlo. Questo metodo viene definito *esplorazione oggetto-attività*.

Ad esempio, per modificare un utente con questo metodo, selezionare la categoria Utente, quindi scegliere l'attività Gestisci utente. Cercare e selezionare l'utente che si desidera gestire. Nei risultati della ricerca fare clic su un'icona per visualizzare l'elenco delle attività che è possibile utilizzare per gestire l'utente selezionato. Nell'elenco è possibile selezionare Modifica utente o qualsiasi altra attività appropriata.

È inoltre possibile configurare elenchi di attività in attività diverse da quelle di gestione. Ad esempio, è possibile aggiungere un elenco di attività ad una scheda Appartenenza. In questo caso, sarà disponibile un elenco di attività per ogni membro incluso nella scheda Appartenenza.

Nota: nell'elenco di attività relativo ad un oggetto specifico vengono visualizzate solo le attività che l'amministratore corrente può utilizzare.

Attività di amministrazione predefinite

In CA Identity Manager è inclusa una serie di attività e ruoli di amministrazione predefiniti che vengono aggiunti a CA Identity Manager importando un file di definizioni dei ruoli nella Console di gestione. Quando si crea un ambiente nella Console di gestione e si decide di creare i ruoli predefiniti, in CA Identity Manager viene importato automaticamente un file di definizioni dei ruoli.

Nota: per supportare alcune funzionalità quali la gestione degli account per alcuni tipi di endpoint, potrebbe essere necessario importare ulteriori file di definizioni dei ruoli per creare i ruoli e le attività necessari.

Solitamente è possibile utilizzare le attività predefinite così come vengono installate, ma può risultare necessario modificare la scheda Profilo nelle attività utente predefinite, quali Crea utente, Modifica utente e Visualizza utente. La scheda Profilo comprende tutti i campi definiti per l'oggetto utente nel file di configurazione delle directory. Potrebbe risultare opportuno limitare il numero di campi visualizzati nella scheda, oppure modificare le proprietà di visualizzazione dei campi.

Nota: si consiglia di creare una copia di un'attività predefinita da modificare anziché modificare l'attività predefinita stessa.

Procedura di creazione di un'attività di amministrazione personalizzata

Un'attività di amministrazione è una funzione amministrativa che un utente può eseguire in Identity Manager. Esempi di attività di amministrazione sono Crea utente, Modifica gruppo e Visualizza appartenenza ruolo.

CA Identity Manager comprende attività di amministrazione predefinite modificabili in base alle proprie esigenze di business.

La procedura di creazione di un'attività di amministrazione personalizzata si articola nei passaggi descritti di seguito.

Nota: nella sezione [Prerequisiti di Active Directory](#) (a pagina 65) sono incluse ulteriori considerazioni nel caso in cui un archivio utenti Active Directory venga gestito con CA Identity Manager.

1. Nella Console utente di CA Identity Manager selezionare Ruoli e attività, Attività di amministrazione, Crea attività di amministrazione.

CA Identity Manager chiederà all'utente se desidera creare una nuova attività oppure crearne una in base a un'attività esistente.

Ad esempio, selezionare l'attività Modifica utente come base per la creazione della nuova attività.

2. Selezionare Crea copia di attività esistente, quindi cercare l'attività da copiare.

Nota: si consiglia di modificare la copia di un'attività predefinita anziché modificare l'attività predefinita stessa.

3. Dopo aver fatto clic su OK, viene visualizzata una schermata contenente le sei schede descritte di seguito.

Scheda	Scopo	Argomento
Profilo	Definire il profilo dell'attività in fase di creazione	Definizione del profilo dell'attività (a pagina 44)
Cerca	Limitare l'intervallo di oggetti gestito dall'attività	Definizione dell'ambito dell'attività (a pagina 49)
Schede	Selezionare e definire le schede da associare all'attività	Selezione delle schede per l'attività (a pagina 60)
Campi	Visualizzare i campi utilizzati in tutte le schede	Visualizzazione di campi nell'attività (a pagina 64)
Eventi	Selezionare un processo del flusso di lavoro per ogni evento se l'ambiente CA Identity Manager e l'attività utilizzano il flusso di lavoro	Assegnazione di processi del flusso di lavoro per gli eventi (a pagina 64)

Scheda	Scopo	Argomento
Utilizzo ruolo	Consente di visualizzare i ruoli relativi all'attività in fase di visualizzazione o modifica.	Visualizzazione utilizzo ruolo (a pagina 64)

Nota: per ulteriori informazioni sulla creazione delle attività di amministrazione personalizzata, consultare la *User Console Design Guide*.

Definizione del profilo dell'attività

Nella scheda Profilo sono disponibili le impostazioni generali dell'attività.

Come definire il profilo dell'attività

1. Scegliere il tipo di oggetto per l'attività, ovvero l'oggetto primario, quindi l'azione da eseguire su tale oggetto.
2. Impostare i campi richiesti, quindi selezionare le caselle di controllo appropriate per l'attività specifica.

Nota: in caso di creazione di un'attività contenente impostazioni di profilo simili a quelle di un'attività esistente, fare clic su *Copia profilo da un'altra attività*. Questa opzione consente di inserire automaticamente le impostazioni di profilo per l'attività in fase di creazione in base alle impostazioni di profilo di un'attività esistente selezionata. A questo punto, specificare un nome ed una descrizione per la nuova attività.

3. (Facoltativo) Associare un gestore delle attività di logica aziendale all'attività.
4. Dopo aver completato questa scheda, procedere al passaggio successivo [Definizione dell'ambito dell'attività](#) (a pagina 49).

Scheda Profilo attività di amministrazione

Nella scheda Profilo dell'attività di amministrazione è possibile definire le impostazioni generali di un'attività di amministrazione.

Questa scheda contiene i campi seguenti:

- **Nome**

Definisce il nome dell'attività.

- **Tag**

Definisce un identificatore univoco per l'attività. Viene utilizzato in URL, servizi Web o file delle proprietà. Può contenere caratteri ASCII (a-z, A-Z), numeri (0-9) oppure caratteri di sottolineatura e deve iniziare con una lettera o un carattere di sottolineatura.

- **Descrizione**

Consente di specificare una nota facoltativa relativa allo scopo dell'attività.

- **Ordine attività**

Specifica l'ordine in base al quale l'attività verrà visualizzata. Se non si specifica alcun ordine, le attività verranno visualizzate in ordine alfabetico.

- **Categoria**

Specifica una categoria per l'attività. Le categorie vengono visualizzate sotto forma di schede nella parte superiore dello schermo.

- **Ordine categoria**

Specifica l'ordine in base al quale la scheda della categoria viene visualizzata. Ad esempio, se questa opzione viene impostata su 3, la categoria specificata verrà visualizzata come terza scheda.

- **Categoria 2**

Specifica la categoria di secondo livello, che viene visualizzata sotto forma di collegamento sotto l'elenco delle schede delle categorie. La categoria di secondo livello viene visualizzata solo quando viene selezionata la scheda relativa alla categoria di primo livello. Ad esempio, se si crea un'attività con la categoria di primo livello Dipendente ed una categoria di secondo livello Gestione dipendenti, la categoria Gestione dipendenti verrà visualizzata solo dopo aver selezionato la scheda Dipendente.

- **Ordine categoria 2**

Specifica l'ordine in base al quale visualizzare la categoria di secondo livello, se nella categoria primaria esistono più categorie di secondo livello.

■ **Categoria 3**

Specifica la categoria di terzo livello, che viene visualizzata nel riquadro di esplorazione. Le attività vengono elencate nella categoria di terzo livello. Ad esempio, in un ambiente predefinito, un utente con ruolo Gestore sistema o Gestore utente accede alla categoria di terzo livello Gestisci utenti quando seleziona la scheda Utenti.

■ **Ordine categoria 3**

Specifica l'ordine in base al quale la categoria di terzo livello viene visualizzata.

■ **Oggetto principale**

Consente di specificare l'oggetto su cui verrà eseguita l'attività.

■ **Azione**

Consente di specificare l'operazione da eseguire sull'oggetto.

■ **Sincronizzazione utente**

Consente di specificare se l'attività sincronizza gli utenti con i criteri di identità. È possibile selezionare una delle seguenti opzioni:

– **Disattivato** (impostazione predefinita)

Consente di specificare che l'attività non attiva la sincronizzazione dell'utente.

– **Al completamento dell'attività**

Consente di specificare che in CA Identity Manager il processo di sincronizzazione degli utenti venga avviato non appena vengono completati tutti gli eventi di un'attività. Questa impostazione rappresenta l'opzione di sincronizzazione predefinita per le attività Crea utente, Modifica utente ed Elimina utente. L'impostazione predefinita per tutte le altre attività è Disattivato.

Nota: se si seleziona l'opzione Al completamento dell'attività per un'attività che include più eventi, CA Identity Manager non sincronizza gli utenti finché tutti gli eventi nell'attività non sono stati completati. Se uno o più di tali eventi richiedono l'approvazione del flusso di lavoro, tale processo potrebbe impiegare diversi giorni. Per evitare che venga atteso il completamento degli eventi per applicare i criteri di identità, selezionare l'opzione A ogni evento.

– **A ogni evento**

Consente di specificare che in CA Identity Manager il [processo di sincronizzazione degli utenti](#) (a pagina 472) venga avviato non appena viene completato ogni singolo evento di un'attività.

Per attività con un evento primario e un evento secondario per lo stesso utente, l'impostazione del processo di sincronizzazione su A ogni evento potrebbe comportare l'applicazione di un maggior numero di criteri di identità ad un utente rispetto alla selezione dell'opzione Al completamento dell'attività.

■ Sincronizzazione account

Consente di sincronizzare gli account esistenti nel server di fornitura, se è attivata la funzionalità di fornitura.

– **Disattivato** (impostazione predefinita)

Consente di specificare che l'attività non attiva la sincronizzazione degli account.

– **Al completamento dell'attività**

Consente di specificare che in CA Identity Manager il processo di sincronizzazione degli account venga avviato non appena vengono completati tutti gli eventi di un'attività.

– **A ogni evento**

Consente di specificare che in CA Identity Manager il processo di sincronizzazione degli account venga avviato non appena viene completato ogni singolo evento di un'attività.

Nota: per ottimizzare le prestazioni, selezionare Al completamento dell'attività. Tuttavia, se si seleziona l'opzione Al completamento dell'attività per un'attività che include più eventi, CA Identity Manager non sincronizza gli account finché tutti gli eventi nell'attività non sono stati completati. Se uno o più di tali eventi richiedono l'approvazione del flusso di lavoro, tale processo potrebbe impiegare diversi giorni. Per evitare che CA Identity Manager attenda il completamento di tutti gli eventi per sincronizzare gli account, selezionare l'opzione A ogni evento.

■ Nascondi nei menu

Consente di disattivare la visualizzazione dell'attività nei menu. Attivare questo controllo se l'attività viene richiamata solo da un URL o da un'altra attività.

■ Attività pubblica

Consente di impostare l'attività come disponibile agli utenti che non hanno effettuato l'accesso a CA Identity Manager. Le attività pubbliche predefinite fanno riferimento ad attività di gestione di password dimenticate e registrazioni automatiche.

■ Attiva controllo

Consente di registrare le informazioni relative all'attività in un database di controllo. Le informazioni di controllo possono essere utilizzate per generare rapporti. Consultare la *Guida alla configurazione*.

■ Attiva flusso di lavoro

Consente di attivare gli eventi di CA Identity Manager associati all'attività per generare i processi del flusso di lavoro, se è installato il motore del flusso di lavoro. Ad esempio, gli eventi associati all'attività Elimina gruppo possono attivare un processo del flusso di lavoro che include un passaggio di approvazione.

- **Attiva servizi Web**

Consente di contrassegnare l'attività come attività per la quale l'output WSDL (Web Services Description Language) può essere generato dalla console di gestione. Attivare questo controllo se si desidera utilizzare l'inoltro remoto delle attività. Per ulteriori informazioni, consultare la *Programming Guide for Java*.

- **Processo del flusso di lavoro**

Consente di attivare la configurazione per il flusso di lavoro del livello attività. Fare clic sull'icona a forma di matita per configurare il flusso di lavoro basato su criterio o non basato su criterio.

- **Priorità di attività**

Consente di determinare l'ordine di esecuzione delle attività da parte di CA Identity Manager. Le attività con una priorità alta verranno eseguite prima di attività con una priorità media o bassa. La priorità predefinita per un'attività è Media.

Nota: è possibile utilizzare l'attività Visualizza attività inviate per cercare attività associate ad una priorità specifica, quindi visualizzarne lo stato.

- **Gestori attività di logica aziendale**

Consente di associare un [gestore delle attività di logica aziendale](#) (a pagina 69) all'attività.

- **Comandi operazione del flusso di lavoro**

Consente di aggiungere pulsanti di azione personalizzati alle attività di approvazione del flusso di lavoro.

- **Copia profilo da un'altra attività**

Consente di copiare i dati dalla scheda Profilo di un'altra attività.

Ad esempio, è possibile copiare le impostazioni della scheda Profilo dall'attività Modifica utente, quindi modificare il nome e la descrizione.

Proprietà di configurazione dell'attività

Il controllo delle proprietà di configurazione dell'attività visualizza le proprietà e determinati comportamenti dell'attività.

Percorso dell'icona attività

Specifica l'URL di un'immagine da utilizzare come icona per l'attività nell'elenco attività.

Anteprima dell'icona attività

Visualizza l'icona per l'attività, come visualizzata negli elenchi attività.

Elimina esplorazione attività

Se selezionata, questa opzione consente di nascondere la barra di spostamento di primo livello e di elenco attività quando un utente seleziona un'attività. In questo modo si impedisce agli utenti di abbandonare l'attività corrente fino a quando non hanno completato le azioni necessarie o annullato l'attività.

Finestra di destinazione

Quando si specifica un valore per questo campo, in CA Identity Manager viene aperta l'attività in una nuova finestra del browser. Utilizzare questo campo per aprire una nuova finestra del browser per un'attività esterna che reindirizza gli utenti a un altro sito Web.

È possibile specificare qualsiasi nome per la finestra.

Nota: non utilizzare questo campo per aprire le attività di amministrazione di CA Identity Manager in una nuova finestra del browser. CA Identity Manager non supporta più finestre del browser per una singola sessione utente di CA Identity Manager.

Definizione dell'ambito dell'attività

Nella scheda Cerca definire l'ambito dell'attività, ovvero il limite degli oggetti disponibili per l'attività. Se, ad esempio, l'oggetto di un'attività è Utenti, è possibile definire gli appaltatori come ambito a livello di utenti per tale attività.

Nota: se l'attività non dispone di alcun oggetto primario o l'azione è una modifica automatica, una visualizzazione automatica o un'approvazione, la scheda Cerca non verrà visualizzata.

Nella scheda Cerca è possibile configurare le seguenti impostazioni:

Schermata di ricerca

Una schermata di ricerca consente di limitare l'ambito dell'attività in base ai filtri definiti. Fare clic su Sfoglia per visualizzare le opzioni disponibili.

Nota: è possibile creare [schermi di ricerca personalizzati](#) (a pagina 50). Per creare una versione modificata di una schermata di ricerca esistente, selezionare la schermata di ricerca, quindi fare clic su Copia. A questo punto, è possibile modificare la schermata di ricerca senza modificare la definizione della schermata di ricerca originale. Per creare una schermata di ricerca, fare clic su Nuovo.

Opzioni di ricerca

Le opzioni di ricerca vengono visualizzate solo quando l'oggetto è un ruolo o un gruppo.

- La prima opzione consente di limitare la ricerca in base ai campi definiti nella schermata di ricerca. All'interno di tali limiti, la ricerca individua tutti i gruppi o ruoli nell'ambito dell'amministratore.
- Le altre opzioni consentono di limitare la ricerca come indicato.

Si noti quanto segue:

- Per impostazione predefinita, gli schermi di ricerca dei gruppi supportano l'applicazione di filtri. Ciò significa che gli amministratori possono specificare criteri per limitare l'ambito delle ricerche dei gruppi. Per rimuovere la funzionalità di applicazione filtri, creare una schermata di ricerca che non contenga campi da includere in una query di ricerca.
- Il messaggio *Filtraggio non supportato*, visualizzato nella scheda Ricerca quando l'oggetto è un ruolo, indica che l'attività visualizza i ruoli che soddisfano i criteri associati all'opzione selezionata. Vengono ignorati i campi di ricerca configurati nella schermata di ricerca.

Gli oggetti modificati devono rimanere nell'ambito dell'amministratore

Quando questa casella di controllo è selezionata, in CA Identity Manager viene visualizzato un errore se le modifiche all'attività fanno perdere all'amministratore l'ambito sull'oggetto primario. Ad esempio, un amministratore può utilizzare Modifica utente per modificare l'attributo Tipologia dipendente di un utente in Responsabile. Questa modifica può porre l'utente fuori dall'ambito dell'amministratore.

configurazione dello schermo di ricerca

La configurazione dello schermo di ricerca consente di limitare l'ambito dell'attività, nonché controllare i campi in base ai quali è possibile eseguire le ricerche. Gli schermi di ricerca sono validi per due tipi di oggetti:

- *Oggetto primario*: oggetto modificato o visualizzato dall'attività.
- *Oggetto secondario*: oggetto correlato all'oggetto primario.

Ad esempio, se si include una scheda Gruppo in un'attività Crea utente, l'utente è l'oggetto primario, mentre il gruppo è l'oggetto secondario. Nella scheda Gruppo è necessario inserire uno schermo di ricerca per i gruppi.

Nota: dopo aver configurato uno schermo di ricerca, è possibile utilizzarlo per qualsiasi attività per cercare un oggetto primario o secondario.

Filtri di ricerca

I filtri di ricerca circoscrivono gli oggetti restituiti dalla ricerca. Ad esempio, se l'oggetto è utenti, è possibile limitare la ricerca in modo che vengano trovati solo gli appaltatori. È possibile configurare un filtro per la ricerca degli utenti la cui opzione Tipologia dipendente sia Appaltatore.

Per le ricerche, è possibile configurare i seguenti campi:

Mostra solo oggetti che rispettano le regole seguenti

Consente di definire criteri aggiuntivi da combinare con il filtro definito dall'utente per limitare la ricerca.

Si noti quanto segue quando si utilizza questo campo:

- A causa dei limiti nelle ricerche dei ruoli di fornitura, con questi criteri vengono ignorati i campi dei filtri aventi lo stesso nome immessi dall'utente.
- Gli attributi utilizzati durante la configurazione di questo campo non devono essere indicati come campi di ricerca disponibili negli schermi di ricerca.

Ad esempio, quando si configura la schermata di ricerca in modo che visualizzi solo i ruoli dove l'attributo Abilitato è impostato su sì, è necessario rimuovere il suddetto attributo dall'elenco di attributi che l'utente può specificare nei criteri di ricerca.

In caso contrario, i criteri specificati dall'utente verranno ignorati.

Filtro di ricerca predefinito

Consente di definire un filtro che verrà visualizzato per impostazione predefinita quando un amministratore utilizza la schermata di ricerca. Ad esempio, se si configura una schermata di ricerca per l'attività Modifica appaltatore ed è risaputo che gli amministratori in genere cercano gli appaltatori in base al nome della società del contratto, è possibile impostare il filtro predefinito su Società contratto = *. Gli amministratori possono ignorare il filtro predefinito mediante l'impostazione di criteri di ricerca diversi. L'impostazione di un filtro predefinito consente di ottimizzare le prestazioni grazie alla definizione di un limite per il numero di risultati restituiti se un amministratore non specifica alcun filtro prima di avviare una ricerca.

Seleziona automaticamente tutti i risultati della ricerca con attività di selezione multipla

Consente di impostare la selezione di tutti i risultati di ricerca per impostazione predefinita. Se si seleziona questa casella di controllo, accanto al nome di tutti gli oggetti inclusi nell'elenco dei risultati della ricerca verrà visualizzata una casella selezionata.

Eseguire automaticamente la ricerca

Consente di specificare che un campo di ricerca verrà visualizzato insieme ai risultati della ricerca.

Imposta automaticamente l'oggetto della ricerca quando compare un solo risultato

Consente di impostare automaticamente l'oggetto primario dell'attività quando un solo oggetto corrisponde al filtro di ricerca impostato.

Si supponga, ad esempio, che questa opzione venga selezionata per una schermata di ricerca utenti associato all'attività Modifica utente. Se un amministratore apre l'attività Modifica utente e definisce un filtro di ricerca che restituisce un solo utente, in CA Identity Manager verrà aperta l'attività Modifica utente per tale utente. L'amministratore non dovrà pertanto selezionare l'utente per aprire l'attività Modifica utente.

Nota: affinché questa impostazione venga applicata, è necessario che anche Eseguire automaticamente la ricerca sia selezionato.

Salva filtro di ricerca

Consente di specificare che il filtro di ricerca per l'attività deve essere salvato per l'utente nella sessione corrente. Quando tale utente eseguirà un'altra ricerca all'interno dell'attività, verrà visualizzato il filtro di ricerca salvato.

Nota: CA Identity Manager salva il filtro di ricerca per la durata della sessione dell'utente. Quando l'utente si disconnette, il filtro di ricerca viene svuotato.

Cerca nell'organizzazione

Consente di visualizzare un filtro organizzazione nella schermata di ricerca. Se si seleziona questa casella di controllo, gli amministratori possono specificare un filtro per limitare le organizzazioni in cui eseguire la ricerca di un oggetto. È possibile specificare le impostazioni predefinite per il filtro di ricerca dell'organizzazione impostando una schermata di ricerca nel campo Ricerca organizzazione.

Salva organizzazione di ricerca

Consente di impostare il salvataggio dell'organizzazione per l'attività se per la ricerca è stata definita un'organizzazione. Quando viene eseguita la successiva ricerca all'interno dell'attività, verrà visualizzata l'organizzazione salvata.

Ricerca organizzazione

Consente di specificare la schermata di ricerca utilizzata in CA Identity Manager per consentire agli amministratori di ricercare un'organizzazione.

Ambito di ricerca organizzazione predefinito

Consente di specificare l'ambito di ricerca organizzazione predefinito che viene visualizzato quando un amministratore utilizza una schermata di ricerca. L'ambito di ricerca determina quali livelli della struttura dell'organizzazione verranno inclusi nella ricerca. Gli amministratori possono ignorare l'ambito di ricerca organizzazione predefinito specificando criteri di ricerca diversi nella schermata di ricerca.

Se ad esempio si configura una schermata di ricerca per un'attività Modifica appaltatore in un ambiente in cui le informazioni sugli appaltatori sono archiviate a vari livelli nella struttura dell'organizzazione, è possibile impostare l'ambito di ricerca organizzazione predefinito su E inferiore.

Ricerca singola espressione

Consente di definire il tipo di filtro di ricerca visualizzato nella schermata di ricerca. Se questa casella di controllo è selezionata, gli utenti possono specificare un unico filtro di ricerca, ad esempio <attributo><comparatore><valore>. Se questa casella di controllo non è selezionata, gli utenti possono specificare più filtri di ricerca. Ad esempio, <attributo1><comparatore><valore1> AND <attributo2><comparatore><valore2>. Nei risultati della ricerca verranno restituiti gli oggetti che soddisfano le condizioni di tutti i filtri. Nell'esempio precedente, nei risultati della ricerca verranno restituiti gli oggetti che includono <valore1> e <valore2>.

Ricerca solo segni di uguale

Impedisce agli amministratori di utilizzare operatori di ricerca diversi dai segni di uguale.

Visualizza numero risultati

Consente di visualizzare il numero dei risultati della ricerca corrispondenti. Quando questa casella di controllo è selezionata, per tutte le ricerche verrà restituito il messaggio "Sono presenti X risultati".

Aggiungi pulsante attività per <nome attività>

Consente di aggiungere un collegamento ad un'altra attività nella schermata di ricerca. Il collegamento viene visualizzato sotto forma di pulsante.

Questo campo in genere viene utilizzato per aggiungere un'attività di creazione ad una schermata di ricerca configurato per l'esplorazione oggetto-attività.

Etichetta facoltativa

Consente di specificare un'etichetta per l'attività selezionata nel campo precedente. Questa etichetta viene visualizzata sul pulsante dell'attività.

Aggiungi pulsante eliminazione multipla per <nome attività>

Consente di aggiungere un collegamento ad un'attività con cui gli amministratori possono selezionare più oggetti da eliminare. Il collegamento viene visualizzato sotto forma di pulsante.

Questo campo in genere viene utilizzato nell'esplorazione oggetto-attività.

Campi di ricerca e risultati della ricerca

Nell'altra parte della schermata di ricerca selezionare i campi che un amministratore può utilizzare in una query di ricerca ed i campi da visualizzare nei risultati della ricerca.

Seleziona i campi in cui può ricercare l'utente

Selezionare i campi che un amministratore può utilizzare per creare una query di ricerca.

Per aggiungere altri campi, selezionare i campi desiderati nella casella di riepilogo sottostante la tabella dei campi di ricerca.

Dopo aver selezionato i campi, è possibile modificare l'ordine in cui sono visualizzati utilizzando le icone raffiguranti una freccia su e una freccia giù a destra del campo.

Nota: se non viene specificato alcun campo in base al quale un amministratore può eseguire una ricerca, la ricerca verrà avviata automaticamente.

Seleziona i campi che compaiono nei risultati di ricerca

Selezionare i campi visualizzati da CA Identity Manager nei risultati della ricerca. È possibile selezionare i campi non disponibili nella query di ricerca.

Per aggiungere altri campi, selezionare i campi desiderati nella casella di riepilogo sottostante la tabella dei campi di ricerca.

Stile

Quando viene selezionato un campo da visualizzare nei risultati della ricerca, è possibile selezionare una delle seguenti opzioni di stile:

■ Nome booleano visualizzato

Consente di visualizzare il nome del campo per tutti i risultati che restituiscono True. Se, ad esempio, si immette Attivato come nome dell'attributo che indica lo stato di un account utente, "Attivato" verrà visualizzato nei risultati delle ricerche di tutti gli account utente attivi.

■ Segno di spunta

Consente di visualizzare il valore come segno di spunta selezionato in base al valore dell'attributo. Se, ad esempio, si seleziona lo stile Segno di spunta per rappresentare lo stato Attivato/Disattivato degli account utente, in CA Identity Manager viene visualizzato un segno di spunta selezionato per tutti gli account attivi.

- **Stringa multivalore**

Consente di visualizzare i valori di un attributo multivalore su righe distinte. I valori sono elencati in ordine alfabetico.

- **Casella di controllo di sola lettura**

Consente di visualizzare il valore come una casella di controllo di sola lettura.

- **Stringa**

Consente di visualizzare il valore come stringa di testo.

■ **Attività**

Consente di aggiungere un elenco di attività ad un campo. Sarà necessario fare clic su un'icona raffigurante una freccia per visualizzare l'elenco delle attività eseguibili sull'oggetto associato al campo di ricerca. Se, ad esempio, si aggiunge un elenco di attività ad un campo Cognome nei risultati della ricerca, sarà possibile fare clic sulla freccia in tale campo per visualizzare l'elenco delle attività eseguibili sull'utente selezionato.

Questa impostazione è utilizzabile anche per visualizzare un valore di attributo come collegamento a un'attività.

Se si seleziona lo stile Attività, accanto alla colonna Stile viene visualizzata un'icona raffigurante una freccia a destra. Fare clic sulla freccia per visualizzare la finestra di dialogo Proprietà campo. Utilizzare questa finestra di dialogo per configurare un elenco di attività.

■ **Elenco attività**

Consente di aggiungere ulteriori attività che gli utenti possono eseguire sugli oggetti nelle schermate di ricerca ed elenco. Ad esempio, è possibile configurare la schermata di ricerca per l'attività Modifica utente per consentire agli utenti di eseguire un'attività, ad esempio la disabilitazione di un utente a partire dall'elenco utenti restituito dalla ricerca.

Quando si seleziona questa opzione, si determina se gli utenti possono accedere all'attività facendo clic su un'icona o di un collegamento di testo.

■ **Menu attività**

Consente di aggiungere ulteriori attività (in modo simile allo stile dell'elenco attività) come voci di menu popup.

Quando si seleziona questa opzione, il pulsante Azione viene visualizzato accanto a ogni oggetto in una ricerca o una schermata elenco. Per visualizzare l'elenco delle attività che è possibile eseguire per un oggetto, è necessario fare clic sul pulsante Azione corrispondente.

Nota: per visualizzare le opzioni di stile dell'elenco attività e del menu attività, selezionare (Separatore) quando si aggiunge un campo nella tabella dei risultati di ricerca. Per ulteriori informazioni sull'aggiunta di attività aggiuntive alle schermate di ricerca ed elenco, consultare la *guida relativa alla progettazione della console utente*.

Ordinabile

Selezionare questa casella di controllo per consentire agli amministratori di ordinare i risultati della ricerca in base a uno o più campi.

Imposta ordine predefinito per i risultati di ricerca

Consente di specificare l'ordine in base al quale i risultati della ricerca vengono visualizzati. I risultati della ricerca vengono inizialmente ordinati in base al primo campo dell'elenco, quindi in base a ciascun campo aggiuntivo nell'ordine di visualizzazione dei campi. Selezionare la casella di controllo Decrescente per ordinare i risultati in ordine decrescente.

Seleziona oggetti con modifiche al campo *nome campo*

Consente di specificare che gli oggetti in cui il campo specificato è cambiato devono essere selezionati quando l'utente fa clic sul pulsante Seleziona.

Restituisci *N* risultati per pagina

Consente di selezionare il numero di risultati da visualizzare per pagina. Se i risultati della ricerca superano il numero specificato, CA Identity Manager visualizza un collegamento a ogni pagina dei risultati.

Guida definita dall'utente negli schermi di ricerca

Per aggiungere testo personalizzato agli schermi di ricerca, è possibile definire il testo desiderato nella casella di testo HTML corrispondente. È possibile aggiungere testo nelle seguenti aree:

- Inizio o fine della pagina
- Prima o dopo la creazione
- Prima o dopo i risultati

Tipi di schermi di ricerca

In Identity Manager sono disponibili i seguenti schermi di ricerca preconfigurati.

Schermata di ricerca del ruolo di accesso

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare i ruoli di accesso che soddisfano i criteri specificati.

Schermata di ricerca attività di accesso

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare le attività di accesso che soddisfano i criteri specificati. Questa schermata di ricerca viene utilizzato per trovare un'attività di accesso da visualizzare o modificare, oppure per aggiungere un'attività ad un ruolo di accesso.

Schermata di ricerca ruolo amministrazione

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare i ruoli di amministrazione che soddisfano i criteri specificati.

Schermata di ricerca attività di amministrazione

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare le attività di amministrazione che soddisfano i criteri specificati. Questa schermata di ricerca viene utilizzato per trovare un'attività di amministrazione da visualizzare o modificare, o per aggiungere un'attività ad un ruolo di amministrazione.

Schermata di ricerca di approvazione

In questa schermata è possibile configurare la visualizzazione della parte superiore di un'attività di approvazione.

Schermata di ricerca utente certificazione iniziale

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare gli utenti per i quali impostare la certificazione obbligatoria. Per gli utenti selezionati, il relativo stato di certificazione verrà impostato su *Certificazione richiesta*.

Schermata di ricerca certificazione utente

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare gli utenti che richiedono la certificazione.

Schermata di ricerca delega

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare altri utenti da aggiungere come delegati. Un delegato è un utente diverso a cui è possibile concedere temporaneamente il permesso di visualizzare e risolvere gli elementi inclusi nel proprio flusso di lavoro.

Schermata di ricerca attivazione/disattivazione utente

In questa schermata è possibile configurare i filtri di ricerca necessari per attivare/disattivare gli utenti che soddisfano i criteri specificati.

Schermata di ricerca utente certificazione finale

In questa schermata è possibile configurare i filtri di ricerca necessari per individuare gli utenti il cui ciclo di certificazione deve essere completato.

Schermata di ricerca contratto di licenza utente finale

In questa schermata è possibile configurare l'attività Registrazione automatica utilizzando una pagina che sarà specifica dell'applicazione basata sull'identità.

Ricerca esplora e correla

In questa schermata è possibile configurare i filtri di ricerca necessari per le definizioni di esplorazione e correlazione che soddisfano i criteri di ricerca specificati.

Ricerca caricamento file alimentatore

In questa schermata è possibile cercare il file alimentatore da caricare. Un file alimentatore consente di automatizzare l'esecuzione di azioni ripetute su un numero elevato di oggetti gestiti.

Schermata di ricerca password dimenticata/Schermata di ricerca ID utente dimenticato

In questa schermata è possibile configurare l'attività Password dimenticata per richiedere agli utenti le informazioni di verifica dell'identità.

Schermata di ricerca gruppi

In questa schermata è possibile configurare i filtri di ricerca necessari per i gruppi, ad esempio i gruppi all'interno dell'organizzazione finanziaria.

Schermata di ricerca set di criteri di identità

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare i set di criteri di identità che soddisfano i criteri specificati.

Schermata di ricerca gestore attributo logico

In questa schermata è possibile configurare i filtri di ricerca necessari per cercare i gestori degli attributi logici. Questa schermata di ricerca viene utilizzato per trovare un gestore degli attributi logici e visualizzarne o modificarne la configurazione.

Schermata di ricerca gestione rapporti

In questa schermata è possibile configurare i filtri di ricerca necessari per cercare un rapporto da visualizzare o eliminare.

Schermata di ricerca utenti non certificati

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare gli utenti non ancora certificati alla fine del periodo di certificazione.

Schermata di ricerca organizzazione

In questa schermata è possibile configurare i filtri di ricerca necessari per limitare la scelta delle organizzazioni solo a determinate organizzazioni secondarie.

Fornitura schermata di ricerca del ruolo

In questa schermata è possibile configurare i filtri di ricerca necessari per recuperare i ruoli di fornitura.

Schermata di ricerca modelli di account

In questa schermata è possibile configurare i filtri di ricerca necessari per recuperare i modelli di account.

Schermata di ricerca criteri di password

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare i criteri di password che soddisfano i criteri specificati.

Schermata di ricerca definizione snapshot

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare una definizione di snapshot da visualizzare, modificare o eliminare.

Schermata di ricerca standard

In questa schermata è possibile configurare i filtri per trovare gli oggetti gestiti personalizzati.

Schermata di ricerca utente

In questa schermata è possibile configurare i filtri di ricerca necessari per trovare gli utenti che soddisfano i criteri specificati. Ad esempio, è possibile cercare gli utenti che sono appaltatori.

Dopo aver completato la scheda Ricerca, scegliere le schede per l'attività.

Selezione delle schede per l'attività

Nella scheda Schede denominare e configurare le schede. Ciascuna scheda contiene un gruppo di campi da includere nell'attività. È possibile includere schede predefinite oppure crearne di nuove. Ad esempio, nella scheda Modifica utente sono disponibili le seguenti schede:

- Profilo
- Ruoli di accesso
- Ruoli di amministrazione
- Gruppi
- Delega elementi di lavoro

Per modificare la definizione di una scheda, fare clic sull'icona di modifica () accanto al nome della scheda desiderata.

Ulteriori informazioni:

[Schede Account](#) (a pagina 61)

[Scheda Pianificazione](#) (a pagina 63)

Schede Account

In genere, la scheda Account viene aggiunta alle attività che consentono di visualizzare o modificare un utente.

Dettagli account

Fare clic su un nome account per eseguire un'azione.

Seleziona	Nome	Tipo di endpoint	Endpoint	Sospeso	Bloccato
☒	 ken	Window NT	IM-term	Attivo	Sbloccato

Crea account

Azioni per gli account selezionati

Aggiorna account	Sospendi	Riprendi	Sblocca	Modifica password
Annulla assegnazione	Assegna	Elimina		

Se la scheda Account viene aggiunta ad un'attività Modifica utente, gli amministratori potranno eseguire altre azioni sugli account degli utenti. Ad esempio:

- Sospendere o riattivare un account.
- Sbloccare un account bloccato automaticamente a causa di un accesso incorretto o non autorizzato. Ad esempio, è possibile che un account venga bloccato quando un utente supera il numero massimo di accessi non riusciti consentiti dal criterio di password di CA Identity Manager.
- Modificare la password per uno o più account utente.
- Assegnare o annullare l'assegnazione di account agli utenti.

Per ulteriori informazioni sulle altre opzioni disponibili nella scheda Account, consultare l'argomento Configurazione account della Guida in linea della console utente.

Prerequisiti per l'utilizzo della scheda Account.

Per utilizzare la scheda Account, è necessario configurare il supporto del provisioning in CA Identity Manager. L'ambiente dovrà inoltre includere una directory di provisioning.

Nota: per configurare il supporto di provisioning per un ambiente, consultare la *Guida alla configurazione*.

Campi della scheda Account

Nella scheda Account vengono visualizzati i dettagli relativi agli account di cui l'utente dispone nei sistemi di endpoint.

Di seguito vengono descritti i principali campi disponibili.

- Nome: nome di accesso, nome di posta elettronica o altro nome associato all'account.
- Tipo di endpoint: tipo di endpoint, ad esempio una directory LDAP, associata all'account.
- Endpoint: endpoint specifico associato all'account.
- Sospeso: uno dei tre possibili stati.
 - Attivo: se l'account è abilitato.
 - Sospeso: se l'account è disabilitato.
 - Attivazione in sospeso (manuale): se l'account non può essere riattivato né sospeso. Per riattivare o sospendere l'account è necessario accedere al sistema di endpoint.
 - Non disponibile viene visualizzato se lo stato non è reperibile perché è impossibile comunicare con l'endpoint.
- Bloccato: visualizzato se l'account è bloccato. Il blocco si verifica quando un utente effettua diversi tentativi di accesso all'account con la password sbagliata. Non disponibile viene visualizzato se lo stato non è reperibile perché è impossibile comunicare con l'endpoint.

Funzioni aggiuntive disponibili nella scheda Account

Quando la scheda Account viene inclusa in un'attività di modifica di un utente, gli amministratori possono utilizzare tale attività per eseguire funzioni specifiche sull'account degli utenti. Le funzioni disponibili vengono definite mediante la configurazione della scheda.

È possibile selezionare le funzioni disponibili mediante l'utilizzo dell'attività Modifica attività di amministrazione su un'attività utente contenente la scheda Account. La scheda Account viene modificata per determinare se funzioni quali, ad esempio, Assegna account e Annulla assegnazione account, sono disponibili nella scheda.

Nota: per ulteriori informazioni, consultare la scheda Configurazione account della Guida in linea.

Scheda Pianificazione

La pianificazione consente di posticipare l'esecuzione automatica di un'attività ad una data futura. Se si pianifica un'attività associata ad un flusso di lavoro, CA Identity Manager esegue tutte le attività in base alla loro definizione inclusa nel flusso di lavoro specifico. Lo stato delle attività pianificate viene visualizzato nella pagina Visualizza attività inoltrate.

Un'attività pianificata non ancora eseguita da CA Identity Manager può essere annullata utilizzando la pagina Visualizza attività inoltrate.

Nota: se un'attività pianificata viene annullata e successivamente inoltrata nuovamente, l'attività viene eseguita immediatamente, a prescindere dall'orario di esecuzione pianificato.

In CA Identity Manager è disponibile un'utilità di pianificazione sotto forma di scheda speciale. Per accedere a tale utilità, è necessario configurare un'attività mediante la scheda Pianificazione.

Aggiunta della scheda Pianificazione ad un'attività di amministrazione

CA Identity Manager consente di pianificare l'esecuzione delle attività ad una data ed ora specifiche. Per pianificare un'attività, è necessario aggiungere la scheda Pianificazione ad un'attività di amministrazione.

Nota: non è possibile aggiungere una scheda Pianificazione a tutte le attività di amministrazione in CA Identity Manager. Se un'attività specifica non può essere pianificata, la scheda Pianificazione non sarà disponibile nella schermata Modifica attività di amministrazione.

Per aggiungere la scheda Pianificazione ad un'attività di amministrazione

1. Fare clic su Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
Verrà visualizzata la pagina Selezionare attività di amministrazione.
2. Selezionare Nome o Categoria nel campo dove, quindi immettere la stringa da ricercare e fare clic su Cerca.
In CA Identity Manager vengono visualizzate le attività di amministrazione che soddisfano i criteri di ricerca.
3. Scegliere un'attività di amministrazione e fare clic su Seleziona.
CA Identity Manager visualizza i dettagli relativi all'attività di amministrazione selezionata.
4. Fare clic su Schede.
Verranno visualizzate le schede configurate per l'attività di amministrazione selezionata.

5. Nell'elenco a discesa delle attività selezionare la pianificazione da visualizzare nella scheda, quindi fare clic su .

La scheda Pianificazione viene aggiunta all'elenco di schede visualizzate nell'attività di amministrazione selezionata.

6. Fare clic su Inoltra.

La scheda Pianificazione viene aggiunta all'attività di amministrazione selezionata.

Visualizzazione di campi nell'attività

Nella scheda Campi vengono visualizzati i campi validi per l'attività corrente. Tali campi corrispondono ai campi creati nelle schede per l'attività corrente. Per modificare i campi utilizzati, tornare alla scheda Schede, quindi selezionare la scheda da modificare.

Dopo aver completato questa scheda, procedere al passaggio [Assegnazione di processi del flusso di lavoro per gli eventi](#) (a pagina 64).

Tuttavia, se nell'ambiente Identity Manager corrente non viene utilizzato il flusso di lavoro, a questo punto è possibile fare clic su Inoltra. Verrà visualizzato un messaggio indicante che l'attività è stata completata. Se l'attività è stata completata correttamente, è possibile aggiungere l'attività al ruolo in modo tale che i membri di tale ruolo possano iniziare ad utilizzarla.

Visualizzazione utilizzo ruolo

Nella scheda Utilizzo ruolo è possibile visualizzare i ruoli che includono l'attività che si sta visualizzando o modificando.

I proprietari dei ruoli possono aggiungere e rimuovere attività dai ruoli.

Nota: in Ruoli di amministrazione predefiniti è riportato l'elenco di attività dei ruoli di amministrazione che vengono installati con CA Identity Manager per impostazione predefinita.

Assegnazione di processi del flusso di lavoro per gli eventi

Se per l'ambiente Identity Manager corrente viene abilitato il flusso di lavoro, utilizzare la scheda Eventi per selezionare un processo del flusso di lavoro per ogni evento avviato dall'attività. Il processo del flusso di lavoro selezionato ignorerà quello selezionato per impostazione predefinita nella console di gestione di Identity Manager.

Per ulteriori informazioni sui mapping predefiniti del flusso di lavoro, vedere il capitolo relativo alle impostazioni avanzate della *Guida alla configurazione*.

Per completare la creazione dell'attività, fare clic su **Inoltra**. Verrà visualizzato un messaggio indicante che l'attività è stata completata. Se l'attività è stata completata correttamente, è possibile aggiungere l'attività al ruolo in modo tale che i membri di tale ruolo possano iniziare ad utilizzarla.

Gestione di un archivio utenti di Active Directory

Se Active Directory è l'archivio utenti, prima di creare le attività di amministrazione, è necessario configurare alcune funzionalità di Active Directory.

Attributo sAMAccountName

L'attributo sAMAccountName è valido per utenti e gruppi. Questo attributo è obbligatorio e deve essere incluso negli schermi delle attività utilizzare per creare utenti e gruppi.

Nota: durante la creazione di utenti, il valore dell'attributo sAMAccountName non può superare 20 caratteri. Questa limitazione non è valida per i gruppi.

È possibile scrivere un gestore personalizzato di attributi logici che generi automaticamente un valore univoco per l'attributo sAMAccountName quando viene creato un utente o un gruppo. In questo caso, l'attributo sAMAccountName può essere incluso come campo nascosto negli schermi **Crea utente** e **Crea gruppo**.

Per ulteriori informazioni, vedere il capitolo relativo agli attributi logici nella *Guida alla programmazione per Java*.

Tipo di gruppo e ambito

In Active Directory sono disponibili due tipi di gruppi:

- **Protezione:** disponibile negli elenchi di controllo di accesso (ACL), che determinano le autorizzazioni per risorse ed oggetti.
- **Distribuzione:** utilizzato per raggruppare gli oggetti, ad esempio utenti e gruppi. I gruppi di distribuzione non possono essere utilizzati per concedere privilegi in Active Directory.

Ogni tipo di gruppo dispone di un ambito che determina quanto segue:

- Percorso membri: posizione in cui si trovano i membri
- Autorizzazioni: posizione in cui è possibile utilizzare il gruppo per i privilegi di accesso, se il gruppo è un gruppo di protezione
- Appartenenza al gruppo in altri gruppi: posizione dei gruppi a cui il gruppo appartiene

Ogni tipo di ruolo può essere associato ad uno degli ambiti descritti nella seguente tabella.

Ambito	Percorso membri	Autorizzazioni	Appartenenza al gruppo in altri gruppi
Universale	I membri del gruppo possono essere gruppi universali, gruppi globali ed utenti di qualsiasi dominio dell'insieme di strutture.	Utilizzabile per concedere l'accesso in qualsiasi dominio di un insieme di strutture.	Possono essere membri dei gruppi locali al dominio o universali in qualsiasi dominio di un insieme di strutture.
Globale	I membri del gruppo possono essere gruppi globali ed utenti dello stesso dominio del gruppo.	Utilizzabile per concedere l'accesso in qualsiasi dominio di un insieme di strutture.	Possono essere membri dei gruppi globali, locali al dominio o universali in qualsiasi dominio di un insieme di strutture.
Locale al dominio	I membri del gruppo possono essere gruppi universali, gruppi globali ed utenti di qualsiasi dominio dell'insieme di strutture. I membri possono inoltre essere gruppi locali al dominio dello stesso dominio.	Utilizzabile solo per concedere l'accesso al dominio in cui si trova il gruppo.	Possono solo essere membri di altri gruppi locali al dominio all'interno del dominio.

Il tipo di gruppo e l'ambito non sono attributi obbligatori. Tuttavia, se il tipo di gruppo e l'ambito non vengono specificati, Active Directory crea un gruppo di protezione con ambito globale.

Per creare gruppi di tipo diverso, è possibile creare un gestore di attributi logici personalizzati. Per ulteriori informazioni, vedere il capitolo relativo agli attributi logici nella *Guida alla programmazione per Java*.

Dopo aver configurato queste funzionalità di Active Directory, procedere al passaggio Creazione di un'attività di amministrazione.

Attività esterne per le funzioni dell'applicazione

Un'attività esterna:

- Consente a un amministratore di eseguire una funzione in un'applicazione diversa da CA Identity Manager dalla console utente
- Facoltativamente passa le informazioni all'applicazione per generare attività specifiche per utenti, gruppi o organizzazioni.

Ad esempio, un'attività esterna può passare informazioni su un'organizzazione ad un'applicazione che genera gli ordini di acquisto. L'amministratore che esegue l'attività può visualizzare gli ordini di acquisto aperti relativi all'organizzazione dalla console utente.

È possibile visualizzare attività esterne aprendo l'applicazione in una nuova finestra del browser, o visualizzandole come schede in un'attività di amministrazione CA Identity Manager.

Per le attività esterne sono disponibili due schede. Tali schede vengono configurate allo stesso modo, anche se sono caratterizzate da un funzionamento diverso.

- La scheda esterna è una scheda visiva, ovvero viene visualizzato il contenuto dell'URL all'interno di una scheda.
- La scheda URL esterno non è una scheda visiva, ovvero l'attività viene reindirizzata all'URL immesso.

Scheda esterna

È possibile aggiungere una scheda esterna a qualsiasi attività di creazione, visualizzazione o modifica per trasformarla in un'attività esterna. Ad esempio, se si aggiunge una scheda esterna a un'attività Crea utente, la scheda viene visualizzata in tale attività.

Per la scheda esterna:

- Non vengono generati eventi per un'attività esterna.
- Facoltativamente, è possibile utilizzare oggetti gestiti.

- Nel campo URL esterno, è possibile specificare l'indirizzo dell'applicazione sotto forma di:
 - Indirizzo completo, compreso il nome di dominio completo, ad esempio:
`http://server1.mycompany.org/report/viewUserReport`
 - Percorso relativo, ad esempio:
`/report/viewUserReport`

Se viene specificato il percorso relativo, in CA Identity Manager il nome di dominio completo del server di installazione di CA Identity Manager viene aggiunto automaticamente.
- Configurare gli attributi per passare all'applicazione sulla scheda Profilo.
- È possibile includere o escludere il DN amministratore o il nome dell'attività nell'URL.

Scheda URL esterno

È possibile aggiungere una scheda URL esterno a un'attività di visualizzazione, come ad esempio Visualizza utente. Quando si utilizza l'attività Visualizza utente, l'utente viene reindirizzato al sito Web identificato dall'URL. Nessuna altra scheda è visibile.

Per una scheda URL esterno:

- La scheda URL esterno deve essere l'unica scheda dell'attività. Se altre schede sono associate alla stessa attività, la scheda esterna non reindirizzerà gli utenti all'URL specificato.
- L'attività può generare eventi che è possibile verificare.
- Nel campo URL esterno, è possibile specificare l'indirizzo dell'applicazione sotto forma di:
 - Indirizzo completo, compreso il nome di dominio completo, ad esempio:
`http://server1.mycompany.org/report/viewUserReport`
 - Percorso relativo, ad esempio:
`/report/viewUserReport`

Se viene specificato il percorso relativo, in CA Identity Manager il nome di dominio completo del server di installazione di CA Identity Manager viene aggiunto automaticamente.

- Facoltativamente, è possibile utilizzare oggetti gestiti.
- È possibile configurare gli attributi da trasmettere all'URL.
Fornire un URL per l'applicazione che si intende avviare e includere gli attributi che si desidera trasmettere all'applicazione.
- È possibile includere o escludere il DN amministratore o il nome dell'attività nell'URL.

Componenti di attività avanzati

I componenti di attività avanzati consentono di specificare l'elaborazione personalizzata per un'attività:

- La convalida a livello di attività permette di convalidare un valore di attributo con altri attributi nell'attività. Ad esempio, è possibile convalidare la correttezza del prefisso di un numero di telefono fornito dall'utente per la città e lo stato dell'utente.
- I [gestori attività di logica aziendale](#) (a pagina 69) eseguono una logica aziendale personalizzata prima che un'attività di CA Identity Manager venga inoltrata per l'elaborazione. Generalmente, la logica aziendale personalizzata convalida i dati. Ad esempio, un gestore attività di logica aziendale può controllare il limite di appartenenza a un gruppo prima che CA Identity Manager aggiunga un nuovo membro al gruppo. Se il limite di appartenenza al gruppo viene raggiunto, il gestore attività di logica aziendale mostra un messaggio per informare l'amministratore del gruppo che è impossibile aggiungere il nuovo membro.

Creazione di gestori delle attività di logica aziendale

Definire il nome completo di classe di un gestore delle attività di logica aziendale nel modo di seguito descritto:

1. Creare o modificare un'attività di amministrazione.
2. Nella scheda Profilo di amministrazione fare clic su Gestori attività di logica aziendale.

Viene visualizzato lo schermo Gestori attività di logica aziendale. In questo schermo sono elencati i gestori delle attività di logica aziendale esistenti assegnati all'attività. Identity Manager esegue i gestori nell'ordine in cui sono visualizzati nell'elenco.

3. Fare clic su Aggiungi.

Viene visualizzato lo schermo Informazioni sul gestore dell'attività di logica aziendale.

Utilizzare lo schermo Informazioni sul gestore dell'attività di logica aziendale per definire le seguenti informazioni relative al gestore dell'attività di logica aziendale che si sta assegnando all'attività:

Nome

Nome che si sta assegnando al gestore dell'attività di logica aziendale.

Descrizione

Descrizione facoltativa del gestore dell'attività di logica aziendale.

Classe Java

Se il gestore dell'attività di logica aziendale viene implementato in Java, corrisponde al nome di classe completo del gestore, ad esempio:

`com.mycompany.MyJavaValidator`

Identity Manager prevede che il file delle classi si trovi nella directory principale definita per i file delle classi Java personalizzati. Per informazioni sulla distribuzione dei file delle classi Java, vedere la *Guida alla programmazione per Java*.

Nome file JavaScript

Se il gestore dell'attività di logica aziendale viene implementato in JavaScript e il codice JavaScript è incluso in un file, specificare il nome del file in questo campo. Ad esempio, è possibile inserire il codice JavaScript in un file se il gestore dell'attività di logica aziendale deve essere utilizzato da più schermi di attività.

Identity Manager prevede che il file si trovi nella directory principale definita per i file JavaScript personalizzati. Per informazioni sulla distribuzione dei file JavaScript, vedere la *Guida alla programmazione per Java*.

Se si archivia il file in una sottodirectory della directory principale, includere il nome della sottodirectory quando si specifica il nome del file JavaScript, ad esempio:

`JavaScriptSubDir\MyJavaScriptBLTH.js`

Le barre devono essere corrette per la piattaforma in cui viene distribuito il file JavaScript.

JavaScript

È possibile implementare un gestore dell'attività di logica aziendale JavaScript immettendo il codice JavaScript completo in questo campo anziché in un file. Ad esempio, è possibile immettere il codice JavaScript in questo campo se lo script è molto breve oppure se non deve essere utilizzato con altri schermi di attività.

Proprietà e Valore

Con le implementazioni Java questi campi sono coppie di dati nome/valore facoltative passate al metodo `init()` del gestore dell'attività di logica aziendale Java in modo che vengano utilizzate nei modi richiesti dal gestore stesso.

Per aggiungere una proprietà definita dall'utente, specificare il nome e il valore della proprietà, quindi fare clic su **Aggiungi**.

Nota: se si aggiunge un gestore dell'attività di logica aziendale Java, riavviare il server delle applicazioni per caricare il gestore.

Eventi ed attività di amministrazione

Le attività di amministrazione includono *eventi*, ovvero azioni eseguite da CA Identity Manager per completare un'attività specifica. Un'attività può includere più eventi. Ad esempio, l'attività **Crea utente** può includere eventi che comportano la creazione del profilo dell'utente, la sua aggiunta a un gruppo e l'assegnazione di ruoli.

CA Identity Manager controlla gli eventi, applica regole aziendali specifiche del cliente associate agli eventi e, quando viene eseguito il mapping degli eventi sui processi del flusso di lavoro, richiede l'approvazione per gli eventi.

Se per un'attività vengono generati più eventi e tali eventi sono mappati sui processi del flusso di lavoro, è necessario completare tutti i processi del flusso di lavoro prima che l'attività possa essere completata in CA Identity Manager.

Eventi primari e secondari

In generale gli eventi sono indipendenti gli uni dagli altri. Alcune attività sono tuttavia associate a un evento primario e a uno o più eventi secondari:

- Se l'evento primario non riesce, tutti i relativi eventi secondari vengono automaticamente rifiutati. Ad esempio, se `CreateUserEvent` non riesce, è inutile che venga seguito da `AddToGroupEvent` per l'utente. Viene inoltre annullata l'attività associata.
- Se non riesce un evento secondario, ciò non influisce sulla riuscita di altri eventi eseguiti per l'attività o sull'esecuzione dell'attività in sé. Ad esempio, in un'attività **Crea utente**, `AddToGroupEvent` può essere rifiutato, ovvero non è possibile aggiungere l'utente a un determinato gruppo, ma è tuttavia possibile creare l'utente (`CreateUserEvent`) e assegnarlo a ruoli di fornitura (`AssignProvisioningRoleEvent`), nonché aggiungerlo ad altri gruppi.

Visualizzazione degli eventi di un'attività

È possibile visualizzare gli eventi associati a un'attività nella console utente di CA Identity Manager.

Visualizzazione degli eventi di un'attività

1. Nella console utente, selezionare Ruoli e attività, Visualizza attività di amministrazione.
2. Cercare e selezionare l'attività desiderata.
3. Selezionare la scheda Eventi.

Vengono visualizzati gli eventi associati all'attività corrente.

Eventi generati per i profili non modificati

Gli oggetti utente, gruppo e organizzazione contengono una serie di attributi fisici memorizzati nella directory utente. Se un attributo fisico di tali oggetti viene modificato in una scheda profilo, Identity Manager genera un evento Modify... anche dopo che l'utente inoltra l'attività. Se ad esempio un attributo *Titolo* viene modificato in una scheda Profilo utente, Identity Manager genera l'evento ModifyUserEvent.

Se un oggetto utente, gruppo oppure organizzazione è rappresentato in una scheda profilo ma nessun attributo fisico è stato modificato quando l'utente fa clic su Inoltra, Identity Manager non genera un evento Modify... bensì un corrispondente evento View..., ovvero:

- ViewUserEvent viene generato invece di ModifyUserEvent
- ViewGroupEvent viene generato invece di ModifyGroupEvent
- ViewOrganizationEvent viene generato invece di ModifyOrganizationEvent

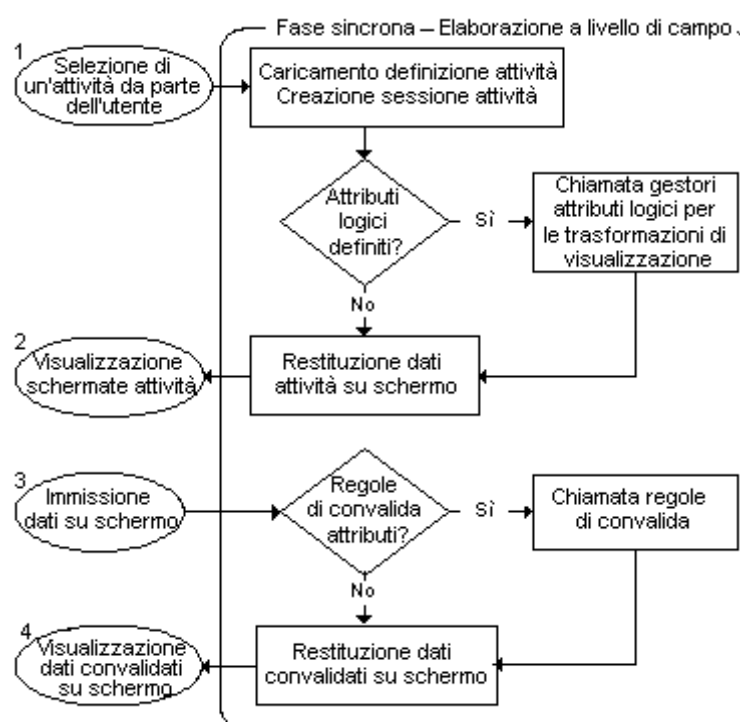
Elaborazione dell'attività di amministrazione

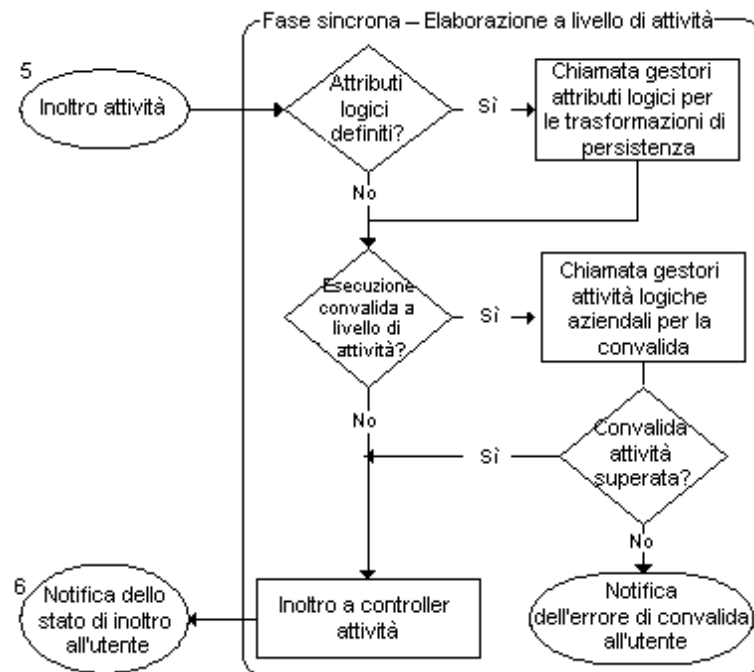
Il tempo necessario per l'elaborazione di un'attività dipende dal numero di passaggi richiesti. Quando un'attività viene inoltrata per l'elaborazione, in CA Identity Manager vengono eseguiti i seguenti passaggi:

1. In CA Identity Manager vengono convalidati i dati inoltrati.
Questa fase è denominata *fase sincrona*.
2. Se è richiesta l'approvazione, l'attività in CA Identity Manager viene inviata al motore del flusso di lavoro.
 - a. Il motore del flusso di lavoro determina i revisori, quindi inserisce l'attività di approvazione nei rispettivi elenchi di lavori.
 - b. Facoltativamente, da CA Identity Manager viene inviato un messaggio di posta elettronica per comunicare l'elemento di lavoro in sospeso ai revisori.
 - c. Un revisore riserva l'elemento di lavoro, rimuovendolo dall'elenco di lavoro di altri revisori, e lo approva o rifiuta.
 - d. Facoltativamente, da CA Identity Manager viene inviato un messaggio di posta elettronica per comunicare lo stato dell'attività agli altri utenti interessati.
Questa fase è denominata *fase asincrona*.
3. L'attività viene quindi eseguita in CA Identity Manager, se non è stata rifiutata.

Elaborazione della fase sincrona

Durante la fase sincrona vengono trasformati e convalidati i dati immessi dagli utenti negli schermi delle attività, quindi viene applicata la logica aziendale a tali dati prima che l'attività venga inviata per l'elaborazione. Nel diagramma seguente è fornita una descrizione di alto livello di ciò che accade durante questa fase.

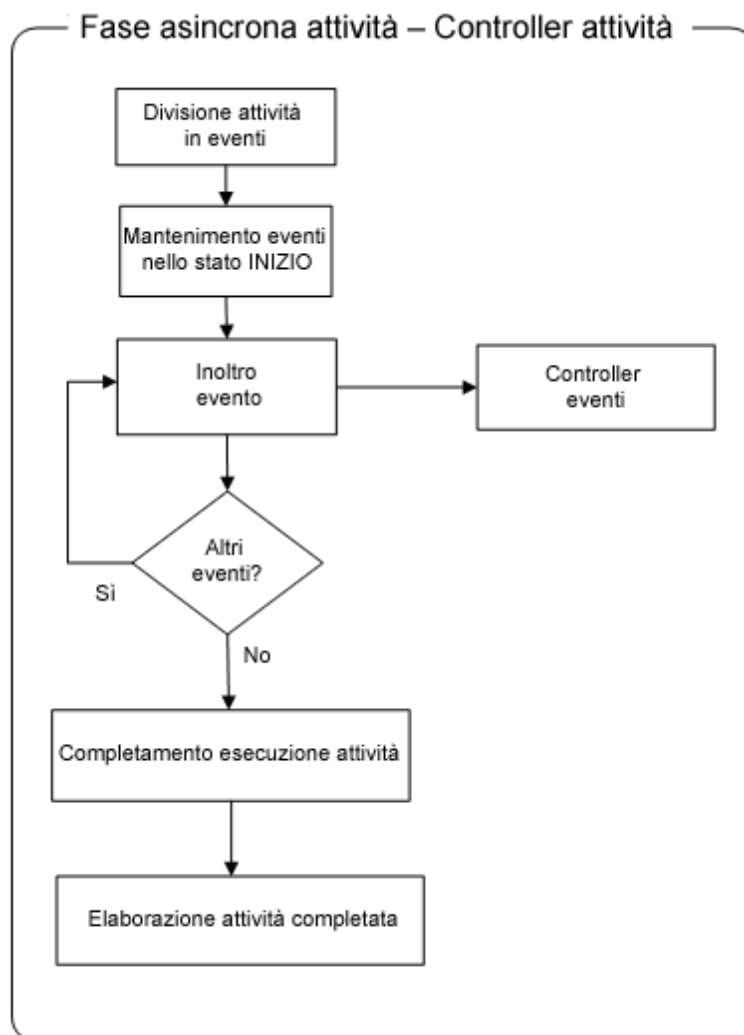




Elaborazione della fase asincrona

Al termine della fase sincrona, l'attività passa alla fase asincrona per l'esecuzione. Durante questa fase, un'attività genera uno o più eventi. Può trattarsi di eventi definiti dall'utente, ad esempio la creazione di un profilo utente o l'aggiunta di un utente a un gruppo, o di eventi generati dal sistema, ad esempio la scrittura di informazioni nel registro di controllo.

Il controller di attività, un componente del server di Identity Manager, è responsabile del ciclo di vita di un'attività e dei relativi eventi, come mostrato nella figura che segue:



Per la maggior parte degli eventi, il ciclo di vita, l'esecuzione e le azioni sono indipendenti da altri eventi. (La creazione di attività richiede l'esecuzione dell'evento di creazione dell'oggetto principale prima degli eventi secondari).

In genere, un evento attraversa i seguenti stati:

- Begin (Inizio)
- Pending (In attesa)
- Approved (Approvato)
- Esegui
- Completato
- Post (Invia)

Nota: in Identity Manager sono disponibili hook, denominati listener di eventi, che restano "in ascolto" in attesa di uno specifico evento o gruppo di eventi. Quando si verifica l'evento, il listener di eventi esegue la logica aziendale personalizzata appropriata per l'evento e lo stato dell'evento corrente. È possibile utilizzare l'API del listener di eventi per scrivere listener di eventi personalizzati. Per ulteriori informazioni, consultare la *Programming Guide for Java*.

Immagini per Attività di amministratore

È possibile creare immagini da utilizzare per le attività di amministrazione che si collocano nella pagina principale.

Capitolo 4: Amministratori e utenti

Questa sezione contiene i seguenti argomenti:

[Creazione di amministratori](#) (a pagina 79)

[Creazione di utenti](#) (a pagina 83)

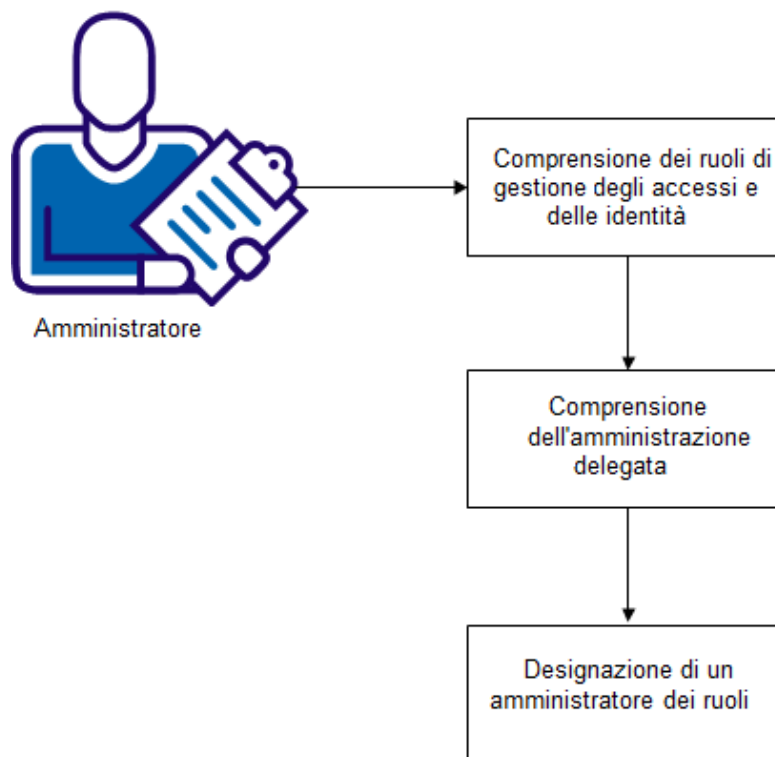
[Procedura per consentire agli utenti la registrazione automatica](#) (a pagina 88)

Creazione di amministratori

È possibile essere interamente responsabili della concessione di tutti ruoli agli utenti del sistema. È inoltre possibile condividere il compito di assegnazione dei ruoli designando amministratori aggiuntivi. Questo approccio viene chiamato *amministrazione delegata*.

Nel diagramma seguente sono illustrate le informazioni e i passaggi utili per la creazione di amministratori aggiuntivi.

Creazione di amministratori aggiuntivi



Gli argomenti seguenti descrivono la procedura per la creazione di amministratori aggiuntivi:

- [Ruoli per la gestione di identità o accessi](#) (a pagina 18)
- [Amministrazione delegata](#) (a pagina 80)
- [Designazione di un amministratore di ruolo](#) (a pagina 81)

Ruoli per la gestione di identità o accessi

Per abilitare la gestione delle identità degli utenti e il loro accesso ad altri account, CA CloudMinder fornisce due tipi di ruoli:

Tipo di ruolo	Scopo
Ruolo di amministrazione	Contiene le attività di amministrazione eseguite dall'utente a cui è stato concesso questo ruolo in CA CloudMinder, ad esempio le attività di modifica della password utente o dell'appartenenza a un gruppo. I ruoli di amministrazione possono comprendere, tra le altre, qualsiasi attività visualizzata nella console utente.
Ruolo di provisioning	Contiene modelli di account che definiscono gli account presenti negli endpoint gestiti, come un sistema di posta elettronica. I modelli di account definiscono inoltre le modalità di mapping degli attributi utente su questi account.
Ruolo di accesso	I ruoli di accesso rappresentano un ulteriore modo per concedere diritti in CA Identity Manager o in un'altra applicazione. Ad esempio, è possibile utilizzare i ruoli di accesso per completare le seguenti operazioni: ■ Fornire accesso indiretto a un attributo utente. ■ Creare espressioni complesse. ■ Impostare un attributo di profilo che un'altra applicazione può utilizzare per determinare i diritti.

Amministrazione delegata

L'amministrazione delegata consiste nell'utilizzare i ruoli per condividere le attività di gestione utenti e di concessione degli accessi alle applicazioni.

Per ciascun ruolo del sistema, un utente può assumere una o di più delle funzioni seguenti:

Funzione	Definizione
Titolare del ruolo	Modifica il ruolo.

Funzione	Definizione
Amministratore di ruolo	Assegna il ruolo ad utenti e altri amministratori di ruolo.
membro del ruolo	Utilizza il ruolo per eseguire attività di amministrazione o di accesso o per utilizzare un account di endpoint.

Dividendo queste funzioni fra gli utenti, è possibile condividere il lavoro di gestione del ruolo. Ad esempio, è possibile far sì che gli amministratori di livello inferiore gestiscano l'appartenenza al ruolo e gli amministratori di livello superiore ne gestiscano le modifiche.

Per implementare l'amministrazione delegata è possibile:

- Designare direttamente un utente come amministratore di un dato ruolo.
- Configurare le *regole di amministrazione* per un ruolo. Le regole di amministrazione definiscono quali utenti possono essere amministratori di un ruolo. Il sistema crea automaticamente amministratori aggiuntivi quando gli utenti soddisfano i criteri specificati nelle regole.

Nota: solo un amministratore in possesso dei privilegi necessari per modificare un ruolo può configurare le regole di amministrazione per quel ruolo. Generalmente, gli amministratori di sistema eseguono questa attività. Per configurare le regole di amministrazione che consentono di delegare l'amministrazione di un ruolo in modo automatico, consultare la sezione intitolata Ruoli di amministrazione nella sezione Informazioni di riferimento della Guida in linea.

Designazione di un amministratore di ruolo

È possibile designare un utente come amministratore di un ruolo. L'amministratore può assegnare allora il ruolo ad altri utenti.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con attività di gestione ruoli.
2. Selezionare Attività, Ruoli e attività.
3. Selezionare una delle seguenti attività:
 - Ruoli di amministrazione, Modifica membri/amministratori del ruolo di amministrazione
 - Ruoli di provisioning, Modifica membri/amministratori del ruolo di provisioning
 - Ruoli di accesso, Modifica membri/amministratori del ruolo di accesso

Viene visualizzata una schermata di ricerca.

4. Selezionare il ruolo che si desidera assegnare all'utente.

5. Fare clic sulla scheda Amministratori.

Viene visualizzato un elenco di amministratori di ruolo.

6. Fare clic su Aggiungi un utente.

Viene visualizzata una schermata di ricerca.

7. Cercare l'utente che si desidera aggiungere come amministratore e fare clic su Seleziona.

Viene visualizzato un elenco aggiornato di amministratori di ruolo.

8. Fare clic su Inoltra.

L'utente diventa un amministratore di ruolo. Questo passaggio completa il processo di delega dell'amministrazione di un ruolo di provisioning. L'amministratore può ora assegnare il ruolo ad altri utenti, concedendo l'accesso agli account di endpoint associati.

Procedura di delega

Una volta presa una decisione sull'utilizzo dei ruoli in base allo Scopo dei ruoli, l'amministrazione delegata viene attuata nel modo seguente:

1. Un amministratore crea un ruolo con regole per il titolare del ruolo, l'amministratore, o il membro.
2. Un titolare del ruolo modifica il ruolo quando sono necessarie delle modifiche.
3. Un amministratore di ruolo:

- Assegna più amministratori di ruolo (facoltativo).
- Assegna più membri del ruolo (facoltativo).

Alcuni utenti sono già amministratori o membri del ruolo se soddisfano le regole definite nel ruolo.

4. Un membro del ruolo utilizza il ruolo:
 - Un membro del ruolo di amministrazione gestisce gli utenti e altri oggetti nell'ambiente di Identity Manager.
 - Un membro del ruolo di accesso esegue delle funzioni nelle applicazioni aziendali.
 - Un membro del ruolo di provisioning utilizza gli account definiti dai criteri nel ruolo.

Esempio di delega

È possibile creare un ruolo con regole per stabilire chi può essere un membro o amministratore. È quindi possibile assegnare il ruolo in modo che altri utenti (che non soddisfanno già le regole) possano diventare un membro o un amministratore del ruolo.

Considerare l'esempio seguente di amministratori che gestiscono i diritti degli utenti finali relativi alle applicazioni aziendali:

- Jeff è titolare del ruolo per il ruolo di Contabile, pertanto quando il ruolo lo richiede, Jeff apporta le modifiche.
- David e Lisa sono amministratori di ruolo per tale ruolo. Assegnano utenti regionali come membri del ruolo.
- Altri utenti sono membri del ruolo senza essere stati assegnati come tali in quanto soddisfano la regola per essere membri del ruolo.

I membri del ruolo utilizzano il ruolo di Contabile per generare ordini di acquisto ed eseguire altre attività nelle applicazioni finanziarie.

La sezione Caratteristiche del ruolo fornisce dettagli sulle regole e sulle altre caratteristiche di un ruolo.

Creazione di utenti

I profili utente consentono agli amministratori di gestire le informazioni utente, i privilegi, l'accesso all'applicazione e ai servizi, e agli utenti di gestire in modo autonomo i propri account e servizi. La creazione dei profili utente è un'attività comune di un amministratore di sistema.

Durante la creazione e la configurazione di un utente, considerare gli elementi di account utente seguenti:

Attività self-service: i profili utenti vengono configurati per impostazione predefinita in modo da consentire l'accesso a determinate attività self-service, quali la modifica della password e delle informazioni di profilo. Un amministratore di sistema con attività appropriate può modificare le attività self-service che può svolgere un utente per impostazione predefinita.

Gruppi: i gruppi semplificano la gestione dei ruoli. Ad esempio, un amministratore di sistema con attività appropriate può configurare più ruoli affinché il sistema lo assegni automaticamente a un utente aggiunto come membro di un gruppo.

Ruoli di amministrazione: i ruoli di amministrazione definiscono le attività che un utente può eseguire nella console utente. Ad esempio, un'attività può consentire a un utente di modificare le informazioni di account utente, quali l'indirizzo o la professione. Un'altra attività può consentire a un utente di amministrare attività, quali concedere l'appartenenza a un gruppo. Quando si assegna un ruolo di amministrazione a un utente, costui può eseguire le attività associate al ruolo.

Account endpoint e ruoli di provisioning: gli account presenti in altri sistemi vengono denominati account endpoint. È possibile assegnare account in endpoint a utenti di CA CloudMinder attraverso ruoli di provisioning. Ad esempio, un utente necessita di un account di Exchange per la posta elettronica, un account di Oracle per l'accesso al database e un account di Active Directory per l'uso del sistema di Windows. Quando si assegna un ruolo di provisioning a un utente, costui riceve gli account endpoint specificati dal ruolo di provisioning.

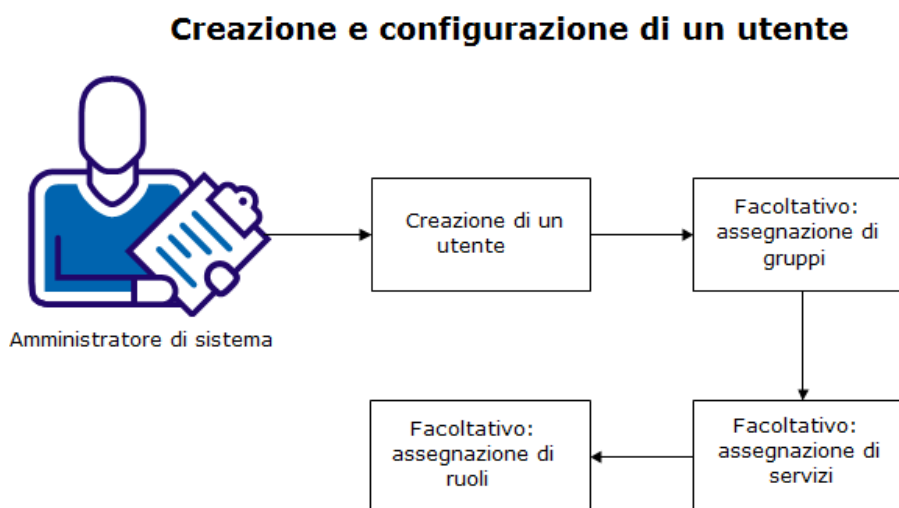
Ruoli di accesso: rappresentano un ulteriore modo per concedere diritti in CA Identity Manager o un'altra applicazione. Ad esempio, è possibile utilizzare i ruoli di accesso per completare le seguenti operazioni:

- Fornire l'accesso indiretto a un attributo utente
- Creare espressioni complesse
- Impostare un attributo in un profilo utente, utilizzato da un'altra applicazione per determinare i diritti

Servizi: i servizi consentono di associare le attività utente, i ruoli, i gruppi e gli attributi selezionati in un unico pacchetto. È possibile gestire questo pacchetto di privilegi come un insieme. Ad esempio, tutti i nuovi dipendenti del reparto Vendite devono accedere a un insieme definito di attività, account su determinati sistemi endpoint e informazioni aggiunte ai loro profili di account utente. Quando si assegna un servizio a un utente, costui riceve l'intero insieme di ruoli, attività, gruppi e attributi di account specificati dal servizio.

Criteri di password: questi criteri consentono di gestire le password degli utenti mediante l'applicazione di regole e restrizioni che disciplinano la scadenza, la composizione e l'utilizzo delle password. Se un amministratore di sistema ha creato criteri di password per l'ambiente dell'utente, tali criteri vengono applicati automaticamente ai nuovi utenti che corrispondono a una o più regole dei criteri di password. Un amministratore di sistema con attività appropriate può modificare i criteri di password.

Nel diagramma seguente sono illustrate le informazioni utili e le fasi per la creazione e la configurazione di un utente.



Nelle sezioni seguenti vengono spiegate in modo dettagliato la creazione e la configurazione di utenti.

1. [Creazione di un utente](#) (a pagina 85).
2. [Assegnazione a gruppi](#) (a pagina 86) (facoltativa).
3. [Assegnazione di un ruolo a un utente](#) (a pagina 86) (facoltativa).
4. [Assegnazione di servizi](#) (a pagina 87) (facoltativa).

Creazione di un profilo utente

Utilizzare questa procedura per creare un profilo utente. In base alla configurazione dell'attività Crea utente, è possibile utilizzare questa attività anche per definire ulteriori elementi di profilo. È possibile aggiungere un utente a un gruppo oppure renderlo membro di un ruolo di amministrazione o di provisioning.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con attività di gestione utenti.
Il ruolo predefinito Manager utente concede i diritti alle attività appropriate.
2. Selezionare Attività, Utenti, Gestisci utenti, Crea utente.
Verrà aperta l'attività Crea utente.

3. Compilare i campi con le necessarie informazioni del profilo utente.
4. Fare clic su Avanti.
5. Compilare i campi nelle altre schede dell'attività, se applicabili.
Ad esempio, aggiungere l'utente a un gruppo o assegnargli un ruolo di amministrazione, un ruolo di provisioning o un servizio, se queste opzioni sono disponibili.
6. Fare clic su Fine.
L'utente è ora creato.

Assegnazione di un gruppo a un utente

È possibile rendere un utente membro di un gruppo.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con attività di gestione utenti.
2. Selezionare Attività, Gruppi, Modifica membri gruppo.
Viene visualizzato un elenco dei gruppi che è possibile gestire.
3. Selezionare un gruppo e fare clic su Seleziona.
Viene visualizzato l'elenco degli utenti assegnati al gruppo.
4. Fare clic su Aggiungi un utente.
5. Cercare un utente che si desidera assegnare al gruppo.
Per visualizzare un elenco di tutti gli utenti per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.
6. Selezionare un utente e fare clic su Seleziona.
Viene visualizzato l'elenco aggiornato degli utenti assegnati al gruppo.
7. Fare clic su Inoltra.
L'utente specificato diventa membro del gruppo.

Assegnazione di un ruolo a un utente

È possibile assegnare ruoli di provisioning a un singolo utente.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con l'attività Modifica membri/amministratori del ruolo di provisioning.
2. Selezionare Ruoli e attività.
3. Selezionare una delle seguenti attività:
 - Ruoli di amministrazione, Modifica membri/amministratori del ruolo di amministrazione
 - Ruoli di provisioning, Modifica membri/amministratori del ruolo di provisioning
 - Ruoli di accesso, Modifica membri/amministratori del ruolo di accesso

Viene visualizzata una schermata di ricerca.
4. Selezionare il ruolo che si desidera assegnare all'utente.

Viene visualizzata la scheda Appartenenza.
5. Fare clic su Aggiungi utente.
6. Cercare un utente al quale si desidera assegnare il ruolo.

Per visualizzare un elenco di tutti gli utenti per i quali si dispone di attività amministrative, fare clic su Cerca senza modificare i criteri di ricerca.
7. Selezionare un utente e fare clic su Seleziona.
8. Fare clic su Inoltra.

I ruoli specificati vengono assegnati all'utente.

Assegnazione diretta di un servizio a un utente

È possibile assegnare un servizio direttamente a un singolo utente. L'utente diviene *membro* del servizio.

Procedere come descritto di seguito:

1. Accedere a Servizi, Richiedi e Visualizza accesso.

Viene visualizzato un elenco dei servizi che è possibile amministrare.
2. Selezionare il servizio che si desidera assegnare all'utente e fare clic su Seleziona.

Viene visualizzato un elenco di utenti assegnati al servizio.
3. Fare clic su Richiedi accesso.
4. Cercare un utente cui si desidera assegnare il servizio.

Per visualizzare un elenco di tutti gli utenti per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.

5. Selezionare un utente e fare clic su Seleziona.

Viene visualizzato un elenco aggiornato degli utenti cui è assegnato il servizio.

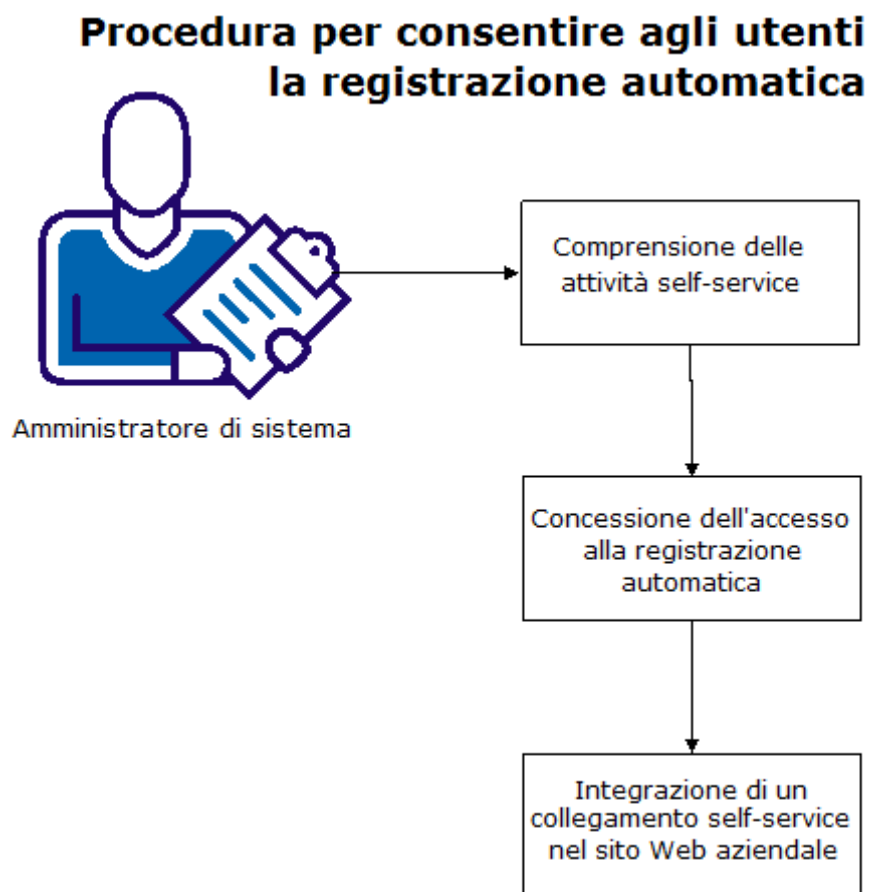
6. Fare clic su Salva modifiche.

L'utente riceve il servizio specificato. L'utente riceve quindi tutte le applicazioni, ruoli, gruppi e attributi inclusi nel servizio.

Procedura per consentire agli utenti la registrazione automatica

Le attività self-service consentono agli utenti di gestire il proprio ambiente. L'attività Registrazione automatica consente di creare il proprio account utente e profilo da una console utente disponibile per l'uso pubblico. Ad esempio, Bentley Cola consente ai nuovi dipendenti e ai clienti di creare i propri account utente e profili attraverso un collegamento incluso nel sito Web aziendale di Bentley Cola.

Nel diagramma seguente vengono illustrate le informazioni utili e le fasi per consentire agli utenti la registrazione automatica.



Nelle sezioni seguenti viene spiegata in modo dettagliato la procedura per consentire l'accesso all'attività di registrazione automatica.

1. [Introduzione alle attività self-service](#) (a pagina 90).
2. [Concessione dell'accesso alla registrazione automatica](#) (a pagina 91).
3. [Integrazione di un collegamento self-service nel sito Web aziendale](#) (a pagina 91).

Attività self-service

Le attività self-service sono azioni eseguibili dagli utenti, in genere attraverso la console utente, per gestire i propri profili. Gli account utente vengono configurati per impostazione predefinita in modo da concedere l'accesso a determinate attività self-service, quali la modifica della password e delle informazioni di profilo. Un amministratore di sistema con privilegi adeguati può modificare quali attività self-service può svolgere un utente per impostazione predefinita.

Le attività self-service si dividono in due tipi:

- **Attività pubbliche:** attività cui gli utenti possono accedere senza immettere le credenziali di accesso. Alcuni esempi di attività pubbliche sono le attività relative alla registrazione automatica, alla password dimenticata o all'ID utente dimenticato.
- **Attività protette:** attività per le quali gli utenti devono immettere credenziali valide. Alcuni esempi di attività protette sono le attività relative alla modifica delle password o delle informazioni relative al profilo.

Nella tabella seguente sono elencate le attività self-service predefinite.

Tipo di attività	Attività
Attività pubblica	■ Registrazione automatica: consente agli utenti di registrarsi presso un sito Web aziendale ■ Ripristino password dimenticata: consente agli utenti di reimpostare una password dimenticata ■ Password dimenticata: consente di visualizzare una password temporanea che gli utenti possono usare per accedere a CA Identity Manager. Quando gli utenti effettuano l'accesso, verrà richiesto di immettere una nuova password. ■ ID utente dimenticato: consente di recuperare o reimpostare un ID utente dimenticato
Attività protetta	■ Richiedi e Visualizza accesso: consente agli utenti di richiedere l'accesso e rimuovere servizi. ■ Modifica password personale: consente di reimpostare la password personale ■ Modifica profilo personale: consente di gestire le informazioni del profilo, ad esempio l'indirizzo ed il numero di telefono ■ Modifica gruppi personali: consente agli utenti di registrarsi ai gruppi disponibili ■ Visualizza ruoli personali: consente di visualizzare i ruoli associati ad un utente ■ Visualizza attività personali inoltrate: consente di visualizzare le attività di CA Identity Manager avviate dall'utente

Accesso alle attività di self-service

Dopo aver configurato le attività self-service per l'ambiente in uso, è possibile aggiungere gli URL di tali attività a un sito Web aziendale.

Gli URL delle attività self-service hanno il seguente formato:

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=task_tag`

In cui:

- *domain* corrisponde al nome di dominio completo del server Web nell'ambiente di esecuzione di CA CloudMinder.
- *public_alias* corrisponde all'alias pubblico dell'ambiente. L'amministratore di sistema definisce l'alias pubblico al momento della creazione dell'ambiente.
- *tag_attività* corrisponde all'identificatore univoco dell'attività.

Per l'attività Ripristino password dimenticata predefinita il tag dell'attività è ForgottenPasswordReset.

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenPasswordReset`

Per l'attività ID utente dimenticato predefinita il tag dell'attività è ForgottenUserID:

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenUserID`

Integrazione di un collegamento self-service nel sito Web aziendale

Per permettere l'accesso a un'attività self-service pubblica da un sito Web aziendale, è possibile aggiungere un collegamento a qualsiasi pagina Web. Quando un utente fa clic sul collegamento, viene visualizzata una schermata dell'attività. Una volta completata l'attività, l'utente viene reindirizzato alla console utente per impostazione predefinita.

Per modificare la pagina di reindirizzamento degli utenti, è possibile aggiungere il tag `task.RedirectURL` all'URL associato al collegamento come segue:

```
<A  
href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&task.RedirectURL=http://domain/redirect_URL">testo del collegamento</A>
```

domain

Nome di dominio completo del server Web nell'ambiente di esecuzione di CA Identity Manager.

public_alias

Stringa univoca aggiunta all'URL per l'accesso alle attività pubbliche.

Le attività pubbliche sono attività self-service, come la registrazione automatica o le attività legate alla password dimenticata. Non è necessario eseguire l'accesso per svolgere le attività pubbliche.

Nota: per ulteriori informazioni sulle attività pubbliche e gli alias, consultare la *Guida alla configurazione*.

tasktag

Identificatore univoco dell'attività. Per determinare il tag di attività, utilizzare Modifica attività di amministrazione per visualizzare il profilo per l'attività.

redirect_URL

URL di reindirizzamento utente dopo il completamento dell'attività.

Ad esempio, è possibile reindirizzare gli utenti a una pagina di benvenuto dopo la registrazione automatica.

testo del collegamento

Testo selezionabile dagli utenti per accedere all'URL di destinazione.

Ad esempio, un'azienda può aggiungere un collegamento che consente agli utenti di reimpostare una password dimenticata per poi reindirizzarli a una pagina di benvenuto.

Il codice HTML seguente rappresenta un esempio di testo di collegamento:

```
<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/  
index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/welcome.html">Reimposta password personale</A>
```

Per reindirizzare gli utenti alla pagina di accesso all'attività self-service, specificare `RefererURL` come valore del tag `task.RedirectURL` come segue:

```
<A  
href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&task.RedirectURL=RefererURL">
```

Configurazione di più attività di self-service

È possibile creare più attività di self-service per tipi di utenti diversi. Ad esempio, è possibile creare un'attività per registrare i nuovi dipendenti ed un'altra attività per registrare i clienti. Grazie all'utilizzo di attività di registrazione automatica diverse, è possibile:

- Raccogliere informazioni diverse
- Registrare gli utenti in organizzazioni diverse
- Reindirizzare gli utenti a pagine di disconnessione diverse dopo la procedura di registrazione
- Utilizzare una marcatura diversa

Nelle figure seguenti sono illustrate le attività di registrazione automatica rispettivamente per i nuovi dipendenti e per i clienti.

Dipendente Registrazione automatica

• = Richiesto

Benvenuti a MyCompany.com! Grazie per far parte del nostro team.

•Nome	
•Cognome	
•Scegli password	
•Immettere nuovamente la password	
Domanda di sicurezza 1	
Risposta 1	
Email	

Cliente Registrazione automatica

• = Richiesto

Grazie per il tuo interesse per MyCompany.Com! Per ricevere informazioni sui nostri prodotti, si prega di fornire le informazioni seguenti:

• Nome	
• Cognome	
Società	
Titolo	
• Scegli password	
• Immettere nuovamente la password	
Domanda di sicurezza 1	
Risposta 1	
Email	

Per configurare più attività di self-service dello stesso tipo, specificare un tag univoco durante la creazione dell'attività. Il campo Tag è disponibile nella schermata Configura profilo relativo all'attività.

Quando si aggiunge il collegamento per accedere all'attività a un sito Web, si aggiunge il tag dell'attività in modo da creare un URL univoco.

Ad esempio, è possibile creare due attività nel modo seguente:

Attività	Tag	URL
Registra come nuovo dipendente	selfregistration_employee	<code>http://dominio/iam/im/alias/index.jsp?task.tag=SelfRegistration_employee</code>
Registra come cliente	selfregistration_customer	<code>http://dominio/iam/im/alias/index.jsp?task.tag=SelfRegistration_customer</code>

Limitazione dell'accesso al ruolo Gestione automatica

Per impostazione predefinita, il ruolo di Gestore automatico, che consente agli utenti di gestire le proprie informazioni di profilo e di visualizzare i propri ruoli e attività inoltrate, viene assegnato a tutti gli utenti.

Per associare il ruolo Gestione automatica ad un sottoinsieme di utenti, eliminare il criterio membri esistente e crearne uno nuovo come descritto nell'argomento Definizione dei criteri membri per un ruolo di amministrazione.

Capitolo 5: Gestione delle password

Questa sezione contiene i seguenti argomenti:

[Gestione delle password in Identity Manager](#) (a pagina 97)

[Panoramica dei criteri di password](#) (a pagina 98)

[Creazione di un criterio di password](#) (a pagina 99)

[Gestione criteri di password](#) (a pagina 114)

[Criteri di password e database relazionali](#) (a pagina 114)

[CA Identity Manager e l'integrazione con i criteri di password di SiteMinder](#) (a pagina 114)

[Reimpostazione della password o sblocco dell'account](#) (a pagina 115)

[Password di sincronizzazione sugli endpoint](#) (a pagina 124)

Gestione delle password in Identity Manager

In Identity Manager sono disponibili numerose funzionalità per la gestione delle password degli utenti.

- Criteri di password: questi criteri consentono di gestire le password degli utenti mediante l'applicazione di regole e restrizioni che disciplinano la scadenza, la composizione e l'utilizzo delle password.
- Gestione password: gli amministratori a cui è stato assegnato il ruolo Gestione password possono reimpostare una password quando un utente si rivolge all'help desk.
- Gestione di password self-service: in Identity Manager sono disponibili numerose attività di self-service che consentono agli utenti di gestire le proprie password. Queste attività includono:
 - Registrazione automatica: gli utenti specificano una password quando si registrano presso un sito Web aziendale.
 - Modifica password personale: gli utenti possono modificare la propria password senza l'aiuto del personale tecnico o dell'help desk
 - Password dimenticata: gli utenti possono reimpostare o recuperare una password dimenticata in seguito alla verifica della propria identità in Identity Manager.
 - Reimposta password o Sblocca account: gli utenti possono reimpostare o recuperare una password dimenticata o sbloccare un account Windows su un sistema da cui abbiano accesso a Identity Manager.
 - ID utente dimenticato: gli utenti possono recuperare un ID utente dimenticato in seguito alla verifica della propria identità in Identity Manager.

- Sincronizzazione password su account endpoint: le modifiche apportate alle password vengono sincronizzate in Identity Manager, nel server di fornitura e nei relativi sistemi di destinazione. Le nuove password vengono verificate in base ai criteri di password di Identity Manager.

Panoramica dei criteri di password

Un criterio di password è un insieme di regole e restrizioni. Queste regole specificano la creazione e la scadenza della password. Quando un criterio di password viene configurato in un ambiente CA Identity Manager, questo viene applicato all'archivio utenti associato all'ambiente. Se una directory utente è associata a più ambienti, un criterio di password definito in un ambiente può essere applicato anche in altri ambienti.

In un criterio password, è possibile configurare le seguenti impostazioni:

Nota: alcune di queste impostazioni richiedono il mapping delle directory degli utenti per determinati attributi. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

- Applicazione di password a un insieme specifico di utenti
- Scadenza password: definire gli eventi che determinano la scadenza di una password, ad esempio il numero di giorni trascorsi o il numero di tentativi di accesso non riusciti. Quando una password scade, l'account utente viene disabilitato.
- Composizione password—Specificare i requisiti del contenuto per le nuove password. Ad esempio, è possibile configurare le impostazioni che richiedono la creazione di password con lunghezza minima di otto caratteri e contenenti un numero e una lettera.
- Espressioni regolari—Fornire un'espressione che determini il formato di una password valida. È possibile specificare se le password corrispondono o meno a tale formato. È possibile specificare anche espressioni regolari multiple.
- Restrizioni password: impostare i limiti per il riutilizzo delle password. Ad esempio, gli utenti devono attendere 90 giorni prima di riutilizzare una password.
- Opzioni password avanzate—Specificare le azioni eseguite da CA Identity Manager, ad esempio la conversione delle password in caratteri minuscoli prima dell'elaborazione. È inoltre possibile specificare la priorità di un criterio password, quando vengono applicati più criteri.

Gli utenti di SiteMinder possono inoltre configurare i criteri di password nell'interfaccia di amministrazione di SiteMinder. Tali criteri vengono visualizzati nella console utente di CA Identity Manager.

Nota: quando CA Identity Manager si integra con SiteMinder, SiteMinder impone *tutti* i criteri di password.

Creazione di un criterio di password

I criteri di password vengono creati attraverso la console utente di CA Identity Manager.

Nota: la disponibilità di alcune opzioni dei criteri di password richiede l'esecuzione del mapping di determinati attributi noti. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

Procedere come descritto di seguito:

1. Nella console utente, selezionare una delle seguenti opzioni:
 - Criteri, Gestisci criteri di password, Crea criterio password.
 - Attività, Criteri, Gestisci criteri di password, Crea criterio password.
2. Immettere un nome univoco e una descrizione facoltativa per il criterio di password.
3. Configurare queste impostazioni dei criteri di password nel modo più adatto alla propria implementazione:
 - [Applicazione di un criterio di password ad un gruppo di utenti](#) (a pagina 100)
 - [Configurazione della scadenza della password](#) (a pagina 102)
 - [Configurazione della composizione della password](#) (a pagina 105)
 - [Specifica di espressioni regolari](#) (a pagina 107)
 - [Impostazione delle restrizioni di password](#) (a pagina 109)
 - [Configurazione delle opzioni avanzate della password](#) (a pagina 113)

Abilitazione dei criteri di password aggiuntivi

CA Identity Manager consente di creare criteri di password di base che gestiscono le password degli utenti imponendo la scadenza la composizione e l'uso della password. Inoltre, è possibile definire le seguenti regole e restrizioni aggiuntive per le password:

- Scadenza delle password:
 - Tenere traccia degli accessi non riusciti o completati
 - Autenticazione di un accesso
 - Scadenza delle password in caso di mancata modifica
 - Inattività delle password
 - Password errata
 - Più espressioni regolari

- Restrizioni delle password:
 - Numero minimo di giorni prima del riutilizzo
 - Numero minimo di password prima del riutilizzo
 - Differenza in percentuale dall'ultima password
 - Ignora la sequenza durante l'analisi delle differenze.

Procedere come descritto di seguito:

1. Andare a Directory, <name of the directory>, Utente nella Console di gestione.
2. Verificare che %PASSWORD DATA% and %ENABLED STATES% -> 'STATE' siano mappati su attributi fisici.
3. Di questi attributi viene eseguito il mapping per impostazione predefinita nei file campione directory.xml. Se di questi attributi non viene eseguito il mapping, consultare la *Guida alla configurazione di CA Identity Manager* per informazioni aggiuntive.

Applicazione di un criterio di password ad un gruppo di utenti

È possibile specificare regole che determinano l'insieme di utenti per i quali è valido un criterio di password. Ciò consente di disporre di un criterio di password da applicare ai dipendenti generici e di un criterio più rigido da applicare ai dirigenti di livello superiore.

Procedere come descritto di seguito:

1. Creare o modificare un criterio di password nella console utente.
2. Selezionare il tipo di filtro da configurare nel campo Filtro di directory.
Per una descrizione dei tipi di filtro disponibili, consultare la tabella riportata di seguito.

Nota: il tipo di archivio utenti a cui il criterio di password si applica determina le opzioni per la casella di riepilogo Filtro di directory. Alcuni tipi di filtro non sono disponibili per i database relazionali e gli archivi utenti di CA Directory in caso di integrazione di CA Identity Manager con SiteMinder.
3. Per specificare una condizione, selezionare un attributo ed un operatore, quindi immettere un valore.
4. Per aggiungere altre condizioni, fare clic sul segno più.

Nella tabella seguente sono descritte le opzioni disponibili per i tipi di filtro di directory e vengono riportati alcuni esempi di ciascun tipo di filtro. Gli attributi sul lato sinistro del simbolo "=" negli esempi seguenti sono come vengono specificati nell'area di definizione della directory dell'utente. Per le attività dell'utente che riguardano la creazione, i criteri di password con filtri di directory configurati sono applicati solo quando vengono soddisfatte entrambe le condizioni seguenti:

- CA Identity Manager non è integrato con SiteMinder.
- Il tipo di filtro della directory non è Utente, Gruppo, Filtro gruppi o Ricerca gruppi.

Tipo di filtro	Utilizzare questo filtro per...	Esempio
In un'organizzazione	Cercare e selezionare un'organizzazione.	
In un gruppo	Cercare e selezionare un gruppo.	
Un utente	Cercare e selezionare un singolo utente.	
Filtro utente (Non disponibile per database relazionali quando sono integrati con SiteMinder)	Specificare un filtro per gli utenti.	Tipo di dipendente = Appaltatore Dipartimento = Protezione
Espressione di ricerca utente	Inserire una query di ricerca per gli utenti.	uid=jsmith (per LDAP) TBLUSERS.ID = jsmith (per database relazionali)
Filtro gruppo (Non disponibile per database relazionali quando sono integrati con SiteMinder)	Specificare un filtro i gruppi.	Sottoscrizione automatica = *
Espressione di ricerca gruppo	Inserire una query di ricerca per i gruppi.	cn=Sales (per LDAP) TBLGROUPS.NAME=GroupA (per database relazionali)
Filtro organizzazione (Non disponibile per database relazionali quando sono integrati con SiteMinder)	Specificare un filtro per le organizzazioni.	Nome organizzazione = *Marketing

Tipo di filtro	Utilizzare questo filtro per...	Esempio
Espressione di ricerca organizzazione	Inserire una query di ricerca per le organizzazioni.	ou=Boston (per LDAP) TBLORGANIZATIONS.NAME=Boston (per database relazionali)
Cerca	Specificare una query non inclusa in altre opzioni per il tipo di filtro.	(&(uid=*rossi))(ou=Milano))

Configurazione della scadenza della password

Per aiutare a gestire l'accesso dell'utente, è possibile definire eventi come tentativi multipli di accesso non riuscito o inattività dell'account. Quando questi eventi si verificano, CA Identity Manager disattiva l'account utente responsabile. Quando CA Identity Manager viene integrato con SiteMinder, è possibile specificare un reindirizzamento.

Nota: queste impostazioni richiedono una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

È possibile configurare le seguenti impostazioni per quanto riguarda la scadenza della password:

- Casella di controllo Traccia degli accessi non riusciti o completati
- Casella di controllo Autenticare se impossibile tenere traccia degli accessi
- Impostazioni scadenza password non modificata
- Impostazioni scadenza password per inattività
- Impostazioni password errate

Casella di controllo Traccia degli accessi non riusciti o completati

Questa casella di controllo abilita e disabilita la registrazione dei tentativi di accesso dell'utente, inclusa l'ora dell'ultimo tentativo di accesso. Se si abilita questa casella di controllo, CA Identity Manager scrive le informazioni di accesso su un attributo dei dati della password nell'archivio utenti.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

Quando la casella di controllo Registra accessi non riusciti viene abilitata, la sezione Password errata e la casella di controllo Autenticare se impossibile tenere traccia degli accessi sono attive. Quando la casella di controllo Registra accessi riusciti è abilitata, la sezione relativa alla scadenza della password per inattività e la casella di controllo Autenticare se impossibile tenere traccia degli accessi sono attive.

Se si hanno criteri di password multipli, assicurarsi che tutti i criteri delle password coinvolte disattivino i dettagli di accesso. In caso contrario, un solo criterio che abilita la registrazione dei dettagli di accesso può provocare un comportamento errato dei criteri di password.

Casella di controllo Autenticare se impossibile tenere traccia degli accessi

La selezione di questa casella di controllo abilita l'accesso quando non è possibile eseguire la registrazione dell'utente. Per impostazione predefinita, questa casella di controllo è disattivata. Quando la registrazione dell'accesso è disattivata, gli utenti non possono accedere.

Quando si seleziona questa casella di controllo, assicurarsi di selezionare anche le caselle di controllo Registra accessi non riusciti o Registra accessi riusciti.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

Impostazioni scadenza password non modificata

Nei campi Scadenza password non modificata è possibile configurare il comportamento delle password scadute. Facoltativamente, è possibile specificare quanto tempo prima della scadenza della password gli utenti verranno avvertiti.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

È possibile configurare i seguenti campi:

Dopo <number> giorni

Determina il numero di giorni attesi dopo la scadenza di una password prima che CA Identity Manager disattivi l'utente o imponga una modifica della password.

Nota: CA Identity Manager non disattiva l'account utente finché l'utente non tenta di accedere, dopo che è trascorso il numero di giorni specificato.

Disattiva utente

La selezione di questo pulsante di opzione disabilita l'utente alla scadenza della password. È possibile abilitare gli utenti disabilitati mediante:

- L'attività Attiva/disattiva utente nella Console utente. (I ruoli Manager di sistema, Manager organizzazione e Manager protezione predefiniti comprendono l'attività Attiva/disattiva utente.)
- L'interfaccia di amministrazione di SiteMinder.

Nota: per ulteriori informazioni, consultare la *Guida all'installazione dei server di criteri per CA SiteMinder*.

Imponi modifica password

Selezionando questo pulsante di opzione viene imposta una modifica della password quando l'utente tenta nuovamente di accedere.

Avvisi scadenza problematica per <number> giorni

Specificare quanti giorni prima della scadenza di una password l'utente deve ricevere una notifica.

Impostazioni scadenza password per inattività

Le impostazioni relative alla scadenza di una password per inattività consentono di specificare il periodo di tempo che deve trascorrere dall'ultimo tentativo di accesso. Trascorso questo periodo un account utente viene considerato inattivo. È possibile utilizzare questa sezione anche per specificare un'azione quando un utente, il cui account è considerato inattivo, ha l'autorizzazione ad accedere.

Per configurare le impostazioni nella sezione relativa alla scadenza della password per inattività, accertarsi di aver abilitato le caselle di controllo che consentono di tenere traccia degli accessi.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

La sezione relativa alla scadenza della password per inattività contiene le seguenti impostazioni:

- Dopo <number> giorni -- Determina il numero di giorni di inattività dopo i quali una password scade.
- Disattiva utente--Disattiva l'utente quando la password scade per inattività e l'account utente viene disattivato. Gli utenti disattivati devono quindi essere riattivati utilizzando l'attività Attiva/Disattiva utente.
- Imponi modifica password -- Impone la modifica di una password, quando questa scade a causa di inattività. L'utente modifica la password al tentativo di accesso successivo.

Impostazioni password errate

Nella sezione delle impostazioni Password errata è possibile specificare quanti tentativi di accesso non riusciti sono consentiti prima di disattivare l'account utente. È possibile inoltre specificare per quanto tempo l'account viene disattivato, prima che un utente possa tentare di accedere di nuovo. Questa sezione è valida solo quando è stata selezionata la casella di controllo Registra accessi non riusciti.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

La sezione Password errata contiene i campi seguenti:

Account disattivato dopo <number> password errate consecutive

Questa impostazione determina il numero di tentativi di accesso consecutivi non riusciti che un utente può effettuare. Limitando il numero di tentativi errati ci si protegge dai programmi progettati per accedere a una risorsa continuando a inserire password finché non viene trovata quella corretta. Se un utente non riesce ad accedere correttamente dopo il numero specificato di tentativi, CA Identity Manager disattiva l'account. Per riabilitare l'account è necessario l'intervento di un amministratore.

Dopo <number> minuti

Questa impostazione determina il periodo di tempo che un utente deve attendere prima di effettuare un ulteriore tentativo di accesso o prima che l'account venga riattivato. Se l'utente immette un'altra password errata, CA Identity Manager disattiva di nuovo l'account. L'utente attende il periodo di tempo specificato prima di provare di nuovo.

Consenti un tentativo di accesso

Questa impostazione specifica il numero di minuti da attendere dopo aver immesso una password errata, prima di poter eseguire un ulteriore tentativo.

Riabilita account

Questa impostazione riattiva un account dopo il numero specificato di minuti.

Configurazione della composizione della password

È possibile specificare regole che determinano la composizione di caratteri per le password appena create. Verificare di aver considerato la massima lunghezza di password durante la determinazione dei valori per i requisiti dei caratteri. Se il numero totale richiesto di lettere e caratteri numerici supera la lunghezza massima della password, tutte le password vengono rifiutate. Ad esempio, se i valori di Lettere o caratteri numerici sono entrambi impostati su sei, tutte le password contengono almeno 12 caratteri (6 lettere e 6 cifre). In questo esempio, se la lunghezza massima della password è di otto caratteri, tutte le password vengono rifiutate.

Le impostazioni di composizione password comprendono:

Lunghezza minima password

Specifica una lunghezza minima per password utente.

Lunghezza massima password

Specifica la lunghezza massima per password utente.

Numero massimo di caratteri ripetuti

Determina il numero massimo di caratteri identici visualizzabili in sequenza in una password.

Ad esempio, se questo valore è impostato su 3, la sequenza "aaaa" non è consentita nella password. Invece, la sequenza "aaa" è accettabile all'interno di una password. Impostare questo valore per assicurare che gli utenti non possano immettere password composte da un carattere singolo.

Lettere maiuscole

Specifica se consentire i caratteri alfabetici in maiuscolo e, in tal caso, il numero minimo contenuto in una password.

Lettere minuscole

Specifica se consentire i caratteri alfabetici in minuscolo e, in tal caso, il numero minimo contenuto in una password.

Lettere

Specifica se consentire le lettere e, in tal caso, il numero minimo contenuto in una password.

Nota: la casella di controllo Lettere viene selezionata automaticamente quando si abilitano i caratteri in maiuscolo o in minuscolo.

Caratteri numerici

Specifica se consentire le cifre e, in tal caso, il numero minimo contenuto in una password.

Lettere o caratteri numerici

Specifica se consentire lettere o caratteri numerici e, in tal caso, il numero minimo contenuto in una password. Se questa impostazione viene impostata insieme a Caratteri numerici, i caratteri possono soddisfare entrambi i requisiti. Ad esempio, se questa opzione e Caratteri numerici sono impostati su 4, la password "1234" è una password valida.

Nota: la casella di controllo Lettere o caratteri numerici viene selezionata automaticamente quando si abilitano i caratteri in maiuscolo o in minuscolo o i numeri.

Segni di interpunzione

Specifica se consentire i segni di interpunzione e, in tal caso, il numero minimo contenuto in una password. I segni di interpunzione comprendono punti, virgole, punti esclamativi, barre rovesciate, trattini e lineette.

Non stampabile

Specifica se consentire i caratteri non stampabili e, in tal caso, il numero minimo contenuto in una password. Non è possibile visualizzare questi caratteri sulla schermata del computer.

Nota: alcuni browser non supportano caratteri non stampabili.

Non alfanumerico

Specifica se consentire caratteri non alfanumerici, tra cui segni di interpunzione e altri simboli (@, \$ e *) e, in tal caso, il numero minimo contenuto in una password. Sono inclusi anche i caratteri non stampabili. Un carattere non alfanumerico soddisfa anche i requisiti di carattere Segni di interpunzione e Non stampabile.

Specifica di espressioni regolari

Le espressioni regolari delle password consentono di specificare modelli di testo di espressioni regolari per la corrispondenza delle stringhe a cui corrisponde, o non corrisponde, ogni password, per essere valida. Questa verifica può essere utile, ad esempio, quando si desidera richiedere che il primo carattere sia una cifra e l'ultimo carattere no.

Per un singolo criterio di password si configurano espressioni multiple. Se si creano espressioni multiple, le password accettabili corrispondono a *tutte* le espressioni specificate.

Procedere come descritto di seguito:

1. Digitare un tag descrittivo per l'espressione (senza spazi bianchi) nel campo Nome.
2. Digitare un'espressione regolare utilizzando la sintassi descritta nella sintassi delle espressioni regolari nel campo Deve corrispondere.
3. Se la password non corrisponde all'espressione regolare, selezionare la casella di controllo nella colonna Non deve corrispondere.

Nota: è possibile specificare espressioni multiple facendo clic sul segno più (+) per aggiungere l'espressione.

Esempio: è possibile utilizzare la seguente definizione di espressione regolare per richiedere che tutte le password inizino con una maiuscola o minuscola letter:Name: MustStartAlpha

Expression: [a-zA-Z].*

Sintassi delle espressioni regolari

In questa sezione viene descritta la sintassi utilizzata per costruire espressioni regolari ai fini della corrispondenza di password. Questa sintassi è coerente con la sintassi delle espressioni regolari supportata per la corrispondenza delle risorse quando si specificano aree di autenticazione.

Caratteri	Risultati
\	Utilizzato per citare un metacarattere (come '*')
\\	Corrisponde a un carattere singolo '\'
(A)	Raggruppa espressioni secondarie (influisce sull'ordine di valutazione del modello)
[abc]	Classe di caratteri semplici (qualsiasi carattere tra parentesi corrisponde al carattere di destinazione)
[a-zA-Z]	Classe di caratteri con intervalli (qualsiasi intervallo di carattere tra parentesi corrisponde al carattere di destinazione)
[^abc]	Classe di caratteri negati
.	Corrisponde a qualsiasi carattere diverso da nuova riga
^	Corrisponde solo all'inizio di una riga

Caratteri	Risultati
\$	Corrisponde solo alla fine di una riga
A*	Corrisponde ad A 0 o più volte (greedy)
A+	Corrisponde ad A 1 o più volte (greedy)
A?	Corrisponde ad A 1 o 0 volte (greedy)
A*?	Corrisponde ad A 0 o più volte (reluctant)
A+?	Corrisponde ad A 1 o più volte (reluctant)
A??	Corrisponde ad A 0 o 1 volta (reluctant)
AB	Corrisponde ad A seguito da B
A B	Corrisponde ad A o a B
\1	Backreference alla prima espressione secondaria tra parentesi
\n	Backreference alla <i>ennesima</i> espressione secondaria tra parentesi

Tutti gli operatori di chiusura (+, *, ?) sono greedy per impostazione predefinita, pertanto corrispondono a quanti più elementi possibili della stringa senza errori di corrispondenza globale. Se si desidera una chiusura di tipo reluctant (non-greedy), è possibile farla semplicemente seguire da '?'. Una chiusura di tipo reluctant corrisponderà a quanti meno elementi possibili della stringa quando si trovano delle corrispondenze.

Impostazione delle restrizioni di password

È possibile definire restrizioni sull'uso delle password. Le restrizioni includono il tempo di attesa richiesto prima di riutilizzare una password e la percentuale di differenza tra una password e quelle selezionate in precedenza. Inoltre, è possibile impedire agli utenti di specificare le parole impostate come pericolose per la protezione o contenenti informazioni personali.

Nota: questa impostazione richiede una configurazione aggiuntiva. Consultare la sezione [Abilitazione dei criteri di password aggiuntivi](#) (a pagina 99).

La sezione Restrizioni comprende i campi seguenti:

N. minimo di giorni prima del riutilizzo

Determina il numero dei giorni di attesa prima di riutilizzare una password.

Numero minimo di password prima del riutilizzo

Determina il numero di password da utilizzare prima di poterne riutilizzare una.

Nota: se si specificano un intervallo di tempo e un numero di password, entrambi i criteri vengono soddisfatti prima di poter riutilizzare una password. Ad esempio, è possibile configurare un criterio di password che richiede l'attesa di 365 giorni e un numero specificato di 12 password prima di riutilizzarne una. Dopo un anno, se sono state utilizzate solo sei password, è necessario utilizzarne altre sei per poter riutilizzare la prima.

Differenza in percentuale dall'ultima password

Specifica la percentuale di caratteri che devono essere contenuti in una nuova password. È possibile impostare il valore su 100. In questo caso, la nuova password non può contenere i caratteri usati nella password precedente.

Ignora la sequenza durante l'analisi delle differenze

Ignora la posizione dei caratteri nella password in fase di determinazione della percentuale.

Ad esempio, se la password iniziale è BASEBALL12 e la casella di controllo Ignora la sequenza durante l'analisi delle differenze è selezionata, 12BASEBALL non è una password accettabile. Se la casella di controllo è deselezionata, 12BASEBALL è una password accettabile perché le lettere si trovano in una posizione diversa.

Per una maggiore protezione, la casella di controllo Ignora la sequenza durante l'analisi delle differenze è selezionata.

Password	Differenza percentuale	Ignora sequenza	Accettata
BASEBALL12 (precedente)	0	Selezionata	Sì
12BASEBALL		Deselezionata	Sì
BASEBALL12 (precedente)	100	Selezionata	No
12BASEBALL		Deselezionata	Sì
BASEBALL12 (precedente)	0	Selezionata	Sì
12SOFTBALL		Deselezionata	Sì

Password	Differenza percentuale	Ignora sequenza	Accettata
BASEBALL12 (precedente)	90	Selezionata	No
12SOFTBALL		Deselezionata	Sì
BASEBALL12 (precedente)	100	Selezionata	No
12SOFTBALL		Deselezionata	No

Attributi di profilo

La configurazione del campo Lunghezza corrispondente impedisce agli utenti di utilizzare informazioni personali nelle password. Il campo Lunghezza corrispondente determina la lunghezza minima della sequenza confrontata dal criterio di password con gli attributi nella voce di directory. Ad esempio, se questo valore viene impostato su quattro, CA Identity Manager verifica che la password non includa gli ultimi quattro caratteri degli attributi del profilo utente, ad esempio, il cognome o il numero di telefono.

Dizionario

Specifica un elenco di stringhe che non è possibile utilizzare nelle password.

Nota: il ritorno a capo segue l'ultima riga della voce di dizionario.

Le impostazioni Dizionario comprendono i campi seguenti:

- Percorso: contiene il percorso completo e il nome del file di dizionario.
- Lunghezza corrispondente: controlla la lunghezza delle stringhe confrontate con valori nel file di dizionario. Nel confronto viene ignorata la distinzione tra maiuscole e minuscole. È possibile lasciare vuoto il campo Lunghezza corrispondente oppure impostarlo su zero. In questi casi, CA Identity Manager rifiuta solo le password che corrispondono esattamente a una stringa nel dizionario. Quando la lunghezza corrispondente è maggiore di zero, CA Identity Manager rifiuta le voci nelle condizioni seguenti:
 - La password include una stringa secondaria che inizia con la stessa serie di caratteri di una voce del dizionario.
 - Il numero di caratteri corrispondenti consecutivi è maggiore o uguale al numero specificato nel campo Lunghezza corrispondente.

Ad esempio, considerare un file di dizionario che contiene le voci seguenti:

- lion
- tiger
- bear

Quando il campo Lunghezza corrispondente viene impostato su quattro produce le azioni seguenti:

"TeddyBear", password rifiutata perché "Bear" corrisponde alla voce "bear" nel file di dizionario.

"prestige", password rifiutata perché "tige" corrisponde ai primi quattro caratteri della voce "tiger" nel file di dizionario.

"Geiger Counter", password accettata perché "iger" non include la prima lettera della voce "tiger" nel file di dizionario.

Configurazione delle opzioni avanzate di password

Le opzioni per i criteri avanzati di password consentono di configurare la pre-elaborazione di password inoltrate prima della convalida e dell'archiviazione. È inoltre possibile assegnare al criterio una priorità per permettere una valutazione prevedibile di criteri di password multiple che si applicano allo stesso spazio dei nomi o directory utente.

Non imporre maiuscole/minuscole | Imponi maiuscole | Imponi minuscole

Determinare se per le password vengono imposte le maiuscole o le minuscole prima dell'elaborazione e dell'archiviazione. Scegliere un'opzione per l'applicazione di maiuscole o minuscole facendo clic sul pulsante di opzione Imponi maiuscole o Imponi minuscole. Altrimenti verificare che sia selezionato il pulsante di opzione Non imporre maiuscole/minuscole (impostazione predefinita).

Importante. Verificare che qualsiasi opzione specificata per l'applicazione di maiuscole o minuscole sia coerente con eventuali requisiti definiti di composizione con distinzione tra maiuscole e minuscole.

Rimuovi spazio bianco iniziale

Selezionare per rimuovere lo spazio bianco iniziale dalla password prima dell'elaborazione.

Rimuovi spazio bianco finale

Selezionare per rimuovere lo spazio bianco finale dalla password prima dell'elaborazione.

Rimuovi spazio bianco inserito

Selezionare per rimuovere ogni spazio bianco inserito prima dell'elaborazione.

Nota: alcune implementazioni di directory utente rimuovono automaticamente lo spazio bianco iniziale o finale dai valori di attributo, in cui vengono archiviate le password utente, prima di archivarli. Le impostazioni specificate nel criterio di password non hanno effetto.

Priorità di valutazione

Specifica la priorità di valutazione del criterio di password. Il valore è compreso tra 0 (impostazione predefinita) e 999. I criteri adatti vengono valutati in ordine decrescente (il primo valore è 999; 0 è l'ultimo).

Applica criteri di password di priorità inferiore

Determina se applicare in seguito criteri di password con priorità inferiore.

Quando si accede a una di queste attività, in CA Identity Manager viene visualizzato l'elenco dei criteri di password validi per l'archivio utenti associato all'ambiente CA Identity Manager corrente. In caso di integrazione di CA Identity Manager con SiteMinder, l'elenco può includere criteri di password creati nell'interfaccia utente di amministrazione di SiteMinder tramite Servizi di password. È possibile gestire i criteri di password creati in CA Identity Manager o SiteMinder.

Criteri di password e database relazionali

Per evitare problemi di sintassi durante l'esecuzione, è opportuno che questo campo si trovi nella tabella primaria.

CA Identity Manager e l'integrazione con i criteri di password di SiteMinder

Importante: CA Identity Manager non pone limitazioni per l'utilizzo di caratteri di punteggiatura nelle password. Tuttavia, se si desidera utilizzare la funzionalità di password di SiteMinder, è consigliabile creare password che soddisfino le restrizioni di SiteMinder.

Reimpostazione della password o sblocco dell'account

In caso di password dimenticata sui sistemi Windows, è possibile configurare il criterio self-service per la visualizzazione del prompt nella schermata di accesso di Windows. È possibile utilizzare questa funzionalità mediante l'installazione del provider delle credenziali per i sistemi Windows Vista e Windows 7.

Con questa funzionalità, l'utente esegue accesso self-service tramite il browser Web Cube, dove viene visualizzata una pagina per la richiesta di modifica password. Una volta compilata la pagina, fare clic su Indietro per tornare alla schermata di accesso di Windows.

Installazione del Provider di credenziali

Procedere come descritto di seguito:

1. Individuare il download dei componenti di fornitura di CA Identity Manager o altro supporto di installazione.
2. Eseguire il programma di installazione in Agente.
Nota: se si esegue l'installazione del provider di credenziali in un sistema operativo a 64 bit, scegliere la versione a 64 bit del software.
3. Rispondere alle domande visualizzate dalla procedura guidata.
4. se si esegue l'installazione del provider di credenziali in un sistema operativo a 64 bit, scaricare [Microsoft Visual C++ 2008 SP1 \(64-bit\)](#).
5. Al completamento dell'installazione, configurare il provider delle credenziali.

Configurazione del Provider di credenziali

Per configurare un sistema su cui è stato installato il Provider di credenziali, è possibile utilizzare uno strumento di configurazione.

Come configurare il Provider di credenziali

1. In Windows Explorer, accedere alla directory su cui è stato installato il Provider di credenziali. Ad esempio:
C:\Programmi\CA\Identity Manager\Credential Provider
2. Fare doppio clic sul seguente file eseguibile:
CAIMCredProvConfig.exe

3. Selezionare il primo provider di credenziali come predefinito.

È possibile che la schermata di accesso non memorizzi le impostazioni se è in uso un secondo provider delle credenziali, come ad esempio quello di Microsoft. Se entrambi i provider vengono riconosciuti come provider predefiniti, la schermata di accesso sceglierà uno tra i due.

4. Disattivare il provider delle credenziali predefinito.
5. Compilare i campi nell'area Impostazioni provider di credenziali come indicato di seguito:

URL Link1

L'URL utilizzato quando un utente fa clic sul collegamento Password dimenticata?. Questo collegamento dovrebbe essere un URL che punta a un'interfaccia Web per la reimpostazione della password.

Di seguito viene riportato un collegamento di esempio:

```
http://eastern.local:8080/iam/im/environment/ca12/index.jsp?  
task.tag=forgottenpassword&facesViewId=/app/page/screen/  
fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%username%  
e%
```

Per questo URL, è necessario che nell'ambiente sia in funzione la registrazione automatica. Verificare inoltre che l'URL Self Service per l'ambiente CA Identity Manager funzioni dal sistema su cui si sta installando il provider di credenziali. Le occorrenze di %nomeutente% vengono sostituite dal valore nel campo del nome utente della finestra di dialogo di accesso.

URL Link2

L'URL utilizzato quando un utente fa clic sul collegamento Sblocca account. Questo collegamento dovrebbe essere un URL che punta a un'interfaccia Web per lo sblocco di un account da parte dell'utente. Le occorrenze di %nomeutente% vengono sostituite dal valore nel campo del nome utente della finestra di dialogo di accesso.

URL Link3

L'URL utilizzato quando un utente fa clic sul collegamento Nuovo account. Questo collegamento dovrebbe essere un URL che punta a un'interfaccia Web per la creazione di un account da parte dell'utente. Il tag %nome utente% non appartiene all'URL.

Utilizzo di un titolo personalizzato

Una stringa personalizzata sostituisce la stringa Powered by ...” visualizzata nella barra del titolo oppure nella finestra di dialogo Restituisci del provider delle credenziali. La posizione della stringa si basa sulle impostazioni di Section 508 Compliance (Conformità sezione 508).

Domain

Il nome del dominio di fornitura.

Section 508 Compliance (Use Return in menu) (Conformità sezione 508) (Utilizza Ritorno in menu)

Consente di attivare la funzione Ritorno in un menu. Se deselezionata, viene utilizzata la finestra di dialogo Ritorno.

Disattivazione di tutte le finestre di dialogo

Impedisce al browser protetto di generare nuove finestre di dialogo, come ad esempio finestre pop-up, messaggi di errore e finestre di dialogo di salvataggio. L'opzione di *disattivazione di tutte le finestre di dialogo* è abilitata per migliorare la protezione del sistema. Tuttavia, può essere disattivata per la risoluzione dei problemi.

6. Impostare i campi disponibili nell'area Impostazioni di protezione browser nel seguente modo:

Elenco Consenti

Schema di espressione regolare corrispondente agli URL per i quali l'accesso è sempre consentito.

Elenco Rifiuta

Schema di espressione regolare corrispondente agli URL per i quali l'accesso è sempre negato.

7. (Facoltativo) Fare clic su Esporta per esportare le impostazioni in un altro sistema.
8. Fare clic su OK per salvare le impostazioni.
9. Riavviare il sistema.

Impostazioni del registro di sistema per il Provider di credenziali

Se si sceglie di non utilizzare l'apposito strumento di configurazione, è possibile modificare le impostazioni del registro di sistema di Windows nella chiave seguente:

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]

link1_cmd

Questo collegamento deve essere l'URL cui verrà diretto l'utente facendo clic sul collegamento 1.

link2_cmd

Questo collegamento deve essere l'URL cui verrà diretto l'utente facendo clic sul collegamento 2. Ad esempio, è possibile aggiungere un collegamento che reindirizza gli utenti a un sito Web per sbloccare gli account.

Se link2_cmd viene lasciato vuoto, nella finestra di accesso di Windows verrà visualizzato solo link1_cmd.

link3_cmd

Questo collegamento dovrebbe caricare un URL che punta a un'interfaccia Web per la creazione di un account da parte dell'utente.

comp508

Consente di attivare la funzione Ritorno in un menu. Se deselezionata, viene utilizzata la finestra di dialogo Restituisci.

domain

Il nome del dominio di fornitura.

langdir

Posizione dei file DLL di lingua localizzati.

disablepwdcp

L'opzione Disattiva Provider di credenziali password Microsoft. 1 sta per disattivato. 0 sta per attivato.

CredentialProviderInstallPath

Il percorso completo della directory di installazione del Provider di credenziali.

configdir

Il percorso completo della directory di installazione del Provider di credenziali.

selectdefaultcredential

Selezionare il primo provider di credenziali come opzione predefinita. Sì è abilitato. No è disabilitato.

Impostazioni di registro del browser Cube

Il componente del browser protetto Cube è associato a diversi valori di registro che ne determinano il comportamento. Le seguenti impostazioni sono contenute nella seguente chiave di registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]

Tipo

REG_SZ(String)

404

Il percorso a un documento HTML standard da visualizzare se il computer non può contattare CA Identity Manager all'avvio.

default

La pagina predefinita per l'accesso se nessun collegamento è incluso nel comando Collegamento 1 o Collegamento 2.

allow

ACL di autorizzazione esplicita Schema di espressione regolare corrispondente agli URL per i quali l'accesso è sempre consentito. Per ulteriori informazioni, consultare la sezione [Elenchi di controllo di accesso Cube](#) (a pagina 120).

close

Consente di chiudere il browser protetto e riporta l'utente alla finestra di dialogo della password dimenticata per il provider di credenziali.

deny

ACL di negazione esplicita. Schema di espressione regolare corrispondente agli URL per i quali l'accesso è sempre negato. Per ulteriori informazioni, consultare la sezione [Elenchi di controllo di accesso Cube](#) (a pagina 120).

langdir

Posizione dei file DLL di lingua localizzati.

rejectinvalidcerts

Controlla che il provider di credenziali accetti solo i certificati SSL validi. Se impostata su No, questa opzione consente l'utilizzo di certificati SSL scaduti o non validi.

I valori validi per questa chiave sono *Si* e *No*.

unreachable

Consente il reindirizzamento a un URL se Cube rileva problemi di connettività.

Valore di esempio: file:///C:\unreachable.html

usecustomtitle

Questo consente di abilitare il titolo personalizzato per il provider di credenziali.

customtitle

Questo è un titolo che si desidera visualizzare nel provider di credenziali.

Creazione di elenchi di controllo di accesso ai cubi

Gli elenchi di controllo di accesso ai cubi sono modelli di espressioni regolari che consentono o negano in modo esplicito il permesso di passare ad un URL selezionato. Gli elenchi di controllo di accesso vengono valutati nell'ordine seguente:

1. Allow (il permesso viene inizialmente consentito in modo automatico)
2. Deny (gli URL negati vengono controllati in seconda istanza)

Esempi dell'elenco di controllo di accesso

"allow"=".pdf"

Consente la visualizzazione dei documenti PDF.

"deny"=".doc|.xls"

Impedisce l'accesso ai documenti di Microsoft Word ed Excel.

Personalizzazione del messaggio Powered by

È possibile che venga visualizzato un messaggio Powered by nella finestra di dialogo Restituisci o nell'opzione di menu Restituisci del Provider delle credenziali. È possibile modificare o rimuovere questo messaggio.

Per personalizzare il messaggio Powered by

1. Scaricare ResEdit, un editor di risorse dall'indirizzo <http://www.resedit.net>.
2. Avviare ResEdit.
3. Modificare il file 1033.dll nella cartella delle lingue.
4. Fare doppio clic sulla tabella delle stringhe.
5. Rimuovere o modificare l'ID risorsa 135, la versione inglese della risorsa per il messaggio.

Ripristino di una password per un accesso Windows

Dopo avere installato il provider di credenziali su un sistema Windows, verrà visualizzato il collegamento Password dimenticata? nella finestra di dialogo di accesso standard di Microsoft Windows. Utilizzare questo collegamento per ripristinare la password o visualizzare i suggerimenti per ricordarla.

Ripristino di una password per un accesso Windows

1. Fare clic su Accedi dalla finestra di dialogo Protezione di Windows. Viene visualizzata la finestra di dialogo di accesso di Windows.
2. Immettere un nome utente valido.
3. Fare clic su Password dimenticata?

Viene visualizzata la pagina di suggerimento password di CA Identity Manager.

Se viene ricordata la password, tornare alla finestra di dialogo di accesso per continuare. In caso contrario, eseguire l'operazione 4 per effettuare l'autenticazione con CA Identity Manager Self Service.

4. Digitare le risposte per le domande di autenticazione.

Nota: se non si conoscono le risposte a tutte le domande, fare clic su Richiedi in modo che la password possa essere ripristinata dall'amministratore.

Nella schermata successiva verrà quindi richiesto di modificare la password.

Installazione invisibile all'utente del provider di credenziali

Il provider di credenziali supporta la modalità di installazione invisibile all'utente. Le proprietà supportate sono sei.

LINK1

Fa riferimento al file SOFTWARE\CA\CAIMCredentialProvider\link1_cmd nel registro.

LINK2

Fa riferimento al file SOFTWARE\CA\CAIMCredentialProvider\link2_cmd nel registro.

LINK3

Fa riferimento al file SOFTWARE\CA\CAIMCredentialProvider\link3_cmd nel registro.

DOMAIN

Fa riferimento al file SOFTWARE\CA\CAIMCredentialProvider\domain nel registro.

COMP508

Fa riferimento al file SOFTWARE\CA\CAIMCredentialProvider\comp508 nel registro.

USECUSTOMTITLE

Fa riferimento al file SOFTWARE\CA\Cube\usecustomtitle nel registro.

CUSTOMTITLE

fa riferimento al file SOFTWARE\CA\Cube\customtitle nel registro.

REJECTINVALIDCERTS

fa riferimento al file SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts nel registro.

UNREACHABLE

fa riferimento alla posizione della pagina irraggiungibile.

La sintassi per impostare il valore di queste proprietà è la seguente:

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity  
Manager\Credential Provider\" LINK1="\<url>\\" LINK2="\<url>\\" LINK3="\<url>\\"  
COMP508="\yes\" REJECTINVALIDCERTS="\yes\" USECUSTOMTITLE="\yes\"  
CUSTOMTITLE="\custom cp title\""
```

oppure

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity  
Manager\Credential Provider\" LINK1="\<url>\\" LINK2="\<url>\\" LINK3="\<url>\\"  
COMP508="\yes\" USECUSTOMTITLE="\yes\" CUSTOMTITLE="\custom cp title\"  
SELECTDEFAULTCREDENTIAL="\yes\" UNREACHABLE="\<url>\\""
```

oppure

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR="C:\Program Files\CA\Identity  
Manager\Credential Provider\"  
LINK1="\<url>\\" LINK2="\<url>\\" LINK3="\<url>\\" COMP508="\yes\"  
USECUSTOMTITLE="\yes\" CUSTOMTITLE="\custom cp title\"  
SELECTDEFAULTCREDENTIAL="\yes\" UNREACHABLE="file:///[INSTALLDIR]<file  
name>\\" CUBE_ALLOW="\\" CUBE_DENY="\\""
```

[INSTALLDIR]

fa riferimento al valore della proprietà INSTALLDIR.

<url>

Specifica l'URL per un'attività di sblocco account o password dimenticata.

<file name>

Definisce il nome del file irraggiungibile.

CUBE_ALLOW

Fa riferimento all'attivazione dell'URL consentita da Cube.

CUBE_DENY

Fa riferimento alla restrizione per l'attivazione dell'URL da Cube.

Password di sincronizzazione sugli endpoint

È possibile installare un agente di sincronizzazione password su alcuni endpoint supportati da CA Identity Manager. L'agente intercetta le richieste di modifica password sull'endpoint e inoltra le modifiche al server di provisioning.

Sincronizzazione password su Windows

CA Identity Manager è in grado di intercettare la modifica di password di un account Windows nativo e di propagare la nuova password su un utente e su tutti gli account appartenenti a quell'utente.

Quando l'agente di sincronizzazione password rileva un tentativo di modifica password, l'agente intercetta la richiesta e la invia al server di provisioning. Il server di provisioning propaga quindi la nuova password sull'utente e sugli altri account associati a quell'utente.

La sincronizzazione di password ha i requisiti seguenti:

- L'agente di sincronizzazione delle password deve essere installato nel sistema in cui le modifiche delle password vengono intercettate.
- Il sistema deve essere gestito come un endpoint acquisito.
- La casella di controllo Agente di sincronizzazione password installato deve essere selezionata nella scheda Impostazioni endpoint.
- Gli account dei sistemi gestiti devono essere esplorati e correlati agli utenti di CA Identity Manager.
- L'ambiente deve consentire le modifiche di password provenienti dagli account di endpoint. Questa funzionalità viene abilitata dagli amministratori con accesso alla console di gestione.

Importante. Formulare le regole delle password con attenzione in modo che una password possa essere applicata a tutti i sistemi. Ad esempio, se la lunghezza richiesta per le password di Windows è di 12 caratteri, tutti i sistemi che accettano password fino a 10 caratteri rifiuteranno le modifiche durante la sincronizzazione.

Il server CA Identity Manager non rileva le restrizioni delle password nell'endpoint. Quando si lavora con gli account di endpoint, il criterio di password deve essere più rigoroso rispetto al criterio di password degli endpoint.

Installazione dell'Agente di sincronizzazione password

È possibile installare l'agente di sincronizzazione password su qualsiasi computer Windows gestito sul quale accedono utenti globali. Su questi sistemi l'agente viene eseguito in background.

Esecuzione del programma di installazione

Prendere nota dei requisiti seguenti:

- Il server di provisioning deve gestire il sistema nel quale si sta installando l'agente.
- Creare un utente che funga da Amministratore per le modifiche delle password: il nome suggerito è etapwsad. Questo utente deve avere il profilo PasswordAdministrator.
- Nel supporto di installazione esistono due agenti di sincronizzazione password di Windows: uno per Windows a 32 bit e uno per Windows a 64 bit. L'agente di sincronizzazione password a 32 bit non è supportato su Windows a 64 bit. FIPS è supportato solo dall'agente di sincronizzazione password a 32 bit.

Procedere come descritto di seguito:

1. Individuare il supporto di installazione di CA Identity Manager.
2. Accedere a \Agent\PasswordSync or \Agent\PasswordSync-x64.
3. Eseguire setup.exe.
4. Rispondere alla procedura guidata di configurazione come segue:
 - a. Nel campo del nome host, immettere il nome del sistema del server di provisioning.
 - b. Modificare la porta secondo necessità se il server di provisioning utilizza una porta non predefinita.

La porta LDAP suggerita, utilizzata per connettersi al server di provisioning, è la porta 20390.
 - c. Fare clic sul pulsante Find domain (Trova dominio) per recuperare il dominio del server di provisioning.
 - d. Se l'installazione del server di provisioning è configurata per il failover, seguire le istruzioni sullo schermo per aggiungere un elenco separato da virgole dei server.
 - e. Fare clic su Avanti.
 - f. Nel campo Amministratore immettere etapwsad come nome utente globale predefinito per l'agente di sincronizzazione password. Questo utente deve avere il profilo PasswordAdministrator. Non esiste per impostazione predefinita.
 - g. Nel campo Amministratore password immettere la password dell'amministratore.

- h. Fare clic su Avanti.
 - i. Dall'elenco a discesa Tipo di endpoint, selezionare il tipo di endpoint dell'host sul quale si sta installando l'agente.
 - j. Dall'elenco a discesa Nome endpoint, selezionare il nome dell'endpoint utilizzato al momento della creazione dell'endpoint nella console utente.
 - k. Fare clic su Configura.
5. Fare clic su Fine quando richiesto per completare l'installazione e riavviare.

Aggiornare l'endpoint nella console utente

Nella console utente, aggiornare l'endpoint per indicare che l'agente è stato installato.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Cercare l'endpoint su cui è installato l'agente.
3. Fare clic sulla scheda Impostazioni endpoint.
4. Selezionare la casella di controllo Agente di sincronizzazione password installato.

Abilitare un ambiente per la sincronizzazione di password

Dopo avere installato l'agente di sincronizzazione password, viene abilitato l'ambiente per la ricezione delle modifiche alle password effettuate sugli endpoint. Per questa attività, è necessario che l'amministratore disponga dell'accesso alla console di gestione e a CA Directory per abilitare l'ambiente per l'accettazione delle modifiche.

Procedere come descritto di seguito:

1. Per i nuovi utenti, utilizzare la console di gestione nel modo seguente:
 - a. Selezionare l'ambiente.
 - b. Selezionare Impostazioni avanzate, Provisioning.
 - c. Selezionare la casella di controllo Enable Password Changes from Endpoint.
2. Per gli utenti esistenti, impostare l'attributo eTPropagatePassword su 1 in CA Directory.

Configurazione di server alternativi per Agente di sincronizzazione password

Per configurare un server alternativo per Agente di sincronizzazione password, utilizzare la configurazione guidata dell'agente di sincronizzazione password.

Aggiunta di un server alternativo per Agente di sincronizzazione password

1. Eseguire PwdSyncConfig.exe situato in *cartella_sync_password\bin*.
2. Immettere i seguenti dati di configurazione:

Host

Specificare il nome host del server di fornitura principale.

Il campo URL server verrà popolato con il nome host specificato.

Porta LDAP

Specificare il numero di porta utilizzato dal computer durante la connessione al server di fornitura.

In CA Identity Manager il campo URL server verrà popolato con l'host e la porta specificati.

3. Fare clic sul pulsante Trova dominio per ottenere l'elenco dei domini.
4. Nella casella a discesa Dominio selezionare il nome del dominio e fare clic su Avanti.
5. Aggiungere il nome host e la porta dei server alternativi nel campo URL server utilizzando il formato seguente:

`ldaps://hostprincipale:20390,ldaps://hostalternativo1:20390`
6. Fare clic su Avanti.
7. Compilare i campi rimanenti nella configurazione guidata.

Modalità di funzionamento dell'agente di sincronizzazione password

Il processo di propagazione ha inizio quando gli utenti globali modificano la loro password su un sistema Windows utilizzando qualsiasi metodo. Una volta immessa la password, si verifica quanto segue:

1. Il sistema operativo Windows verifica che la password soddisfi i criteri di password. Se Windows non accetta la password, la richiesta di modifica viene rifiutata, viene visualizzato un messaggio di errore e non viene eseguita nessuna ulteriore azione, compresa la sincronizzazione.
2. Il sistema Windows trasmette la richiesta di modifica della password all'agente Sincronizzazione password di CA Identity Manager; se quest'ultimo è a sua volta configurato per il controllo della qualità delle password, inoltra la password al server di fornitura per il controllo della qualità della password. Se la password non soddisfa le regole di qualità di CA Identity Manager, la richiesta di modifica viene ignorata e viene visualizzato un messaggio di errore. La password di Windows rimane immutata e non viene eseguita alcuna sincronizzazione.

3. Una password che soddisfa le regole di qualità di Windows e CA Identity Manager viene inoltrata dall'agente di sincronizzazione password al server di fornitura affinché venga propagata.
4. CA Identity Manager aggiorna la password utente globale e la propaga ad alcuni o a tutti gli account associati all'utente globale.

Nota: i criteri di password per Windows e CA Identity Manager devono essere identici o coerenti, poiché i messaggi di errore visualizzati si basano sul criterio di password di Windows, anche se CA Identity Manager rifiuta la richiesta.

Il parametro di configurazione `password_update_timeout` (`eta_pwdsync.conf`) specifica per quanto tempo (in secondi) l'agente di sincronizzazione password deve attendere la conferma di propagazione della modifica della password proveniente dal server CA Identity Manager. Se il PSA non riceve una conferma entro questo periodo, procede come se la propagazione fosse avvenuta e registra un avviso (`eta_pwdsync.log`) in cui viene indicato che non è stato possibile verificare la propagazione della modifica della password. Il valore minimo del parametro è zero (0); in questo caso il PSA non attenderà la conferma. Per ulteriori informazioni, consultare la sezione relativa alla configurazione dell'agente di sincronizzazione della password (`eta_pwdsync.conf`) nella guida in linea di Manager fornitura.

Controllo della qualità delle password a livello di account

Il controllo della qualità delle password viene eseguito quando sugli endpoint gestiti vengono creati o modificati account, oppure quando vengono impostate password per l'utente globale. Il controllo della qualità delle password sugli account si limita a verifiche basate sui caratteri delle password. Le verifiche per gli utenti globali basate sulla cronologia delle modifiche recenti (frequenza di aggiornamento e di riutilizzo della password) non vengono eseguite sugli account poiché CA Identity Manager non registra tutte le modifiche delle password account. CA Identity Manager non dispone quindi di una cronologia di modifica delle password accurata sulla base della quale effettuare tali verifiche.

Il controllo delle password account è gestito dai seguenti parametri di configurazione del dominio:

- Endpoint type/Check Account Passwords (Tipo endpoint/Controllo password account)
- Tipo endpoint/Controllo password account vuote

Il valore di ciascun parametro specifica, per ciascun endpoint gestito, il livello di controllo da eseguire. L'endpoint può essere specificato nei seguenti modi:

```
ALL
-ALL
<Nomespaziodeinomi>
-<Nomespaziodeinomi>
<Nomespaziodeinomi>:<Nomedirectory>
-<Nomespaziodeinomi>:<Nomedirectory>
```

Laddove indicato, il segno meno (-) disattiva il parametro. Se invece è assente, il parametro è attivato. I formati [-]<Nomespaziodeinomi> controllano tutti gli endpoint del tipo di endpoint indicato, mentre i formati [-]<Nomespaziodeinomi>:<Nomedirectory> controllano gli endpoint singoli. I formati [-]ALL controllano tutti gli endpoint di tutti i tipi. Il valore predefinito di entrambi i parametri è -ALL.

Ciascuno di questi parametri può essere specificato più volte. Se lo stesso endpoint è specificato da più valori, verrà usato l'ultimo valore indicato. È possibile specificare innanzitutto regole generali e poi regole specifiche, così da ignorare le regole generali.

Il parametro di controllo delle password degli account consente una verifica equivalente al controllo di qualità delle password utente globale. Quando questo parametro è attivato per un endpoint, CA Identity Manager verifica le password presenti in una modifica richiesta relativa a un account esistente, inclusi i tentativi di impostare una password vuota. Durante la creazione di un account, se non viene fornita alcuna password, il controllo di qualità delle password non viene eseguito.

Il controllo di password account vuote consente di controllare anche le password vuote durante la creazione degli account. Se il profilo password è attivato e richiede una password lunga almeno un carattere, la creazione dell'account non potrà essere effettuata se non viene specificata una password. Questo parametro è disgiunto da Check Account Passwords (Controlla password account) perché per alcuni tipi di endpoint è ammesso creare un account senza password.

Nota: il controllo della qualità delle password account non viene eseguito per le password di account sincronizzati se la password fornita corrisponde alla password utente globale corrente.

Imposizione della qualità delle password

L'opzione Sincronizzazione password intercetta le richieste di modifica su sistemi nativi (ad esempio Windows NT/ADS) e le inoltra al server CA Identity Manager. Il server sincronizza la password utente globale e le password account associate all'utente globale. Sia le regole di CA Identity Manager che quelle del sistema nativo (Windows NT/ADS) relative alla qualità delle password per un profilo di password sono utilizzabili per imporre il controllo della qualità delle password.

Configurazione della sincronizzazione delle password

L'agente di sincronizzazione password viene configurato inizialmente durante l'installazione e può essere riconfigurato in qualunque momento mediante la procedura guidata di configurazione della sincronizzazione password. È possibile effettuare un ulteriore intervento di configurazione. Ad esempio, è possibile modificare le impostazioni per il controllo qualità delle password o modificare i timeout mediante il file `eta_pwdsync.conf`.

Il file si trova nella cartella `password_sync_folder\data\`. Tutte le chiavi di questo file di configurazione vengono impostate durante l'installazione dell'agente di sincronizzazione password. Pertanto, è necessario modificare queste chiavi solo se necessario. Per ulteriori informazioni, consultare il testo di questo file.

Importante. Come precauzione, creare un backup del file di configurazione prima di modificarlo.

Sezione [Server]

Chiave	Descrizione	Predefinito
host	Consente di specificare il server di dominio che gestisce la propagazione di password.	Nessuno
porta	Consente di specificare la porta di ascolto LDAP del server di provisioning.	20411
use_tls	Consente di specificare se TLS/SSL viene utilizzato per assicurare la comunicazione tra l'agente di sincronizzazione password e il server di provisioning.	Sì
admin_suffix	Consente di specificare il suffisso di dominio dell'utente di amministrazione utilizzato dall'agente di sincronizzazione password per accedere a CA Identity Manager.	Nessuno
admin	Consente di specificare il nome di account dell'utente di amministrazione utilizzato dall'agente di sincronizzazione password per l'accesso a CA Identity Manager.	Nessuno
password	Consente di specificare la password per il nome account specificato nella chiave di amministrazione.	Nessuno

Sezione [eTaDomain]

Chiave	Descrizione	Predefinito
Dominio	Consente di specificare il dominio di provisioning in cui è stato installato l'agente di sincronizzazione password.	Nessuno
etrust_suffix	Consente di specificare il suffisso per l'intero prodotto CA Identity Manager.	Nessuno
domain_suffix	Consente di specificare il suffisso di dominio per il dominio di provisioning.	Nessuno
endpoint type	Consente di specificare il tipo di endpoint in cui è stato installato l'agente di sincronizzazione password.	Nessuno
endpoint	Consente di specificare l'endpoint per il quale l'agente di sincronizzazione password intercetta le password.	Nessuno
endpoint_dn	Consente di specificare il nome distinto dell'endpoint.	Nessuno
container_dn	Consente di specificare il nome distinto del contenitore che contiene gli account le cui password vengono modificate.	Nessuno
acct_attribute_name	Consente di specificare il nome di attributo dell'account, ad esempio eTN16AccountName per Windows NT.	Dipende dal tipo di endpoint
acct_object_class	Consente di specificare l'objectClass degli account.	Dipende dal tipo di endpoint

Sezione [PasswordProfile]

Chiave	Descrizione	Predefinito
profile_enabled	Consente di specificare se la funzionalità di controllo del profilo della password è abilitata.	No
profile_dn	Consente di specificare se la procedura guidata di configurazione password genera un DN per il profilo della password.	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

Sezione [Timeout]

Chiave	Descrizione	Predefinito
search_acct_dn	Consente di specificare il valore di timeout quando si cerca il DN dell'account.	120 secondi
pwd_update	Consente di specificare il valore di timeout quando si propagano le password.	400 secondi
pwd_quality_check	Consente di specificare il valore di timeout (in secondi) quando si esegue il controllo di qualità delle password.	1

Sezione [Logs]

Chiave	Descrizione	Predefinito
log_file	Consente di specificare il file di registro che contiene i messaggi registrati provenienti dall'agente di sincronizzazione password.	..\Programmi\CA\Identity Manager Password Sync Agent
log_level	Consente di specificare il livello di registrazione. I valori validi sono: 1--Inizializzazione file 2--Aggiornamento password riuscito o non riuscito 3--Debug connessione 4--Analisi	0, per nessuna registrazione

Failover

Se il server di provisioning è inattivo o sovraccarico, è possibile che l'agente di sincronizzazione password esegua il failover su un altro server. Il failover richiede che più server di provisioning siano a disposizione dello stesso dominio e che l'agente utilizzi tali server.

La sezione che [configura l'agente per l'utilizzo di server alternativi](#) (a pagina 127) fornisce le istruzioni di configurazione.

Attivazione della registrazione dei messaggi

Per scoprire il motivo per il quale una modifica di password è stata rifiutata, consultare i messaggi di registro inviati dall'agente di sincronizzazione delle password. Tutti i messaggi registrati sono memorizzati nel file `eta_pwdsync.log`. Per impostazione predefinita, questo file si trova nella cartella `..\Program files\CA\CA Identity Manager Password Sync Agent`.

Il file contiene la registrazione dei seguenti messaggi:

- Messaggi di errore, che vengono sempre registrati.
- Messaggi di diagnostica (flusso dei processi, traccia), attivabili o disattivabili in base al valore del parametro `logging_enabled=yes|no` nel file `eta_pwdsync.conf`.

Per diagnosticare meglio i problemi, esaminare il file `eta_pwdsync.log` e il registro del server di fornitura in riferimento allo stesso periodo di tempo.

Il parametro di configurazione `log_level` è stato reso obsoleto, ma conservato per compatibilità con le versioni precedenti: `log_level=0` è ora `logging_enabled=no` e `log_level=anything else` è ora `logging_enabled=yes`. Se nel file di configurazione sono presenti sia i parametri nuovi che quelli obsoleti, l'impostazione esplicita del parametro `logging_enabled=yes|no` ha la precedenza sull'impostazione indiretta determinata dal parametro obsoleto `log_level=numero`.

Nota: l'elenco di connettori è stato incluso in `eta_pwdsync.log`, ma l'agente non fornisce più tale informazione.

Verifica dell'installazione

Una volta installato l'agente di sincronizzazione password, modificare una password sul sistema Windows per verificare che la password utente globale associata all'account venga a sua volta modificata.

Sincronizzazione password su UNIX e Linux

CA Identity Manager è in grado di intercettare la modifica della password di un account in un sistema UNIX o Linux e di propagarla a tutti gli altri account associati con il proprio utente globale. Il componente utilizzato per autenticare le password nei sistemi di protezione esterni viene chiamato PAM (Pluggable Authentication Module). Con PAM, CA Identity Manager autentica le password nei sistemi di protezione esterni in modo che gli utenti globali possano utilizzare le password di sistema esistenti per accedere a CA Identity Manager.

Sincronizzazione di password in UNIX

Viene fornito un modulo di sincronizzazione password che consente di rilevare eventi di modifica di password mediante il framework UNIX PAM. Il modulo di sincronizzazione password in UNIX informa il server di provisioning di eventuali modifiche di password. Il server di provisioning rileva l'utente globale associato e propaga le modifiche agli altri account collegati automaticamente.

I sistemi operativi UNIX che supportano il framework PAM includono:

- AIX v5.3 su piattaforma Power con PAM abilitato
- HP-UX v11.00 su una piattaforma PA-RISC e piattaforme Itanium® 2
- Solaris v2.6 e successive su piattaforme Sparc e Intel
- Linux a 32 bit con glibc v2.2 e successive su piattaforma s390 o Intel i386

Nota: nelle piattaforme Linux, il file binario test_sync deve trovarsi nel PERCORSO per tutti gli utenti, ma solo l'utente root, ovvero il titolare, deve disporre dei permessi di esecuzione.

Per aggiungere questa libreria al percorso per tutti gli utenti, includere questo comando nel file /etc/bashrc globale:

```
export PATH=$PATH:/etc/pam_CA_eta
```

Funzionamento di PAM di UNIX

Il processo seguente descrive le funzioni di PAM di UNIX:

1. Una password utente UNIX viene modificata per uno dei motivi seguenti:
 - Decisione dell'utente.
 - L'utente viene obbligato a modificare la password dalle impostazioni di sistema o da un intervento manuale.
 - La password dell'utente viene modificata da un amministratore.
2. La nuova password viene inviata al servizio di password del framework PAM.
3. Il servizio di password del framework PAM richiama la libreria PAM per aggiornare i file di protezione UNIX locali.
4. Il servizio di password del framework PAM richiama il modulo di sincronizzazione password UNIX (pam_CA_eta) per informare il server di provisioning della modifica della password.
5. Il server di provisioning aggiorna la password dell'utente globale associato e di tutti gli account associati all'utente globale.

Requisiti per l'utilizzo della sincronizzazione password in UNIX

I requisiti per l'utilizzo della funzionalità di sincronizzazione password in UNIX sono i seguenti:

- L'agente di sincronizzazione password UNIX deve essere installato sul sistema UNIX su cui si desidera rilevare le modifiche delle password.
- Gli agenti remoti UNIX e CAM devono essere installati sul sistema UNIX su cui risiede l'agente di sincronizzazione password UNIX.
- Il sistema deve essere gestito come un endpoint acquisito. È necessario selezionare la casella di controllo Agente di sincronizzazione password installato nelle proprietà dell'endpoint acquisito.
- Gli account dei sistemi gestiti devono essere esplorati e correlati agli utenti globali.
- L'ambiente deve consentire le modifiche di password provenienti dagli account di endpoint. Questa funzionalità viene abilitata dagli amministratori con accesso alla console di gestione.

Installazione della funzionalità PAM di UNIX

Eseguire la procedura seguente per installare PAM di UNIX.

Per installare la funzionalità PAM di UNIX

1. Selezionare il file del pacchetto che corrisponde alla propria piattaforma UNIX:

Sistema operativo UNIX	Nome file pacchetto
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. Trasferire il file del pacchetto scelto in una cartella temporanea (/tmp) sul server UNIX mediante FTP in modalità binaria o qualsiasi altro strumento di trasferimento file in grado di supportare i file binari. Una sessione di trasferimento di esempio può venire visualizzata come segue:

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. Accedere come utente root sul server UNIX ed estrarre il file del pacchetto:

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

Su Linux, utilizzare il comando:

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. Copiare la configurazione e i file TLS nella cartella di configurazione predefinita:

```
# cd pam_CA_eta-1.1
# mv pam_CA_eta /etc
```


5. Copiare il modulo pam_CA_eta nella cartella delle librerie di protezione:

Su AIX, utilizzare il comando:

```
# cp -p pam_CA_eta.o /usr/lib/security/
```

Su HP-UX, utilizzare il comando:

```
# cp -p libpam_CA_eta.1 /usr/lib/security/
```

Su HP-UX Itanium2, utilizzare il comando:

```
# cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
```

Su Linux i386 o s390, utilizzare il comando:

```
# cp -p pam_CA_eta.so /lib/security/
```

Su Solaris Sparc o Intel, utilizzare il comando:

```
# cp -p pam_CA_eta.so /usr/lib/security/
```

6. (Facoltativo) Copiare i programmi di verifica:

```
# cp -p test_* /etc/pam_CA_eta
```

```
# cp -p pam_test* (/usr)/lib/security/
```

Ulteriori informazioni

[Risoluzione dei problemi relativi alla sincronizzazione di password in UNIX](#) (a pagina 144)

Aggiornare l'endpoint nella console utente

Nella console utente, aggiornare l'endpoint per indicare che l'agente è stato installato.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Cercare l'endpoint su cui è installato l'agente.
3. Fare clic sulla scheda Impostazioni endpoint.
4. Selezionare la casella di controllo Agente di sincronizzazione password installato.

Abilitare un ambiente per la sincronizzazione di password

Dopo avere installato l'agente di sincronizzazione password, viene abilitato l'ambiente per la ricezione delle modifiche alle password effettuate sugli endpoint. Per questa attività, è necessario che l'amministratore disponga dell'accesso alla console di gestione e a CA Directory per abilitare l'ambiente per l'accettazione delle modifiche.

Procedere come descritto di seguito:

1. Per i nuovi utenti, utilizzare la console di gestione nel modo seguente:
 - a. Selezionare l'ambiente.
 - b. Selezionare Impostazioni avanzate, Provisioning.
 - c. Selezionare la casella di controllo Enable Password Changes from Endpoint.
2. Per gli utenti esistenti, impostare l'attributo eTPropagatePassword su 1 in CA Directory.

Configurazione della funzionalità di sincronizzazione password in UNIX

La configurazione della funzionalità di sincronizzazione password in UNIX richiede l'impostazione di parametri nei file seguenti:

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

Importante. Perché la password di un utente con privilegi avanzati sia archiviata nel file di configurazione pam_CA_eta.conf, è necessario che tale file possa essere letto solo dall'account principale. Notare che le impostazioni file nel file del pacchetto includono owner=root e mode=500 e che lo switch -p del comando cp le preserva durante l'installazione.

Configurazione del file pam_CA_eta.conf

Per configurare il file pam_CA_eta.conf, eseguire la procedura seguente.

Per configurare il file pam_CA_eta.conf

1. Accedere alla cartella /etc/pam_CA_eta.
2. Modificare il file pam_CA_eta.conf. Questo file di configurazione contiene la propria documentazione.

```
#
#  CA - CA Identity Manager
#
#  pam_CA_eta.conf
#
#  Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional
#               alternate server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
#               server
# value: a valid TCP/IP port number
# default: 20390
# port 20390

# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP
operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#               server is used.
#               Cloud based server is accessed by proxying the requests
#               through the on-premise CS, requiring use of remote-server
#               set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity
Manager server
# value: a numeric value
# default: 100
# size-limit 100

# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta

# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain    im

# keyword: user
# description: the CA Identity Manager Global User name used to bind to the
CA Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin

# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager
Global User
# value: the password of the above Global User
# default: no default
```

password SECRET

keyword: directory-type
description: the CA Identity Manager Unix Endpoint type of this Unix server
value: ETC or NIS
default: ETC
endpoint-type ETC

keyword: endpoint-name
description: the CA Identity Manager Unix Endpoint name of this Unix server
value: a valid Unix Endpoint name string
default:
ETC: the result of the "hostname" command (ie: gethostname() system call)
NIS: "domain [hostname]" where "domain" is the result of the "domainname" command
(ie: getdomainname() system call) and "hostname" the result of the "hostname" command (ie: gethostname() system call)
endpoint-name dirname

keyword: tls-cacert-file
description: the name of the CA Identity Manager CA certificate file
value: a valid full path file name
default: /etc/pam_CA_eta/eta2_cacert.pem
tls-cacert-file /etc/pam_CA_eta/eta2_cacert.pem

keyword: tls-cert-file
description: the name of the CA Identity Manager client certificate file
value: a valid full path file name
default: /etc/pam_CA_eta/eta2_clientcert.pem
tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem

keyword: tls-key-file
description: the name of the CA Identity Manager client private key file
value: a valid full path file name
default: /etc/pam_CA_eta/eta2_clientkey.pem
tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem

keyword: tls-random-file
description: the name of the "pseudo random number generator" seed file
value: a valid full path file name
default: /etc/pam_CA_eta/prng_seed
tls-random-file /etc/pam_CA_eta/prng_seed

keyword: use-status

```
# description: this module will exit with a non-zero status code in case of
failure.
# value: yes or no
# default: no
# use-status no

# keyword: verbose
# description: this module will display informational or error messages to
the user.
# value: yes or no
# default: yes
# verbose yes
```

Nota: i parametri di server, dominio e password non hanno un valore predefinito e devono essere aggiornati.

Configurare il file pam.conf

Il file /etc/pam.conf è il file di configurazione PAM principale. È necessario modificare il file per inserire una riga nello stack del servizio di password. Su alcuni sistemi di Linux, il file pam.conf viene sostituito da /etc/pam.d. In questo modo, sarà necessario modificare il file /etc/pam.d/system-auth.

Per configurare il file pam.conf

1. Se si sta configurando il modulo PAM su un sistema Linux appropriato, accedere alla directory /etc o alla directory /etc/pam.d.
2. Modificare il file pam.conf per inserire una riga di sincronizzazione password nello stack del servizio di password. Per le configurazioni specifiche per le piattaforme, consultare gli esempi seguenti:

```
passwd password required /usr/lib/security/pam_unix.so
```

```
passwd password optional /usr/lib/security/pam_CA_eta.so
```

3. (Facoltativo) È possibile aggiungere i parametri facoltativi seguenti nella riga del modulo pam_CA_eta:

config=/path/file

Indica la posizione di un file di configurazione alternativo.

syslog

Invia messaggi di errore e informativi al servizio syslog locale.

trace

Genera un file di traccia per ogni operazione di aggiornamento di password. I file di traccia vengono denominati /tmp/pam_CA_eta-trace.<nnnn> dove <nnnn> è il numero PID del processo di password.

4. Implementare le seguenti modifiche alla configurazione specifiche per le piattaforme:

Per i sistemi AIX, aggiungere le righe seguenti alla fine del file /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login password optional /usr/lib/security/pam_CA_eta.so syslog
passwd password optional /usr/lib/security/pam_CA_eta.so syslog
rlogin password optional /usr/lib/security/pam_CA_eta.so syslog
su password optional /usr/lib/security/pam_CA_eta.so syslog
telnet password optional /usr/lib/security/pam_CA_eta.so syslog
sshd password optional /usr/lib/security/pam_CA_eta.so syslog
OTHER password optional /usr/lib/security/pam_CA_eta.so syslog
```

Per i sistemi HP-UX, aggiungere le righe seguenti alla fine del file /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login password optional /usr/lib/security/libpam_CA_eta.1 syslog
passwd password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional /usr/lib/security/libpam_CA_eta.1 syslog
OTHER password optional /usr/lib/security/libpam_CA_eta.1 syslog
```

Per i sistemi HP-UX Itanium2, aggiungere le righe seguenti alla fine del file /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login password optional /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

```
passwd password optional /usr/lib/security/$ISA/libpam_CA_etc.1 syslog
dtlogin password optional /usr/lib/security/$ISA/libpam_CA_etc.1 syslog
dtaction password optional /usr/lib/security/$ISA/libpam_CA_etc.1 syslog
OTHER password optional /usr/lib/security/$ISA/libpam_CA_etc.1 syslog
```

Per i sistemi Sun Solaris, aggiungere la riga pam_CA_etc dopo la riga pam_unix esistente:

```
#
# Password management
#
other password required /usr/lib/security/pam_unix.so.1
other password optional /usr/lib/security/pam_CA_etc.so syslog
```

Per i sistemi Linux, aggiungere la riga pam_CA_etc tra le righe pam_cracklib e pam_unix esistenti:

```
password required /lib/security/pam_cracklib.so retry=3 type=
password optional /lib/security/pam_CA_etc.so syslog
password sufficient /lib/security/pam_unix.so nullok use_authok md5
shadow
password required /lib/security/pam_deny.so
```

5. Per i sistemi AIX, modificare il file /etc/security/login.cfg per impostare auth_type = PAM_AUTH. In questo modo, si abilita il framework PAM che non è abilitato per impostazione predefinita. Si tratta di un'impostazione di runtime, pertanto non è necessario riavviare il sistema perché abbia effetto.

Risoluzione dei problemi relativi alla sincronizzazione di password in UNIX

È possibile risolvere gli errori della funzionalità PAM di UNIX mediante syslog e i messaggi di traccia ed eseguendo test sulla configurazione, la connessione LDAP/TLS, la sincronizzazione di password e il framework PAM.

Ulteriori informazioni

[Attivazione dei messaggi syslog](#) (a pagina 144)

[Attivazione dei messaggi di traccia](#) (a pagina 145)

Attivazione dei messaggi syslog

Aggiungere il parametro syslog alla riga pam_CA_etc nel file /etc/pam.conf per consentire al modulo pam_CA_etc di generare messaggi di errore e informativi. Quando l'opzione di registrazione è in uso, l'amministratore UNIX vede i messaggi informativi nel file syslog ogni volta che un account UNIX modifica la password. Tali messaggi forniscono di solito informazioni sufficienti per diagnosticare i problemi di base.

È possibile impostare questa opzione in modo permanente sui sistemi di produzione, in quanto non richiede molte più risorse di quando viene eseguita in modalità invisibile.

Attivazione dei messaggi di traccia

Se i messaggi syslog non forniscono informazioni sufficienti, la modalità di traccia può fornire più dettagli. Per ciascuna operazione di aggiornamento di password, il modulo di traccia genera un file denominato `/tmp/pam_CA_eta-trace.<nnnn>` (dove `<nnnn>` è il PID del processo `passwd`) con una voce per la maggior parte delle chiamate di funzione utilizzate dal modulo e per i dati utilizzati o ripristinati da tali funzioni.

Anche se i file di traccia possono essere letti solo dall'account principale, essi contengono le nuove password non crittografate. Per questo motivo, questo parametro non deve essere utilizzato in modo permanente su un sistema di produzione.

Verifica del file di configurazione

È possibile utilizzare lo strumento `test_config`, che si trova nella directory `/etc/pam_CA_eta`, per verificare il file di configurazione. Per prima cosa, configurare la struttura delle cartelle nel modo seguente:

1. Spostare la cartella `pam_CA_eta` in `/etc`.
2. Copiare tutto quello che si trova in `pam_CA_eta-1.1` in `/etc/pam_CA_eta`.

Di seguito viene riportata una riga di comando di esempio:

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

Di seguito viene riportato un esempio di sessione:

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

Come visualizzato nell'output del comando, è stato generato un file di traccia che contiene tutti i dettagli dell'analisi del file di configurazione.

Visualizzare il servizio CAM

È possibile eseguire la procedura seguente per scoprire chi ha avviato il servizio.

Per visualizzare il servizio CAM

1. Accedere al computer UNIX come root mediante il client Telnet o SSH.
2. Immettere il seguente comando UNIX:

```
ps -ef | grep cam
```

Verrà visualizzata una pagina simile alla seguente:

```
root 13822          1 11 11:30:12 ?    0:00 cam
```

```
root 13843 13753   3 11:56:31 pts/5  0:00 grep cam
```

Nota: se l'utente root del sistema non avvia i servizi, questi sembreranno avviati, ma non sarà possibile utilizzarli. CA Identity Manager genera il messaggio seguente:
Autorizzazione negata: l'utente deve essere root.

Verifica della connessione LDAP/TLS

È possibile utilizzare lo strumento `test_ldap`, situato nella directory `/etc/pam_CA_eta`, per verificare la connessione al server di provisioning (mediante i parametri del file di configurazione). Di seguito viene riportata una riga di comando di esempio:

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

Di seguito viene riportato un esempio di sessione:

```
./test_ldap [config=/path/to/config_file]
```

```
# ./test_ldap: succeeded
```

```
Trace file is /tmp/test_ldap-trace.1277
```

Come visualizzato nell'output del comando, è stato generato un file di traccia che contiene tutti i dettagli dell'analisi del file di configurazione e della connessione al server di provisioning.

Verifica della sincronizzazione di password

Per verificare che l'aggiornamento della password di un account locale venga propagato correttamente dal server di provisioning, è possibile utilizzare lo strumento `test_sync`, situato nella cartella `/etc/pam_CA_eta`. Di seguito viene riportata una riga di comando di esempio:

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

Di seguito viene riportato un esempio di sessione:

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA Identity Manager password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA Identity Manager password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

Come viene mostrato nell'output del comando, è stato generato un file di traccia che contiene tutti i dettagli dell'analisi del file di configurazione, della connessione al server di provisioning e dell'aggiornamento dell'account.

Quando si utilizza la modalità dettagliata (mediante il parametro `verbose yes` predefinito nel file di configurazione), il comando fornisce messaggi informativi e di possibili errori relativi alla propagazione delle password.

Verifica del framework PAM

Una libreria di test PAM è disponibile per verificare che le modifiche alle password vengano rilevate correttamente dal framework PAM.

Per verificare il framework PAM

1. Copiare il file `pam_test` nella cartella `/usr/lib/security(/hpux32)`.
2. Aggiungere una riga di classe password per la libreria `pam_test` senza parametri.

Di seguito viene riportato un esempio per Solaris:

```
other password optional /usr/lib/security/pam_test
```

3. Emettere un comando `passwd` su un utente di prova e cercare la riga con tag `pam_test[<pid>]` nel file `syslog`.

L'output del comando mostra il nome del file di traccia generato, ad esempio:

```
pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
```

Sincronizzazione password su OS400

L'agente di sincronizzazione password consente di propagare agli altri account gestiti da CA Identity Manager le modifiche alle password eseguite nel sistema endpoint OS/400. L'agente di sincronizzazione password funziona nel modo seguente:

1. Installare ed eseguire l'agente sul sistema endpoint OS/400.
Come parte dell'installazione, il programma viene registrato con il sistema OS/400 in modo che quando gli utenti modificano le password, l'agente invia le modifiche delle password al server di provisioning.
2. Il server di provisioning propaga la modifica della password agli account associati.
Le modifiche delle password iniziate dal comando Change Password (CHGPWD) o dalla API Change Password (QSYCHGPW) vengono ricevute dall'agente.
3. L'agente registra l'esito positivo o negativo dell'operazione in un file di registro in PWDSYNCH/LOG.

Per installare l'agente di sincronizzazione della password:

1. Individuare il supporto di installazione del componente di provisioning.
2. Eseguire il programma di installazione dell'agente di sincronizzazione password o OS/400 in \Agent
3. Attenersi alle istruzioni visualizzate sullo schermo per completare l'installazione.

Nota: le istruzioni di installazione nel collegamento del software dell'agente di endpoint sono incluse nelle sezioni seguenti.

Installare l'agente di sincronizzazione password di OS400

È necessario disporre dei privilegi *ADDOBJ e dei requisiti seguenti perché l'agente possa ricevere le notifiche di modifica password:

- È necessario impostare il valore di sistema QPWDVLDPGM su *REGFAC
- È necessario registrare il programma con il comando WRKREGINF
EXITPNT(QIBM_QSY_VLD_PASSWRD)
- L'ambiente deve consentire le modifiche di password provenienti dagli account di endpoint. Questa funzionalità viene abilitata dagli amministratori con accesso alla console di gestione.

L'agente viene avviato solo quando viene effettuata una modifica della password. Per modificare la password, emettere il comando CHGPWD.

Nota: è necessario contrassegnare l'utente globale per la sincronizzazione di password.

Su iSeries

1. Accedere come utente con privilegi *ALLOBJ e *SECADM (ad esempio, QSECOFR).
2. Creare un ruolo chiamato PWDSYNCH:

```
CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
```

Nota: come misura di protezione, l'utente viene creato con la password scaduta.

3. Creare un savefile per archiviare il pacchetto di installazione in una libreria a scelta (ad esempio, MYLIB):

```
CRTSAVF MYLIB/PWDSYNCH
```

4. Sul computer Windows in cui si trova il savefile, utilizzare l'FTP per trasferire il savefile nel sistema iSeries:

```
ftp <hostname>
binario
cd MYLIB
put PWDSYNCH.FILE
```

5. Sul sistema iSeries, estrarre il programma dal savefile:

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

Questo comando estrae e installa l'agente di sincronizzazione nella libreria PWDSYNCH.

6. Verificare l'installazione:

```
DSPLIB PWDSYNCH
```

Vengono visualizzati gli oggetti seguenti:

Oggetto	Tipo	Ambiente
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Configurare iSeries per l'utilizzo di PWDSYNCH come programma di uscita di convalida password:

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. Sull'iSeries, specificare i parametri di connessione per il server di connessione CA IAM:

```
EDTF FILE(PWDSYNCH/CONFIG)
```

Installare l'agente di sincronizzazione password di OS400

È necessario disporre dei privilegi *ADDOBJ e dei requisiti seguenti perché l'agente possa ricevere le notifiche di modifica password:

- È necessario impostare il valore di sistema QPWDVLDPGM su *REGFAC
- È necessario registrare il programma con il comando WRKREGINF
EXITPNT(QIBM_QSY_VLD_PASSWRD)
- L'ambiente deve consentire le modifiche di password provenienti dagli account di endpoint. Questa funzionalità viene abilitata dagli amministratori con accesso alla console di gestione.

L'agente viene avviato solo quando viene effettuata una modifica della password. Per modificare la password, emettere il comando CHGPWD.

Nota: è necessario contrassegnare l'utente globale per la sincronizzazione di password.

Su iSeries

1. Accedere come utente con privilegi *ALLOBJ e *SECADM (ad esempio, QSECOFR).
2. Creare un ruolo chiamato PWDSYNCH:

```
CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
```

Nota: come misura di protezione, l'utente viene creato con la password scaduta.

3. Creare un savefile per archiviare il pacchetto di installazione in una libreria a scelta (ad esempio, MYLIB):

```
CRTSAVF MYLIB/PWDSYNCH
```

4. Sul computer Windows in cui si trova il savefile, utilizzare l'FTP per trasferire il savefile nel sistema iSeries:

```
ftp <hostname>  
binario  
cd MYLIB  
put PWDSYNCH.FILE
```

5. Sul sistema iSeries, estrarre il programma dal savefile:

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

Questo comando estrae e installa l'agente di sincronizzazione nella libreria PWDSYNCH.

6. Verificare l'installazione:

```
DSPLIB PWDSYNCH
```

Vengono visualizzati gli oggetti seguenti:

Oggetto	Tipo	Ambiente
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

- Configurare iSeries per l'utilizzo di PWDSYNCH come programma di uscita di convalida password:

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```
- Sull'iSeries, specificare i parametri di connessione per il server di connessione CA IAM (CA IAM CS):

```
EDTF FILE(PWDSYNCH/CONFIG)
```

Aggiornare l'endpoint nella console utente

Nella console utente, aggiornare l'endpoint per indicare che l'agente è stato installato.

Procedere come descritto di seguito:

- Accedere alla console utente.
- Cercare l'endpoint su cui è installato l'agente.
- Fare clic sulla scheda Impostazioni endpoint.
- Selezionare la casella di controllo Agente di sincronizzazione password installato.

Abilitare un ambiente per la sincronizzazione di password

Dopo avere installato l'agente di sincronizzazione password, viene abilitato l'ambiente per la ricezione delle modifiche alle password effettuate sugli endpoint. Per questa attività, è necessario che l'amministratore disponga dell'accesso alla console di gestione e a CA Directory per abilitare l'ambiente per l'accettazione delle modifiche.

Procedere come descritto di seguito:

- Per i nuovi utenti, utilizzare la console di gestione nel modo seguente:
 - Selezionare l'ambiente.
 - Selezionare Impostazioni avanzate, Provisioning.
 - Selezionare la casella di controllo Enable Password Changes from Endpoint.
- Per gli utenti esistenti, impostare l'attributo eTPropagatePassword su 1 in CA Directory.

Configurazione SSL

Il protocollo SSL viene utilizzato per crittografare la comunicazione tra l'agente di sincronizzazione e il server di provisioning. Questo è importante per l'agente di sincronizzazione perché il protocollo SSL invia password nella rete. Si consiglia di utilizzare sempre il protocollo SSL.

L'agente di sincronizzazione deve ritenere attendibile il certificato del server di provisioning per potersi connettere a SSL. Pertanto è necessario che il certificato sia installato sul computer iSeries e configurato in modo che il certificato sia ritenuto attendibile dall'agente di sincronizzazione. Queste attività vengono eseguite da Digital Certificate Manager, un componente facoltativo di OS/400. Consultare la documentazione di OS/400 per informazioni sull'installazione e la configurazione di Digital Certificate Manager.

Installazione del certificato del server di provisioning

Per utilizzare SSL, è necessario installare i seguenti componenti del sistema operativo sul computer iSeries:

- Programma provider di accesso crittografico con licenza (5722 AC3)
- Digital Certificate Manager (Opzione 34 di OS/400)
- Server IBM HTTP per iSeries (5722 DG1)

Su iSeries

1. Caricare il certificato del server di provisioning dal computer del server di provisioning a iSeries. È possibile trovare il certificato in:

C:\Programmi\CA\Identity Manager\Provisioning
Server\Data\Tls\server\et2_cacert.pem
2. Accedere a DCM.

Utilizzando un browser Web, accedere su `http://<hostname>:2001`. Quando viene richiesto, accedere come QSECOFR e fare clic su Digital Certificate Manager.
3. Fare clic su Select a Certificate Store (Seleziona un archivio certificati) e selezionare l'archivio certificati di *SYSTEM. Se questo archivio non esiste, creare un archivio chiamato *SYSTEM e immettere la password dell'archivio certificati.

4. Importare il certificato come Certificato dell'autorità di certificazione mediante DCM.

Fare clic su Manage Certificates (Gestisci certificati), Importa certificato. Selezionare l'opzione Certificate Authority (CA) (Autorità di certificazione (CA)) e immettere il nome del file del certificato del server di provisioning. (Questa è la posizione in cui è stato caricato il certificato al passaggio 1). Immettere l'etichetta Server di provisioning per il certificato.

5. Dopo avere importato il certificato dell'autorità di certificazione nel KeyStore *SYSTEM dell'endpoint, assicurarsi che il client di IBM Directory QIBM_GLD_DIRSrv_CLIENT possa accedere al KeyStore *SYSTEM. In caso contrario, la chiamata di inizializzazione SSL di PSA non verrà completata.
6. Configurare l'applicazione client dei servizi directory in modo che ritenga attendibile il certificato del server di provisioning aprendo Manage applications (Gestisci applicazioni), Define CA Trust list (Definisci elenco attendibilità dell'autorità di certificazione) e scegliendo Directory Services Client (Client dei servizi directory).

Il certificato del server di provisioning viene elencato qui se è stato importato correttamente al passaggio 4.

Fare clic su Attendibile per il certificato del server di provisioning, quindi fare clic su OK.

7. Concedere l'autorizzazione di lettura PUBLIC ai file SSL e l'accesso in lettura all'archivio certificati *SYSTEM:

(/QIBM/userdata/ICSS/Cert/Server/default.kdb)

Concedere l'autorizzazione di lettura ed esecuzione alla cartella padre

(/QIBM/userdata/ICSS/Cert/Server)

Nota: l'adozione dell'autorità dell'utente PWDSYNCH non funziona nel file system /, pertanto è necessario concedere l'accesso a tutti gli utenti.

Disinstallazione dell'agente di sincronizzazione password

Se è necessario disinstallare l'agente di sincronizzazione password, seguire questa procedura.

Dal punto di uscita di convalida della password

1. Rimuovere PWDSYNCH:

```
RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
```

2. Eliminare la libreria dell'agente di sincronizzazione:

```
DLTLIB PWDSYNCH
```

3. Eliminare l'utente PWDSYNCH

DLTUSRPRF PWDSYNCH

4. Rimuovere il certificato del server di provisioning seguendo le istruzioni SSL per accedere a DCM e lavorare con l'archivio certificati *SYSTEM:

Fare clic su Manage Certificates (Gestisci certificati), Delete certificate (Elimina certificato) e selezionare Certificate Authority (CA) (Autorità di certificazione (CA))

Selezionare il certificato del server di provisioning e fare clic su Elimina.

È necessario impostare correttamente il parametro dell'agente di password OS/400

Il valore del parametro pwd_case_action deve essere impostato correttamente per garantirne il corretto funzionamento. I valori corretti includono:

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

Se pwd_case_action = [invalid value], per la password verranno impostate le lettere maiuscole.

Nota: Se viene impostato il flag pwd_case_action su pwd_to_uppercase o pwd_to_lowercase nel file di configurazione OS400 PSA, la password potrebbe non essere propagata all'utente globale se le password fornite non sono conformi alle impostazioni del criterio di password nel server di provisioning. Ad esempio, per alcuni criteri di password potrebbe essere necessario che i valori di password contengano almeno 1 valore in lettere maiuscole o minuscole.

Nota: prendere nota del valore di sistema QPWDLVL (Livello di password) quando si configura l'agente di sincronizzazione password

- Quando QPWDLVL è impostato su 0 (valore predefinito) nel sistema AS400, sono supportate le password con una lunghezza compresa tra 1 e 10 caratteri maiuscoli.
- Quando QPWDLVL viene impostato su 2 o 3, sono consentite password di lunghezza compresa tra 1 e 128 caratteri e con un misto di lettere maiuscole e minuscole.

Per impostazione predefinita, PSA propaga la password non modificata al server di provisioning. Tuttavia, indipendentemente dal valore di QPWDLVL, è possibile obbligare PSA a propagare password con lettere maiuscole o minuscole impostando pwd_case_action su pwd_to_uppercase o pwd_to_lowercase.

Capitolo 6: Gruppi

È possibile creare diversi tipi di gruppi o una combinazione di essi:

- Gruppo statico: elenco di utenti che vengono aggiunti in modo interattivo
- Gruppo dinamico: gli utenti appartengono al gruppo se soddisfano una query LDAP (è richiesta una directory LDAP come archivio utenti)

Nota: Il campo Query gruppo dinamico non viene incluso nell'attività Crea gruppo o in altre attività di gruppo anche se esiste nel directory.xml di un gruppo. Il campo Query gruppo dinamico viene incluso nell'attività con la modifica della schermata di profilo associata.

- Gruppo nidificato: gruppo contenente altri gruppi (è richiesta una directory LDAP come archivio utenti)

Nota: Per visualizzare i gruppi statici, dinamici e nidificati a cui appartiene un utente, utilizzare la scheda Gruppi dell'oggetto Utente. La scheda è presente nelle attività di visualizzazione e modifica utente per impostazione predefinita.

Questa sezione contiene i seguenti argomenti:

[Creazione di un gruppo statico](#) (a pagina 155)

[Creazione di un gruppo dinamico](#) (a pagina 156)

[Parametri di Query gruppo dinamico](#) (a pagina 157)

[Creazione di un gruppo nidificato](#) (a pagina 159)

[Esempio di gruppi statici, dinamici e nidificati](#) (a pagina 161)

[Amministratori gruppo](#) (a pagina 162)

Creazione di un gruppo statico

È possibile associare una raccolta di utenti in un *gruppo statico*. La gestione del gruppo statico consiste nell'aggiunta o nella rimozione di singoli utenti nell'elenco di appartenenza al gruppo. Per visualizzare l'elenco dei membri di un gruppo, utilizzare la scheda Appartenenza, inclusa per impostazione predefinita nelle attività Visualizza gruppo e Modifica gruppo.

Nota: nella scheda Appartenenza vengono visualizzati solo i membri aggiunti esplicitamente al gruppo, non i membri aggiunti in modo dinamico.

Come creare un gruppo statico

1. Nella console utente, selezionare Gruppi, Crea gruppo.
2. Scegliere se creare un nuovo gruppo o una copia di un gruppo esistente e fare clic su **OK**.

3. Nella scheda Profilo, immettere un nome gruppo, un'organizzazione, una descrizione e un nome dell'amministratore del gruppo.
4. Fare clic sulla scheda Appartenenza.
5. Fare clic su Aggiungi un utente.
6. Cercare gli utenti da includere.
7. Inserire un segno di spunta accanto agli utenti e fare clic su Seleziona.
8. Fare clic su Inoltra.

Creazione di un gruppo dinamico

È possibile creare un *gruppo dinamico* definendo una query filtro LDAP mediante la console utente per determinare in modo dinamico l'appartenenza al gruppo durante il runtime senza dover ricercare e aggiungere i singoli utenti.

Se ad esempio si desidera generare un gruppo con tutti i dipendenti statunitensi di NeteAuto, è possibile definire un filtro di ricerca LDAP analogo al seguente nel campo Query gruppo dinamico della console utente:

```
ldap:///cn=Employees,o=NeteAuto,c=US??sub
```

Inoltre, è possibile modificare questa query per individuare dipendenti fuori dagli Stati Uniti.

In [Esempio di gruppi statici, dinamici e nidificati](#) (a pagina 161) vengono illustrati esempi di un gruppo creato mediante gruppi statici, dinamici e nidificati.

Il campo Query gruppo dinamico viene incluso nell'attività con la modifica della schermata di profilo associata. Non è incluso per impostazione predefinita nell'attività Crea gruppo.

Nota: per abilitare i gruppi dinamici, gli amministratori di sistema configurano il supporto nel file di configurazione della directory (directory.xml):

- Aggiungere l'elemento GroupTypes alla sezione Comportamento dei gruppi di directory nella maniera seguente:

```
<GroupTypes type=type>
```

type può corrispondere a [NESTED](#) (a pagina 159), DYNAMIC oppure ALL.

L'elemento GroupTypes rispetta l'uso delle lettere maiuscole e minuscole.

- Eseguire il mapping dell'attributo noto %DYNAMIC_GROUP_MEMBERSHIP% su un attributo fisico esistente in un archivio utenti.

Per creare un gruppo dinamico

1. Nella console utente, selezionare Gruppi, Crea gruppo.
2. Scegliere se creare un nuovo gruppo o una copia di un gruppo esistente e fare clic su **OK**.
3. Nella scheda Profilo, immettere un nome gruppo, un'organizzazione, una descrizione e un nome dell'amministratore del gruppo.
4. Immettere un filtro di ricerca LDAP come nell'esempio seguente nel campo Query gruppo dinamico:

```
ldap:///cn=Employees,o=NeteAuto,c=US??sub?
```

5. Fare clic su Inoltra.

Nota: solo un amministratore con l'attività Modifica gruppo può modificare l'appartenenza dinamica a un gruppo.

Parametri di Query gruppo dinamico

Nella ricerca è possibile utilizzare i parametri di query dinamica seguenti:

```
ldap:///<ricerca_DN_di_base>??<ambito_ricerca>?<filtroricerca>
```

- *<ricerca_DN_di_base>* è il punto da cui iniziare la ricerca nella directory LDAP. Se non viene specificato il DN base nella query, l'organizzazione del gruppo viene assunta come DN base predefinito.
- *<ambito_ricerca>* specifica la portata della ricerca e comprende:
 - *sub* -- Restituisce voci al livello del DN base e inferiore
 - *one* -- Restituisce voci un livello al di sotto del DN base specificato nell'URL. (impostazione predefinita).
 - *base* -- Utilizza *one*, ignorando *base* come opzione di ricerca.

L'utilizzo di *one* o *base* consente di ottenere solo gli utenti nell'organizzazione DN base.

Con *sub* si ottengono invece tutti gli utenti all'interno dell'organizzazione DN base e tutte le sotto-organizzazioni nella struttura.

- *<filtroricerca>* è il filtro da applicare alle voci nell'ambito della ricerca. Quando si immette un filtro di ricerca, utilizzare la sintassi di query LDAP standard, come segue:

(<operatore logico><confronto><confronto...>)

- <operatore logico> è uno dei seguenti:

O logico: |

E logico: &

NON logico: !

- <confronto> indica <attributo><operatore><valore>

Ad esempio:

(&(city=milano)(state=Italia))

Il filtro di ricerca predefinito è (objectclass=*).

Tenere presente quanto segue durante la creazione di una query dinamica:

- il prefisso "ldap" deve essere in lettere minuscole, ad esempio:
ldap:///o=MyCorporation??sub?(title=Manager)
- Non è possibile specificare il nome host del server LDAP o il numero porta. Tutte le ricerche si eseguono nella directory LDAP associata all'ambiente.

La tabella seguente include esempi di query LDAP:

Descrizione	Query
Tutti gli utenti che sono responsabili.	ldap:///o=MyCorporation??sub?(title=Manager)
Tutti i responsabili nella filiale di New York Ovest	ldap:///o=MyCorporation??one?(&(title=Manager)(roomNumber=NYWest))
Tutti i tecnici con cellulare	ldap:///o=MyCorporation??one? (&(employeetype=technician)(mobile=*))
Tutti i dipendenti con numero tra 1000 e 2000	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
Tutti gli amministratori di help desk impiegati presso la società per più di 6 mesi	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) Nota: la query richiede la creazione di un attributo DOH per la data di assunzione dell'utente.

Nota: i confronti $>$ e $<$ (maggiore di e minore di) sono lessicografici, non aritmetici. Per i dettagli sul loro uso, consultare la documentazione del server directory LDAP.

Creazione di un gruppo nidificato

Se l'archivio utenti è una directory LDAP, è possibile aggiungere un gruppo come membro di un altro gruppo. Il gruppo è detto *gruppo nidificato*.

Il gruppo che contiene il gruppo nidificato è detto *gruppo padre*. I membri del gruppo nidificato diventano membri del gruppo padre. Tuttavia, i membri del gruppo padre non diventano membri di un gruppo nidificato.

I gruppi nidificati sono analoghi alle liste di distribuzione di posta elettronica, che consentono di aggiungere una lista come membro di un'altra. Con i gruppi nidificati, è possibile aggiungere gruppi e utenti come membri di un gruppo. Nidificando un gruppo nell'elenco di appartenenza di un altro, è possibile includere tutti i membri dei gruppi nidificati.

Ad esempio, se sono stati creati gruppi distinti per i reparti di produzione, design, spedizione e contabilità di una società, è possibile creare un gruppo padre per l'intera società nidificando tutti i gruppi dei diversi reparti come membri del gruppo padre della società. Ne deriva che eventuali modifiche apportate ai gruppi nidificati di produzione, design, spedizione e contabilità si rifletteranno automaticamente nel gruppo nidificato per l'intera società. Un gruppo nidificato in un altro può essere dinamico e/o contenere a sua volta altri gruppi nidificati.

La figura in [Esempio di gruppi statici, dinamici e nidificati](#) (a pagina 161) illustra un gruppo padre creato mediante gruppi statici, dinamici e nidificati.

Tenere presente quanto segue prima di creare un gruppo nidificato:

- Solo un amministratore con l'attività Modifica membri del gruppo può aggiungere o modificare gruppi nidificati nell'elenco dei membri statici del gruppo nella console utente.
- Solo gli utenti con adeguati privilegi di amministrazione possono modificare, aggiungere o rimuovere membri in un gruppo.

Ad esempio, se il Gruppo A padre viene creato dai gruppi nidificati B e C, l'amministratore del Gruppo A può modificare solo i membri del Gruppo A, non di B e C. La modifica dei gruppi B e C è consentita solo ai relativi amministratori.

- Per abilitare i gruppi nidificati, gli amministratori di sistema configurano il supporto dei gruppi nidificati nel file di configurazione della directory (directory.xml):
 - Aggiungere l'elemento GroupTypes alla sezione Comportamento dei gruppi di directory nella maniera seguente:

```
<GroupTypes type=type>
```

type può corrispondere a NESTED, [DYNAMIC](#) (a pagina 156) oppure ALL.

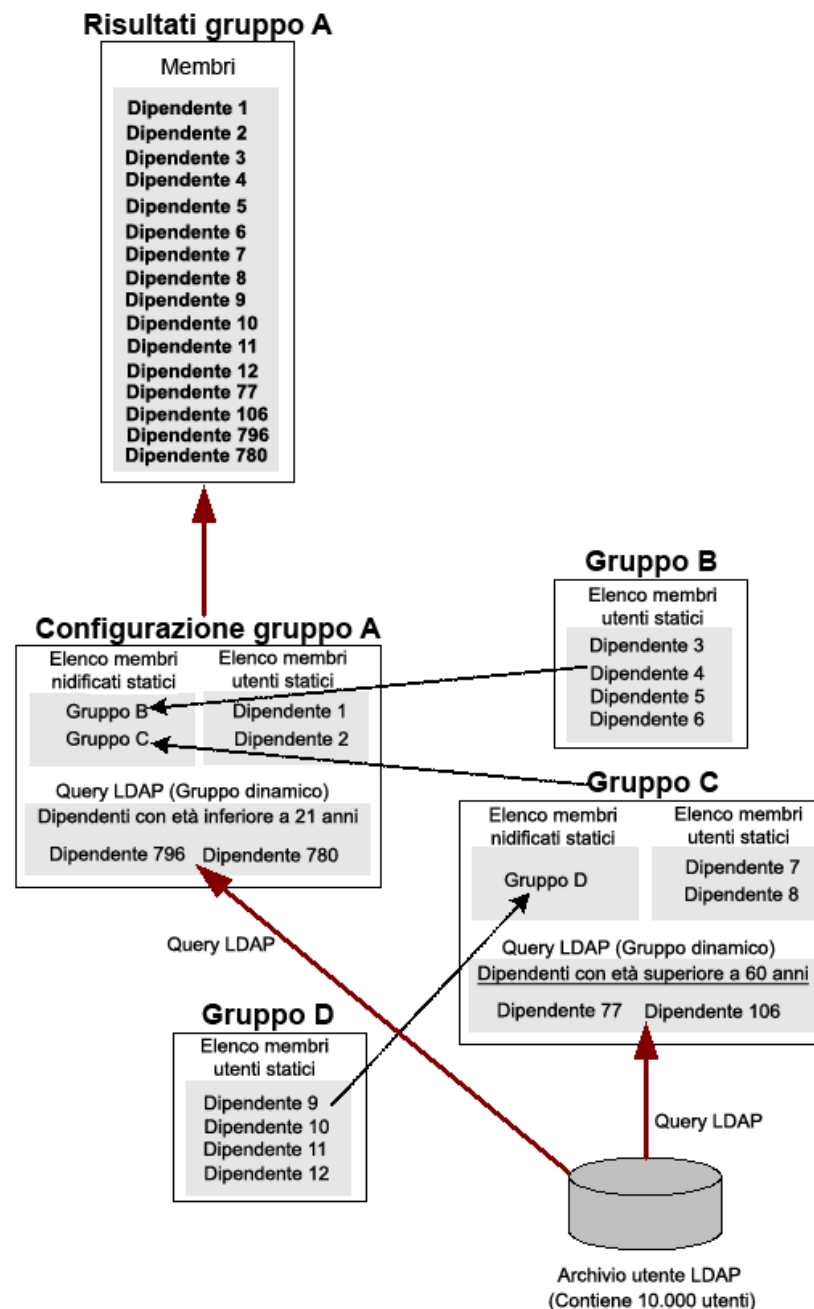
L'elemento GroupTypes rispetta l'uso delle lettere maiuscole e minuscole.
 - Eseguire il mapping dell'attributo noto %NESTED_GROUP_MEMBERSHIP% su un attributo fisico esistente in un archivio utenti.

Come creare un gruppo nidificato

1. Nella console utente, selezionare Gruppi, Crea gruppo.
2. Scegliere se creare un nuovo gruppo o una copia di un gruppo esistente e fare clic su **OK**.
3. Nella scheda Profilo, immettere un nome gruppo, un'organizzazione, una descrizione e un nome dell'amministratore del gruppo.
4. Nella scheda Appartenenza:
 - a. Fare clic su Aggiungi un gruppo per aggiungere un gruppo nidificato a questo gruppo.
 - b. Cercare un gruppo esistente.
 - c. Inserire un segno di spunta accanto al gruppo e fare clic su Seleziona.
 - d. Fare clic su Inoltra.

Esempio di gruppi statici, dinamici e nidificati

I gruppi possono essere complessi e costituiti da una combinazione di gruppi dinamici, statici o nidificati. Nella figura seguente è illustrato un esempio di un gruppo padre creato da gruppi statici, dinamici e nidificati.



Nella figura precedente:

- Il Gruppo A, padre, contiene i gruppi nidificati B e C, due utenti statici e una query dinamica LDAP che elenca tutti i dipendenti di età inferiore ai 21 anni.
- Il gruppo B è composto da quattro utenti statici.
- Il Gruppo C, padre, contiene il gruppo nidificato D, due utenti statici e una query dinamica LDAP che elenca tutti i dipendenti di età superiore ai 60 anni.
- Il gruppo D contiene quattro utenti statici.
- Nella parte superiore della figura sono elencati i membri del Gruppo A risultanti dai gruppi nidificati, dalle query dinamiche e dagli elenchi di membri statici dei Gruppi B, C e D.

Amministratori gruppo

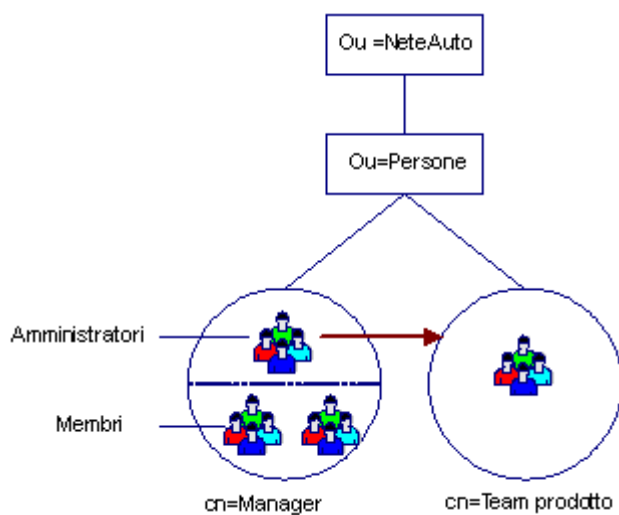
La scheda Amministratori delle attività Crea o Modifica gruppo consente di specificare gli utenti e i gruppi come amministratori di un gruppo. Quando si assegna un utente come amministratore di un gruppo, verificare che l'amministratore disponga di un ruolo con un ambito adeguato alla gestione del gruppo. Ad esempio:

1. Selezionare Modifica gruppo per assegnare un utente come amministratore di un gruppo.
2. Assegnare a tale utente un ruolo di amministrazione con attività di gestione, come ad esempio Modifica membri del gruppo o attività di gestione utenti mediante la scheda Gruppi.
3. Verificare che il ruolo disponga dell'ambito appropriato per il gruppo.
 - a. Utilizzare Visualizza ruolo di amministrazione per il ruolo assegnato alle attività di gestione del gruppo.
 - b. Dalla scheda Membri, verificare l'esistenza del criterio e la presenza delle seguenti condizioni:
 - Una regola membri soddisfatta dall'amministratore del gruppo
 - Una regola di ambito che include il gruppo
 - Una regola di ambito che include alcuni utenti da aggiungere al gruppo

Nota: per abilitare i gruppi affinché siano amministratori di altri gruppi, gli amministratori di sistema dovranno configurare il supporto dell'amministratore del gruppo nel file di configurazione della directory (directory.xml):

- Impostare il tipo AdminGroupTypes su ALL nella sezione Comportamento dei gruppi di amministrazione della directory. L'elemento AdminGroupTypes rispetta l'uso delle lettere maiuscole e minuscole.
- Eseguire il mapping dell'attributo noto %GROUP_ADMIN_GROUP% su un attributo fisico esistente in un archivio utenti.

Quando si assegna un gruppo come amministratore, soltanto gli amministratori di tale gruppo saranno amministratori del gruppo creato o modificato. I membri del gruppo di amministrazione specificato non dispongono di alcun privilegio di gestione del gruppo. La seguente immagine mostra un gruppo a sua volta amministratore di un altro gruppo.



In questo esempio:

- Il manager gruppi è l'amministratore del gruppo Team di prodotto.
- Gli amministratori dei manager possono gestire il gruppo Team di prodotto. I membri del gruppo Manager non possono invece eseguire questa operazione.

Capitolo 7: Account endpoint gestiti

In CA Identity Manager è possibile gestire gli account su sistemi endpoint se l'installazione di CA Identity Manager include un server di provisioning. È possibile gestire account, ad esempio un account di Exchange, Windows NT o Oracle, nonché gestire account orfani e di sistema, che attualmente non sono associati a CA Identity Manager.

Questa sezione contiene i seguenti argomenti:

[Integrazione di endpoint gestiti](#) (a pagina 166)

[Sincronizzazione di utenti, account e ruoli](#) (a pagina 173)

[Sincronizzazione inversa con gli account endpoint](#) (a pagina 180)

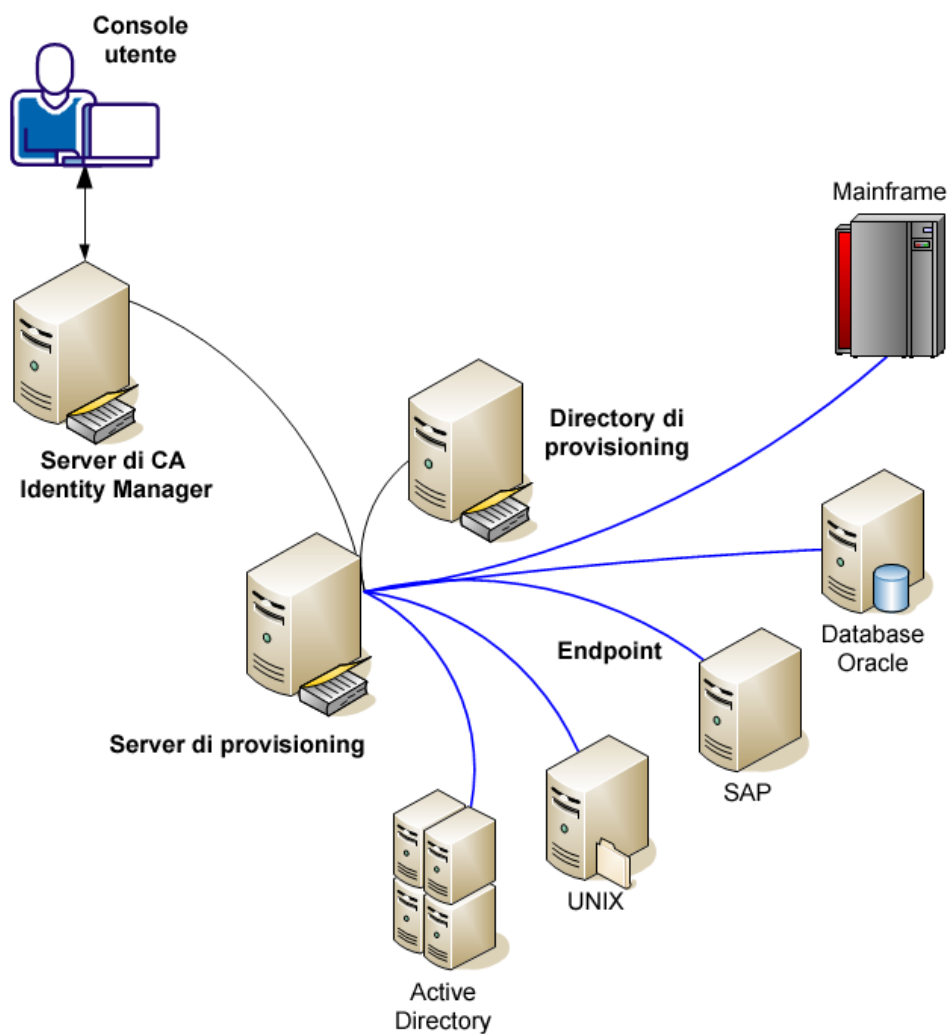
[Estensione degli attributi personalizzati agli endpoint](#) (a pagina 191)

[Attività degli account](#) (a pagina 193)

[Operazioni di account avanzate](#) (a pagina 198)

Integrazione di endpoint gestiti

Con CA Identity Manager è possibile gestire account su sistemi multipli da un'interfaccia utente singola, la console utente. Gli account sono su sistemi a cui ci si riferisce come endpoint gestiti o semplicemente endpoint. Nell'esempio seguente vengono gestiti utenti su cinque endpoint.



È possibile assegnare account su qualsiasi combinazione di endpoint a un utente. Quando si integra un endpoint, CA Identity Manager associa ogni account endpoint con un utente nella directory di provisioning.

Le procedure seguenti descrivono come integrare gli endpoint, in modo che gli account endpoint possano essere gestiti dalla console utente.

1. [Importazione del file di definizione dei ruoli](#) (a pagina 167)
2. Creazione di regole di correlazione
3. Aggiunta dell'endpoint all'ambiente
4. Creazione di una definizione di esplorazione e correlazione
5. Esplorazione e correlazione dell'endpoint

Importazione del file di definizione dei ruoli

Le definizioni dei ruolo vengono importate da un file che interessa il nuovo endpoint. Questa procedura richiede l'accesso alla console di gestione.

Procedere come descritto di seguito:

1. In Console di gestione, fare clic su Ambienti.
2. Selezionare l'ambiente al quale si sta aggiungendo l'endpoint.
3. Fare clic su Role and Task Settings (Impostazioni ruolo e attività).
4. Fare clic su Importa.
5. Selezionare un endpoint sotto Tipo di endpoint.
6. Fare clic su Fine.
Lo stato dell'importazione appare nella finestra corrente.
7. Fare clic su Continua per uscire.
8. Riavviare l'ambiente in modo che le modifiche vengano applicate.

Creazione di regole di correlazione

Un amministratore ospitante o un amministratore con il compito Configura attributi di correlazione può creare regole utilizzate quando si esamina un endpoint. L'attività Esegui Esplora e correla utilizza queste regole per la parte di correlazione dell'attività.

Le regole di correlazione determinano il tipo di mapping di un attributo dell'account endpoint con un attributo dell'utente nella console utente. Ad esempio, in Access Control esiste un attributo che viene chiamato AccountName. È possibile creare una regola per eseguirne il mapping su FullName nella console utente. Se le regole provocano due mapping su un attributo dell'utente, viene utilizzato il primo valore del parametro.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Fare clic su Sistema, Configurazione di provisioning, Configura attributi di correlazione.
3. Fare clic su Aggiungi.
4. Definire una regola di correlazione nel modo seguente:
 - a. Selezionare un elenco di attributi dell'utente globale.

Questo valore fa riferimento all'attributo dell'utente classificato nella Directory di provisioning.
 - b. Abilitare la casella di controllo Impostare un attributo account specifico.
 - c. Selezionare un tipo di endpoint.
 - d. Selezionare un attributo account che si applica all'attributo dell'utente globale.
 - e. Facoltativamente, completare i campi della sottostringa.

Se il campo Inizio sottostringa è vuoto, l'elaborazione inizia all'inizio della stringa. Se il campo Fine sottostringa è vuoto, l'elaborazione inizia all'inizio della stringa.
5. Fare clic su OK.
6. Fare clic su Inoltra.

Nota: quando si modifica una regola di correlazione, assicurarsi di esaminare l'endpoint, anche se controllato precedentemente.

Esempio di regole di correlazione

L'esempio seguente fornisce impostazioni d'esempio per un endpoint Active Directory.

```
GlobalUserName  
FullName=LDAP Namespace:globalFullName  
FullName=ActiveDirectory:DisplayName  
CustomField01=ActiveDirectory:Telephone
```

Le azioni seguenti si verificano per ciascun account precedentemente non messo in correlazione, che viene trovato mettendo in correlazione account in un contenitore di Active Directory:

1. Il Server di provisioning confronta il primo parametro (GlobalUserName) con l'attributo dell'account endpoint Active Directory (NT_AccountID). Il server tenta di trovare l'utente globale univoco il cui nome corrisponde al valore attributo NT_AccountID per tale account. Se viene rilevata una corrispondenza univoca, il Server di provisioning associa l'account con l'utente globale. Se viene rilevata più di una corrispondenza, il Server di provisioning esegue il passaggio 5. Se non viene rilevata alcuna corrispondenza, il Server di provisioning esegue il passaggio successivo.
2. Il Server di provisioning considera il secondo parametro (FullName=LDAP Namespace:globalFullName). Poiché questo valore è specifico di un altro tipo di endpoint, viene ignorato e il Server di provisioning esegue il passaggio successivo.
3. Il Server di provisioning considera il terzo parametro (FullName=ActiveDirectory:DisplayName). Poiché questo valore è specifico di Active Directory, viene utilizzato. Il server tenta di trovare l'utente globale univoco il cui FullName corrisponde al valore attributo DisplayName per tale account. Se viene rilevata una corrispondenza univoca, il Server di provisioning associa l'account con l'utente globale. Se viene rilevata più di una corrispondenza, il Server di provisioning esegue il passaggio 5. Se non viene rilevata alcuna corrispondenza, il server di provisioning esegue la fase 4.
4. Il Server di provisioning considera il parametro finale (CustomField01=ActiveDirectory:Telephone). Poiché questo valore è specifico di Active Directory, viene utilizzato. Il server tenta di trovare l'utente globale univoco il cui attributo Campo personalizzato 01 è uguale al valore attributo Telefono per tale account. Il nome assegnato all'attributo dell'utente globale personalizzato mediante proprietà globali dell'Attività di sistema non viene visualizzato qui. Se viene rilevata una corrispondenza univoca, il Server di provisioning associa l'account con l'utente globale. Se viene rilevata più di una corrispondenza, il Server di provisioning esegue il passaggio 5. Se non viene rilevata alcuna corrispondenza, il Server di provisioning esegue il passaggio successivo.
5. Il Server di provisioning associa l'account con l'oggetto [utente predefinito]. Se l'oggetto [utente predefinito] non esiste, viene creato dal server.

Aggiunta dell'endpoint all'ambiente

L'endpoint viene aggiunto all'ambiente in cui si desidera gestirlo. Qualsiasi amministratore con l'attività Crea endpoint può eseguire questa procedura.

Procedere come descritto di seguito:

1. Selezionare Endpoint, Gestisci endpoint, Crea endpoint.
2. Selezionare un tipo di endpoint.
3. Compilare i campi delle schede.

I campi obbligatori sono preceduti da un cerchio rosso.

Nota: non utilizzare il simbolo # nel nome dell'endpoint, poiché questo carattere viene ignorato nelle ricerche.

4. Fare clic su Inoltra.

A questo punto è possibile creare una [definizione di esplorazione e correlazione](#) (a pagina 170) in modo da poterne gestire gli account.

Creazione di una definizione di esplorazione e correlazione

Per aggiungere utenti che esistono in un endpoint, creare una definizione di esplorazione e correlazione per tale endpoint. Qualsiasi amministratore con l'attività Crea esplora e correla definizione può creare la definizione.

Procedere come descritto di seguito:

1. In un ambiente fare clic su Endpoint, Esplora e correla definizioni, Crea esplora e correla definizione.
2. Fare clic su OK per avviare una nuova definizione.
3. Inserire un nome significativo in Esplora e Correla nome.
4. Fare clic su Seleziona metodo contenitore/endpoint/esplorazione per scegliere un endpoint e i contenitori, se esistono. Per un endpoint di grandi dimensioni, la ricerca dei contenitori potrebbe richiedere tempo; è possibile utilizzare il filtro di ricerca per ridurre i tempi.
5. Scegliere un metodo di esplorazione per il contenitore. Il processo di esplorazione e correlazione include i contenitori selezionati e i relativi sottocontenitori. Per un contenitore di directory, include tutti i contenitori nella struttura secondaria.

6. Fare clic sulle azioni di esplorazione e correlazione da eseguire:

- **Cerca oggetti gestiti nella directory:** trova gli oggetti archiviati sull'endpoint e non nella directory di provisioning.
- **Esegui correlazione tra account e utenti:** gli oggetti individuati con la funzione di esplorazione vengono messi in correlazione con gli utenti nella directory di provisioning. Sono disponibili due scelte di correlazione.

- **Utilizzo di utenti esistenti**

Utilizzare questa opzione per una [regola di correlazione](#) (a pagina 167) che corrisponda a ogni account con un utente creato in precedenza.

Se l'utente viene individuato, l'oggetto viene correlato all'utente. Se vengono rilevati più utenti, l'account viene associato all'utente predefinito. Se non viene individuato alcun utente, questa opzione crea l'utente (se tutti gli attributi obbligatori sono noti) e viene correlata all'account utente; in caso contrario, viene correlata all'account con l'utente predefinito.

- **Crea gli utenti necessari**

Utilizzare questa opzione per la correlazione degli account sull'endpoint primario. Questa opzione presuppone che gli account sull'endpoint abbiano esattamente lo stesso nome degli utenti. L'algoritmo di correlazione-corrispondenza non viene utilizzata con questa opzione. Ogni account viene semplicemente associato all'utente con lo stesso nome. Se l'utente non esiste ancora, viene creato. Nessun account viene associato all'utente predefinito.

- **Aggiorna campi utente:** se esiste un mapping tra i campi oggetto e i campi utente, questi ultimi vengono aggiornati con i dati presenti nei campi oggetto.

Gli utenti vengono creati senza attributi facoltativi quali nome, indirizzo e numeri di telefono. Durante l'acquisizione iniziale di un endpoint, utilizzare questa opzione per impostare questi attributi degli utenti mediante valori degli attributi account. Durante le successive operazioni di esplorazione e correlazione, utilizzare questa opzione per aggiornare gli attributi utente e per applicare le modifiche apportate agli attributi account, utilizzando strumenti diversi da CA Identity Manager.

7. Fare clic su Inoltra.

A questo punto, un amministratore con l'attività [Esegui Esplora e correla](#) (a pagina 172) completa l'integrazione dell'endpoint.

Esplorazione e correlazione dell'endpoint

Un amministratore ospitante o un altro amministratore con l'attività Esegui Esplora e correla esegue questa procedura. La fase di esplorazione dell'attività identifica gli account nell'endpoint. La fase di correlazione fa corrispondere gli account con gli utenti in CA Identity Manager o crea gli account.

Procedere come descritto di seguito:

1. In un ambiente fare clic su Endpoint, Esegui Esplora e correla.
2. Selezionare Esegui ora per eseguire l'operazione di esplorazione e correlazione immediatamente, oppure [Pianifica nuovo processo](#) (a pagina 421) per rimandare l'operazione a un momento successivo oppure in base a una pianificazione ricorrente.

Nota: per questa operazione è necessario che il fuso orario del browser client coincida con quello del server. Ad esempio, se sul client sono le 22:00 di martedì, mentre sul server sono le 07:00, la definizione di esplorazione e correlazione non funzionerà.

3. Fare clic su una definizione di esplorazione e correlazione da eseguire.
4. Fare clic su Inoltra.

Gli account utente esistenti sull'endpoint verranno creati o aggiornati in CA Identity Manager, in base alla definizione di esplorazione correlazione creata dall'utente.

5. Verificare l'attività eseguita correttamente nel modo seguente:
 - a. Fare clic su Sistema, Visualizza attività inoltrate.
 - b. Completare il campo del nome dell'attività nel modo seguente: Esegui Esplora e correla
 - c. Fare clic su Cerca.

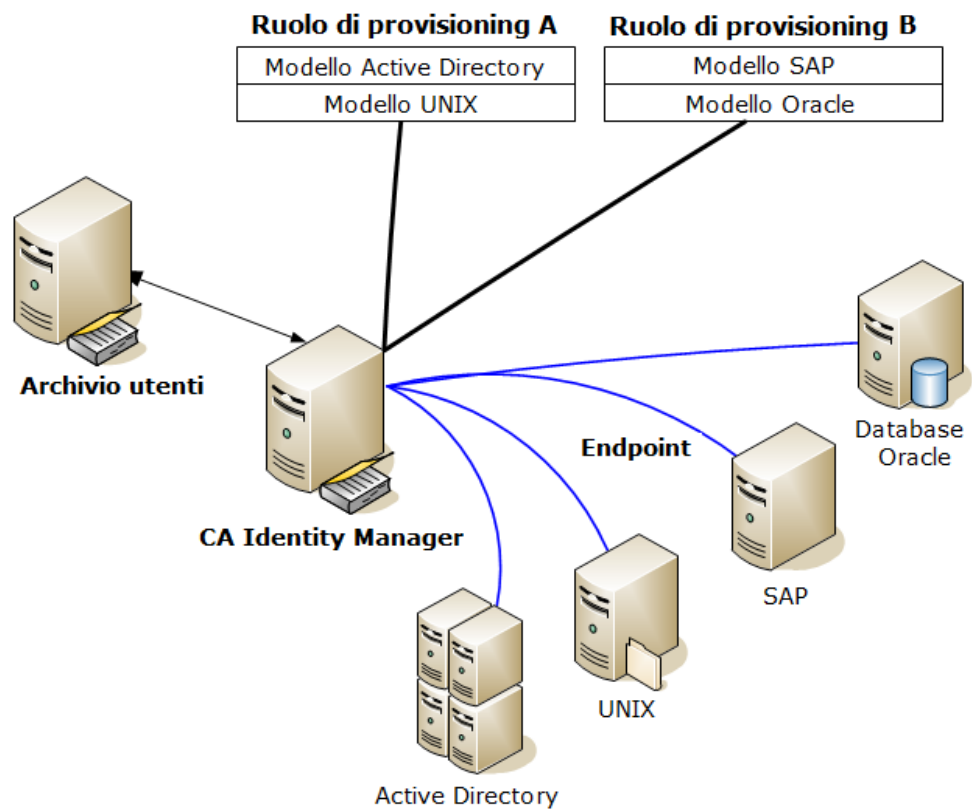
Nei risultati viene indicato se l'attività è stata completata correttamente.

Nota: è possibile interrompere un'attività Esplora e Correla durante la visualizzazione dello stato dell'attività in Visualizza attività inoltrate. L'interruzione dell'attività ne impedisce l'elaborazione e lo stato dell'attività visualizzato corrisponde allo stato precedente all'interruzione. Tutte le notifiche generate vengono inviate per garantire la sincronizzazione dei sistemi.

Sincronizzazione di utenti, account e ruoli

L'integrazione di account ed endpoint multipli in un sistema singolo di gestione degli utenti può causare una perdita di sincronizzazione. I ruoli di provisioning o i modelli di account che vengono assegnati a un utente possono differire dagli account attualmente esistenti per tale utente.

Ad esempio, considerare una situazione con due ruoli di provisioning, uno con i modelli di account UNIX e Active Directory e un altro con i modelli SAP e Oracle. L'utente john_smith ha il ruolo di provisioning A, che contiene i modelli di account UNIX e Active Directory, ma tale utente ha solo un account Active Directory. È possibile che il modello di account UNIX sia stato aggiunto al ruolo dopo essere stato aggiunto all'utente. Perciò, l'amministratore sincronizza l'utente con la definizione attuale di ruolo.



Le situazioni seguenti costituiscono altri motivi che possono causare la perdita di sincronizzazione con i ruoli di provisioning o i modelli di account:

- I precedenti tentativi di creare gli account necessari non sono andati a buon fine a causa di problemi legati all'hardware o al software nella propria rete, causando la perdita di account.
- I ruoli di provisioning e i modelli di account vengono modificati. Ciò comporta account extra o mancanti.
- Gli account sono stati assegnati a modelli di account dopo la loro creazione, quindi gli account esistono, ma non sono sincronizzati con i relativi modelli di account.
- La creazione di un nuovo account viene ritardata, in quanto era stato specificato che l'account sarebbe stato creato successivamente.
- È stato acquisito un endpoint. Durante l'esplorazione e la correlazione, il Server di provisioning non ha assegnato automaticamente ruoli di provisioning agli utenti. Aggiornare il ruolo per indicare gli utenti che necessitano di account sull'endpoint. Qualsiasi account messo in correlazione con un utente viene classificato come account extra quando l'utente viene sincronizzato.
- È stato assegnato un account esistente a un utente, copiando l'account sull'utente.
- È stato creato un account per un utente, invece di assegnare l'utente a un ruolo. Ad esempio è stato copiato un utente su un modello di account che non è in un ruolo di provisioning per tale utente. L'account viene classificato come account extra o come account con un modello di account extra. Se si copia l'utente su un endpoint per creare un account utilizzando il modello di account predefinito, tale account potrebbe essere un account extra.

Le sezioni seguenti spiegano come eseguire i tre tipi di sincronizzazione:

1. [Sincronizzazione utente con ruoli](#) (a pagina 175).
2. [Sincronizzazione utente con modelli account](#) (a pagina 175).
3. [Sincronizzazione account endpoint con modelli account](#) (a pagina 177).

Sincronizzazione utente con ruoli

Questa attività crea, aggiorna o elimina gli account, in modo che siano conformi ai ruoli di provisioning assegnati a un utente. Ad esempio, gli amministratori utilizzano strumenti nativi su un endpoint, per aggiungere o eliminare account, ma l'endpoint non è ancora stato riesplorato per aggiornare la directory di provisioning. Perciò gli utenti hanno account extra o mancanti. Questa attività assicura inoltre che ciascun account appartiene ai modelli di account corretti.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Attività, Utenti, Sincronizzazione, Verifica sincronizzazione ruolo.
3. Selezionare un utente.

Viene visualizzata una schermata che mostra gli account previsti, gli account extra e gli account mancanti.

4. Fare clic su Sincronizza per far corrispondere gli account con il modello in questo ruolo.

- a. È possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account per l'utente prescrive lo stesso account, l'account viene creato unendo tutti i modelli di account interessati.

Questo account viene assegnato ai modelli di account attualmente non sincronizzati con l'account.

- b. È possibile selezionare una casella di controllo per eliminare gli account extra. Tuttavia, gli utenti possono avere motivi legittimi per avere questi account. In questo caso lasciare questa opzione deselezionata.

Su determinati endpoint la funzione di eliminazione dell'account è disattivata; per questo motivo l'account non viene eliminato.

Sincronizzazione utente con modelli account

Questa attività sincronizza gli attributi per gli account endpoint con i modelli di account associati per un determinato utente. Tuttavia la sincronizzazione completa dipende dai seguenti fattori:

- La sincronizzazione completa dell'account si verifica in due situazioni. Un modello di account utilizza una [sincronizzazione sicura](#) (a pagina 178) o due o più modelli di account sono stati aggiunti a un account.
- Se un modello di account utilizza una [sincronizzazione minima](#) (a pagina 178), tale attività avvia una sincronizzazione account che coinvolge solamente questo modello. Se l'account non fosse stato precedentemente sincronizzato con altri modelli di account prima di questo aggiornamento, potrebbe essere ancora non sincronizzato anche in seguito.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Attività, Utenti, Sincronizzazione, Verifica sincronizzazione modello account.
3. Selezionare un utente.

Viene visualizzata una schermata che mostra gli account previsti, gli account extra e gli account mancanti.

4. Fare clic su Sincronizza per far corrispondere gli account con il modello.

- a. È possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account per l'utente prescrive lo stesso account, l'account viene creato unendo i modelli di account interessati.

Questo account viene assegnato ai modelli di account non sincronizzati con l'account. La sincronizzazione dell'account non è necessaria sugli account appena creati.

- b. È possibile selezionare una casella di controllo per eliminare gli account extra. Tuttavia, gli utenti possono avere motivi legittimi per avere questi account. In questo caso lasciare questa opzione deselezionata.

Su determinati endpoint la funzione di eliminazione dell'account è disattivata; per questo motivo l'account non viene eliminato.

Attributi solo per i nuovi account

In un modello di account, alcuni attributi vengono applicati solo durante la creazione dell'account. Ad esempio, l'attributo Password è un'espressione di regola che definisce la password per i nuovi account. Questa espressione di regola non aggiorna mai la password di un account. Le modifiche apportate all'espressione di regola per la password interessano solo sugli account creati successivamente all'impostazione di tale espressione.

Analogamente, un'espressione di regola modello per un attributo di account di sola lettura interessa solo gli account creati successivamente all'impostazione di tale espressione. La sua modifica non incide sugli account esistenti.

Sincronizzazione account endpoint con modelli di account

Questa attività sincronizza un account endpoint dopo la modifica di un modello di account associato. Ad esempio, se un account Active Directory non ha gruppi, ma il modello di account associato può includere gruppi.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Attività, Endpoint, Gestisci endpoint, Verifica sincronizzazione account endpoint.
3. Selezionare un endpoint.

A questo punto compare una schermata che mostra gli account su tale endpoint, i modelli di account associati e quali attributi non sono sincronizzati.

4. Fare clic su Sincronizza per far corrispondere gli attributi di tali account con ciò che è definito nel modello di account.

Le modifiche effettuate ai modelli di account condizionano gli account esistenti nel modo seguente:

- Se si modifica il valore di un attributo di compatibilità, l'attributo account corrispondente viene aggiornato in modo da sincronizzarlo con il valore dell'attributo del modello di account. Consultare la descrizione di sincronizzazione minima e sicura.
- Alcuni attributi account vengono designati dal connettore come non aggiornati in caso di modifiche al modello di account, ad esempio l'attributo Password e determinati attributi che possono essere impostati dal tipo di endpoint unicamente durante la creazione dell'account.

Aggiornamento degli attributi

Quando vengono modificati gli attributi di compatibilità in un modello di account, è possibile che l'attributo corrispondente negli account venga modificato. Questa modifica ha un impatto sugli attributi dell'account. L'impatto si basa sui seguenti fattori:

- Se la definizione del modello di account prevede l'utilizzo della sincronizzazione minima o sicura.
- Se l'account appartiene a più modelli di account.

Sincronizzazione minima

La *sincronizzazione minima* assicura che gli utenti dispongano degli attributi di compatibilità minimi richiesti per i relativi account. Si tratta della sincronizzazione predefinita nella maggior parte dei tipi di endpoint. Se si aggiorna un modello che utilizza la sincronizzazione minima, CA Identity Manager aggiorna gli attributi di capacità nel modo seguente:

- Se viene aggiornato un campo numerico in un modello di account e il nuovo numero è maggiore di quello nell'account, il valore nell'account viene modificato in modo che corrisponda al nuovo numero.
- Se una casella di controllo in un modello di account non era selezionata e successivamente viene selezionata, la casella di controllo viene aggiornata in tutti gli account in cui non è selezionata.
- Se viene modificato un elenco in un modello di account, vengono aggiornati tutti gli account per includere tutti i valori presenti nel nuovo elenco che non erano inclusi nell'elenco di valori dell'account.

Se un account appartiene ad altri modelli di account, a prescindere dal fatto che tali modelli utilizzino la sincronizzazione minima o sicura, in CA Identity Manager viene consultato solo il modello modificato. Questa procedura risulta più efficiente rispetto al controllo di tutti i modelli di account. Poiché con la sincronizzazione minima vengono solo aggiunte compatibilità agli account, in genere non è necessario consultare altri modelli di account.

Nota: in caso di propagazione da un modello di account con sincronizzazione minima, le modifiche che comportano la rimozione o la riduzione di compatibilità possono lasciare alcuni account privi di sincronizzazione. Tenere presente che la sincronizzazione minima non determina mai la rimozione o la riduzione di compatibilità. Senza consultare altri modelli per un account, la propagazione non considera se la sincronizzazione minima è sufficiente.

In questa situazione, utilizzare Sincronizza utente con modelli account per sincronizzare l'account con i rispettivi modelli di account.

Sincronizzazione sicura

La sincronizzazione sicura garantisce che gli account presentino gli stessi attributi account specificati nel modello di account.

Ad esempio, a un modello di account UNIX esistente è stato aggiunto un gruppo. All'inizio, il modello di account inseriva gli account nel gruppo del personale. Adesso si desidera inserire gli account nei gruppi del personale e del sistema. Tutti gli account associati al modello di account si considerano sincronizzati quando ciascuno è inserito in entrambi i gruppi del personale e del sistema (e in nessun altro gruppo). Gli account non presenti nel gruppo del personale sono aggiunti a entrambi i gruppi.

Tra gli altri fattori da considerare vi sono le seguenti situazioni:

- Se il modello di account utilizza la sincronizzazione sicura, qualsiasi account che appartiene ad altri gruppi, diversi da quelli del personale e del sistema, viene rimosso da quei gruppi extra.
- Se il modello di account utilizza la sincronizzazione minima, gli account vengono aggiunti ai gruppi del personale e del sistema. Qualsiasi account con gruppi aggiuntivi definiti resta inserito in questi gruppi.

Nota: Sincronizzare regolarmente gli account con i relativi modelli per far sì che gli account rimangano sincronizzati con i relativi modelli di account.

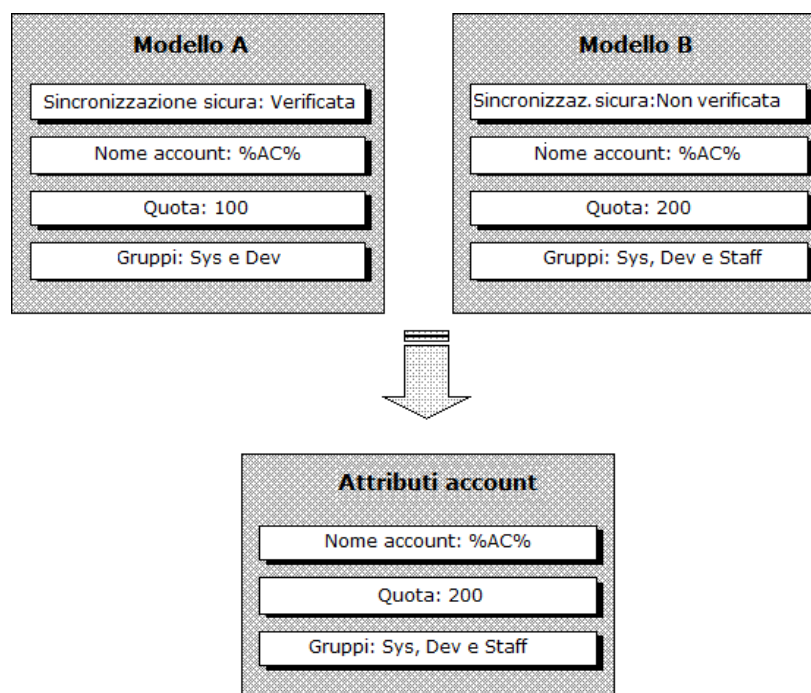
Account con più modelli

La sincronizzazione dipende anche se l'account appartiene a più modelli di account. Se un account ha un solo modello di account che utilizza la sincronizzazione sicura, ogni attributo viene aggiornato in modo che corrisponda esattamente a quanto restituito dal valore dell'attributo del modello di account. Si ottiene lo stesso risultato come se l'attributo fosse un attributo iniziale.

Un account può appartenere a più modelli di account, come nel caso di un utente che appartiene a più ruoli di provisioning, ognuno dei quali prevede un certo livello di accesso sullo stesso endpoint gestito. In questo caso, CA Identity Manager associa quei modelli di account in un unico modello di account valido che definisce il soprainsieme di compatibilità prese dai singoli modelli di account. Questo modello di account utilizza una sincronizzazione minima se tutti i singoli modelli di account sono minimi, oppure la sincronizzazione sicura se un singolo modello di account è sicuro.

Nota: in genere viene utilizzata solo la sincronizzazione minima o solo quella sicura per i modelli di account che controllano un account, a seconda se i propri ruoli aziendali definiscono completamente gli accessi necessari per gli utenti. Se gli utenti non rientrano in ruoli ben precisi ed è richiesta flessibilità per concedere compatibilità aggiuntive agli account utente, utilizzare la sincronizzazione minima. Se è possibile definire ruoli per specificare esattamente gli accessi necessari agli utenti, utilizzare la sincronizzazione sicura.

L'esempio seguente mostra l'associazione di più modelli di account in un singolo modello di account valido. In questo esempio, un modello di account viene contrassegnato per la sincronizzazione minima e l'altro per la sincronizzazione sicura. Di conseguenza, il modello di account valido creato combinando i due modelli di account viene considerato come un modello di account con sincronizzazione sicura. L'attributo Quota, espresso con un numero intero, adotta il valore maggiore dai due modelli di account, mentre l'attributo Gruppi con più valori adotta l'unione dei valori tratti dai due criteri.



Sincronizzazione inversa con gli account endpoint

Anche se la creazione, l'eliminazione e la modifica degli account siano di pertinenza di CA Identity Manager, non è possibile impedire che un utente di un sistema endpoint possa eseguire autonomamente tali operazioni. Questa situazione può verificarsi per motivi di emergenza oppure a scopi dannosi, ad esempio l'azione di un hacker. La sincronizzazione inversa assicura il controllo degli account di cui un utente dispone su ogni endpoint, identificando le discrepanze tra gli account CA Identity Manager e quelli presenti sugli endpoint.

Ad esempio, se un account è stato creato nel dominio Active Directory utilizzando uno strumento esterno, CA Identity Manager deve essere informato di questo potenziale problema di sicurezza. Inoltre, il bypass di CA Identity Manager provoca l'assenza di processi di approvazione e rapporti di verifica.

Le possibili discrepanze tra gli endpoint CA Identity Manager e gli endpoint gestiti sono di due tipi:

- Rilevazione di un nuovo account
- Modifica di un account esistente

È possibile trattare entrambi i casi mediante la definizione di criteri per la gestione della modifica. L'esecuzione dei criteri verrà quindi attivata utilizzando Esplora e Correla per aggiornare CA Identity Manager.

Funzionamento della sincronizzazione inversa

La sincronizzazione inversa degli account endpoint funziona come descritto di seguito:

1. Un amministratore o un utente malintenzionato crea o modifica un account in un endpoint.
2. Quando la funzione Esplora e correla viene eseguita sull'endpoint, l'account nuovo o modificato viene rilevato.
3. Il server di fornitura invia una notifica al server CA Identity Manager.
4. Il server CA Identity Manager cerca un criterio di sincronizzazione inversa che corrisponda alla modifica nell'endpoint.
5. Se viene rilevato un criterio corrispondente, viene eseguito. Se a questo account si applicano più criteri e tali criteri hanno lo stesso ambito, viene eseguito quello con la priorità più alta.
6. In base al criterio, viene eseguita una delle azioni seguenti:
 - Per un nuovo account, il criterio accetta, elimina o sospende l'account oppure lo invia per l'approvazione del flusso di lavoro.
 - Per un account modificato, il criterio accetta il valore, lo ripristina all'ultimo valore noto oppure lo invia per l'approvazione del flusso di lavoro.
7. Se è selezionato il flusso di lavoro, viene generato un nuovo evento per il flusso di lavoro e vengono impostati i responsabili dell'approvazione. Viene quindi eseguita una delle seguenti azioni:
 - Per un nuovo account, il responsabile dell'approvazione può accettare, eliminare o sospendere l'account, oppure assegnarlo ad un utente.
 - Per un account modificato, il processo del flusso di lavoro corrisponde a quello utilizzato se il valore viene modificato nella console utente, ad eccezione del fatto che i valori rifiutati vengono ripristinati a livello di endpoint.

Mapping degli attributi endpoint

Per utilizzare la sincronizzazione inversa per un attributo in un account endpoint, è necessario eseguire il mapping su un attributo visibile nella console utente. Alcuni attributi, come ad esempio il nome account e la password vengono mappati per impostazione predefinita. Il mapping degli altri attributi non viene invece eseguito. Ad esempio, il mapping dell'appartenenza al gruppo di attributi di Active Directory non viene eseguito. Per alcuni tipi di endpoint, nessun attributo viene mappato.

Per verificare se è possibile eseguire il mapping dell'attributo

1. Dalla console utente, fare clic su Endpoint, oppure su Attività, Endpoint.
2. Fare clic su Modifica inversa, quindi su Crea criterio account modificato mediante sincronizzazione inversa.
3. Indicare se si desidera creare un nuovo criterio oppure copiarne uno.
4. Fare clic su Tipo di endpoint e scegliere un endpoint, come ad esempio Active Directory.
5. Fare clic su Nome attributo per visualizzare un elenco di attributi di cui è possibile eseguire il mapping.
6. Fare clic su Annulla.

Il criterio viene annullato in quanto lo si è utilizzato soltanto per verificare quali attributi possono essere sottoposti a mapping.

Importante. È possibile gestire determinati attributi soltanto mediante gli strumenti nativi dell'endpoint. Pertanto, se un utente endpoint modifica il tipo di attributo, l'evento inverso produrrà un errore al momento dell'attivazione del criterio di sincronizzazione. Tuttavia, le modifiche apportate agli altri attributi dell'evento inverso non vengono invertite. Pertanto, si consiglia di non eseguire il mapping degli attributi che possono essere gestiti soltanto sull'endpoint.

Per mappare gli attributi endpoint per la sincronizzazione inversa

1. Fare clic su Endpoint, Modifica endpoint.
2. Cercare e selezionare un endpoint che richieda la sincronizzazione inversa.
3. Fare clic sulla scheda Mapping attributo.
4. Selezionare Utilizza impostazioni personalizzate.
5. Fare clic su Aggiungi per aggiungere un nuovo attributo personalizzato.
6. Selezionare un attributo personalizzato disponibile. Ad esempio, utilizzare il campo personalizzato 10 se non viene utilizzato nel proprio ambiente.

7. Mappare l'attributo personalizzato al nome dell'attributo account che si desidera gestire.
8. Ripetere i passaggi da 5 a 7 per aggiungere i mapping tra tutti gli attributi account necessari e l'attributo personalizzato selezionato.

È possibile utilizzare lo stesso attributo personalizzato (nel nostro esempio il campo personalizzato 10) per tutti gli attributi da gestire.

9. Fare clic su Inoltra.

Per creare valori di previsione per l'endpoint

Dopo aver eseguito il mapping di tutti gli endpoint, sarà possibile esplorare l'endpoint. Per eseguire l'operazione è necessario disattivare le notifiche in entrata e riattivarle al completamento dell'esplorazione. La disattivazione delle notifiche consente di eliminare le notifiche superflue. In caso contrario, tutti gli account che dispongono di valori nei nuovi attributi genererebbero una notifica durante l'operazione di esplorazione.

1. In Manager fornitura, disattivare la notifica in ingresso come descritto di seguito:
 - a. Fare clic su System (Sistema), Domain configuration (Configurazione dominio), CA Identity Manager Server (Server CA Identity Manager), Enable Notification (Attiva notifica).
 - b. Scegliere No.
 - c. Riavviare il server di fornitura per rendere effettive le modifiche.
2. Nella console utente, fare clic su Endpoint, Esegui Esplora e correla.

Scegliere una definizione di esplorazione e correlazione in cui la correlazione sia deselezionata.

Questa azione consente di ricompilare gli attributi dell'archivio utente con i nuovi dati di attributo endpoint. Se l'endpoint è di grandi dimensioni, questa attività può richiedere del tempo.
3. Riattivare la notifica in ingresso in Manager fornitura.
4. Riavviare il Server di provisioning.

Alla successiva operazione di esplorazione e correlazione eseguita sull'endpoint, verranno generate notifiche di modifica account. Le notifiche vengono generate se viene apportata una modifica ad un attributo mappato ad un attributo utente globale al quale si applica un criterio.

Ulteriori informazioni:

[Attributi di compatibilità e attributi iniziali](#) (a pagina 213)

Criteri per la sincronizzazione inversa

Quando in un endpoint viene creato o modificato un account, i criteri per la sincronizzazione inversa intraprendono azioni di risposta appropriate. Ad esempio, un utente crea alcuni account Active Directory in diverse UO del dominio aziendale. L'utente modifica inoltre alcuni account Microsoft Exchange. Utilizzando criteri di sincronizzazione inversa per gli account è possibile rilevare gli account nuovi e modificati e fornire azioni di risposta adeguate.

Mediante la sincronizzazione inversa è possibile eseguire le seguenti operazioni:

- Configurare un criterio per accettare il nuovo account, rifiutarlo oppure inviarlo per l'approvazione del flusso di lavoro.
- Configurare un criterio per accettare una modifica ad un attributo, ripristinare l'attributo originale, oppure inviarle la modifica per l'approvazione del flusso di lavoro.
- Quando un account viene inviato per l'approvazione del flusso di lavoro, il responsabile dell'approvazione può eseguire una delle seguenti operazioni:
 - Rifiutarlo (eliminarlo/sospenderlo dall'endpoint oppure modificare il valore perché corrisponda a quello presente nell'archivio utenti di CA Identity Manager)
 - Accettarlo ed aggiornare l'archivio utenti di CA Identity Manager in modo che corrisponda all'account
 - Assegnarlo ad un utente nella console utente (nel caso delle creazioni di account)

Creazione di un criterio per i nuovi account

Se si desidera definire un processo da eseguire quando in un endpoint viene rilevato un nuovo account, è necessario creare un criterio account applicato ai nuovi account. I criteri per i nuovi account vengono eseguiti quando vengono rilevati i nuovi account solo se l'opzione Correla è inclusa nella definizione di esplorazione e correlazione. Se un account viene rilevato quando è in esecuzione un'operazione di sola esplorazione, il criterio verrà eseguito la prossima volta che l'opzione Correla sarà inclusa durante l'esplorazione dell'endpoint.

Per creare un criterio per i nuovi account

1. Dalla console utente, fare clic su Endpoint, oppure su Attività, Endpoint.
2. Nuova inversione, Crea nuovo criterio account mediante sincronizzazione inversa.
3. Immettere un nome e una descrizione per il criterio.
4. Immettere i seguenti parametri:
 - **Priorità:** la priorità del criterio. Il criterio con la priorità maggiore è quello con il numero più basso. Se due criteri hanno la stessa priorità e lo stesso ambito, può essere eseguito l'uno o l'altro. Assicurarsi pertanto di impostare livelli di priorità diversi.
 - **Tipo endpoint:** tutti gli endpoint o un tipo di endpoint specifico.
 - **Endpoint:** il nome dell'endpoint specifico. Se per Tipo endpoint è impostato Tutti, l'unica opzione disponibile è All endpoints (Tutti gli endpoint).
 - **Contenitore:** il contenitore in cui risiede l'account. Questo campo riguarda esclusivamente gli endpoint gerarchici. Inserire il contenitore sotto forma di un elenco di nodi, che termina con l'endpoint. Ad esempio, per una OU AD il cui percorso è "ou=child,ou=parent,ou=root,dc=domain,dc=name" il formato "child,parent,root" è corretto.
 - **Utente correlato:** consente di controllare quando eseguire il criterio sulla base dell'individuazione di un utente correlato nella directory di fornitura.

5. In Azioni, selezionare una delle seguenti opzioni:
 - Accetta: sull'account non vengono eseguite azioni. Questa opzione risulta utile se esistono due criteri, uno che rifiuta tutti i nuovi account e uno, con priorità maggiore, che accetta gli account creati in una specifica UO. Di conseguenza, se l'account è stato creato in quella UO, viene accettato. Il criterio di rifiuto ha priorità più bassa e non viene eseguito.
 - Elimina: consente di rimuovere l'account dall'endpoint.
 - Sospendi: consente di lasciare l'account nell'endpoint, sospendendolo.
 - Invia per approvazione: consente di inviare la modifica per l'approvazione del flusso di lavoro.
6. Se si imposta l'azione Invia per approvazione, procedere come segue:
 - a. Fare clic sull'icona accanto a Processo del flusso di lavoro.
 - b. Scegliere un processo del flusso di lavoro.
 - c. Fare clic su OK.
7. Fare clic su Inoltra.

Se si assegna un processo del flusso di lavoro, è necessario [creare un'attività di approvazione](#) (a pagina 188).

Creazione di un criterio per gli account modificati

È possibile gestire mediante la sincronizzazione inversa qualsiasi attributo account di un account endpoint, a condizione che sia [definito nel mapping degli attributi](#) (a pagina 182).

Per definire un processo per i casi in cui viene rilevata una discrepanza tra gli account endpoint esistenti e i relativi valori noti in CA Identity Manager, è necessario creare un criterio account applicato agli account esistenti. Nel caso degli attributi multivalore, è possibile che sia stato aggiunto o rimosso più di un valore. In questo caso, il criterio viene applicato separatamente a ogni valore, oppure è possibile creare criteri diversi per valori diversi.

Per creare un criterio per gli account modificati

1. Dalla console utente, fare clic su Endpoint, oppure su Attività, Endpoint.
2. Fare clic su Modifica inversa, quindi su Crea criterio account modificato mediante sincronizzazione inversa.
3. Immettere un nome e una descrizione per il criterio.
4. Immettere i seguenti parametri:
 - **Priorità:** la priorità del criterio. Il criterio con la priorità maggiore è quello con il numero più basso. Se due criteri hanno la stessa priorità e lo stesso ambito, può essere eseguito l'uno o l'altro. Assicurarsi pertanto di impostare livelli di priorità diversi.
 - **Tipo endpoint:** tutti gli endpoint o un tipo di endpoint specifico.
 - **Endpoint:** il nome dell'endpoint specifico. Se per Tipo endpoint è impostato Tutti, l'unica opzione disponibile è All endpoints (Tutti gli endpoint).
 - **Contenitore:** il contenitore in cui risiede l'account. Questo campo riguarda esclusivamente gli endpoint gerarchici. Inserire il contenitore sotto forma di un elenco di nodi, che termina con l'endpoint. Ad esempio, per una OU AD il cui percorso è "ou=child,ou=parent,ou=root,dc=domain,dc=name" il formato "child,parent,root" è corretto.
 - **Attributo:** il nome fisico.
 - **Valore:** rappresentazione del valore in formato stringa, che può contenere l'asterisco (*) come carattere jolly. Il carattere jolly si riferisce a qualsiasi valore nella modifica.

5. In Azioni, selezionare una delle seguenti opzioni:
 - Accetta: consente di aggiornare il valore dell'account nell'archivio utente di CA Identity Manager in modo che corrisponda al valore nell'account endpoint.
 - Rifiuta: consente di reimpostare il valore originale dell'attributo senza effetti sulle altre modifiche agli attributi per l'account.
 - Invia per approvazione: consente di inviare la modifica per l'approvazione del flusso di lavoro.
6. Se si imposta l'azione Invia per approvazione, procedere come segue:
 - a. Fare clic sull'icona accanto a Processo del flusso di lavoro.
 - b. Scegliere un processo del flusso di lavoro.
 - c. Fare clic su OK.
7. Fare clic su Inoltra.

Se si assegna un processo del flusso di lavoro, è necessario [creare un'attività di approvazione](#) (a pagina 188).

Creazione di un'attività di approvazione per la sincronizzazione inversa

Le attività di approvazione inversa vengono create per i criteri che contengono un'azione Send to Workflow (Invia a flusso di lavoro. Considerare le linee guida riportate di seguito per la creazione delle attività:

- Per le attività di approvazione dei nuovi account, sono possibili due scelte.
 - È possibile creare una schermata di approvazione generica per gli account. La schermata di profilo dell'attività mostra solo informazioni generali sull'account. L'attività Approva nuovo account inverso funziona come illustrato di seguito.
 - Se è necessario che il responsabile dell'approvazione visualizzi i dettagli del nuovo account, la schermata deve essere specifica del tipo di endpoint. Pertanto, l'attività di approvazione con la schermata andrebbe utilizzata solo per i criteri specifici per quel tipo di endpoint. L'attività deve includere la scheda Approvazione inversa.
- Per le attività di approvazione delle modifiche agli account, la schermata di approvazione deve essere specifica di un tipo di endpoint, in modo che il responsabile dell'approvazione possa visualizzare i valori modificati.

Le attività di approvazione inversa sono identiche alle attività di approvazione utilizzate per le modifiche agli account. Se per uno specifico tipo di endpoint esiste già un'attività di approvazione, è possibile utilizzare tale attività. Per un nuovo account è necessaria una scheda di approvazione inversa aggiuntiva. Se non esiste un'attività di approvazione per il tipo di endpoint, attenersi alla seguente procedura.

Per creare un'attività di approvazione per la sincronizzazione inversa

1. Nella console utente, fare clic su Attività, Ruoli e attività, oppure fare clic su Ruoli e attività.
2. Fare clic su Attività di amministrazione, Crea attività di amministrazione.
3. Selezionare l'attività di modifica per l'endpoint.
Il nome dovrebbe iniziare con Modifica e specificare il nome del tipo di endpoint, ad esempio Modifica account Active Directory.
4. Apportare le seguenti modifiche nella scheda Profilo:
 - Modificare il nome della nuova attività.
 - Modificare il tag dell'attività.
 - Modificare l'azione in Approva evento.
5. Apportare le seguenti modifiche nella scheda Schede:
 - a. Rimuovere tutte le schede Relazione.
 - b. Se si tratta di un'attività di approvazione dei nuovi account, aggiungere la scheda Approvazione inversa. Spostare questa scheda in modo che diventi la prima scheda.
 - c. Copiare e modificare le schermate di approvazione nelle schede in base alle proprie esigenze.
Nota: l'utilizzo di alcune schermate di account durante un'attività di approvazione potrebbe generare alcuni errori. In tal caso, modificare la schermata di account predefinita nella scheda affinché l'attività possa essere eseguita.
6. Fare clic su Inoltra.
7. Se si tratta di un'attività di approvazione dei nuovi account, aggiungere l'attività ad un ruolo al quale il responsabile dell'approvazione dovrebbe appartenere. Il ruolo definisce l'ambito utente, che viene utilizzato per cercare gli utenti ai quali è possibile assegnare il nuovo account.

Esecuzione della sincronizzazione inversa

La sincronizzazione inversa viene eseguita quando si utilizza l'attività Esegui Esplora e correla. Quest'attività consente di aggiornare l'archivio di provisioning di CA Identity Manager con gli account nuovi o modificati su un endpoint.

Per eseguire la sincronizzazione inversa

1. Creare una definizione di esplorazione e correlazione che includa un'opzione Correla. La correlazione è necessaria per la rilevazione di nuovi account.
2. Fare clic su Attività, Endpoint, Esegui Esplora e correla.
3. Scegliere una definizione che si applichi all'endpoint contenente gli account nuovi o modificati.

Nota: quando si esegue la correlazione all'utente esistente, è necessario che l'utente esista nella directory di fornitura. In caso contrario, l'utente viene correlato all'utente predefinito in tale directory. L'archivio utenti di The CA Identity Manager non è compreso nell'ambito dell'attività Esplora e Correla.

4. Fare clic su Inoltra.

Se un criterio non dispone di un processo del flusso di lavoro, gli account sono già elaborati come definito nel criterio.

Nota: Se su un account rilevato dal criterio di sincronizzazione inversa sono stati rifiutati più attributi, tutte le azioni vengono inserite in un unico evento. Se tuttavia tale evento non riesce a causa di un problema relativo ad uno degli attributi, non viene aggiornato alcun attributo.

Se il flusso di lavoro è compreso nel criterio, le approvazioni generate dalla sincronizzazione inversa vengono visualizzate nella schermata Flusso di lavoro, Visualizza elenco lavori personali del responsabile dell'approvazione.

Per i nuovi account, il responsabile dell'approvazione può fare le seguenti scelte:

- Sospendere o eliminare l'account nell'endpoint, selezionando Elimina o Sospendi, quindi facendo clic su Rifiuta.
- Accettare il nuovo account facendo clic su Approva.

Se il responsabile dell'approvazione non seleziona un utente nel campo Utente correlato, l'account viene assegnato all'utente predefinito. Se il campo Utente correlato è compilato nell'attività di approvazione, l'account viene correlato a tale utente. Il campo Utente correlato contiene l'utente suggerito individuato dal meccanismo di correlazione, se è possibile individuare un utente.

Per gli account modificati, il responsabile dell'approvazione può fare le seguenti scelte:

- Per ogni account, visualizzare i valori modificati ed approvarli o rifiutarli come se le modifiche fossero state avviate nella schermata di gestione account.

- Visualizzare le modifiche agli attributi di capacità (ad esempio un gruppo Active Directory) come eventi di approvazione separati.

Per verificare se la sincronizzazione inversa ha avuto esito positivo

1. Passare a Sistema, Visualizza attività inviate.
2. Compilare il campo del nome attività con Attività di fornitura
3. Fare clic su Cerca.

Nei risultati viene indicato se l'evento di sincronizzazione inversa è stato completato correttamente.

Estensione degli attributi personalizzati agli endpoint

Il server di fornitura può gestire gli attributi degli endpoint personalizzati. Affinché CA Identity Manager possa leggere tali attributi associati a ruoli di fornitura, è necessario compiere ulteriori operazioni.

Per estendere gli attributi personalizzati agli endpoint

1. Generare i metadati dalla tabella dell'analizzatore se questo connettore è stato creato con una versione di CA Identity Manager precedente alla r12.5.

Per ulteriori informazioni, consultare la *Programming Guide for Java Connector Server*.

2. Utilizzare Connector Xpress come segue:
 - a. Installare i metadati nel nodo namespace.
 - b. Generare un file JAR, un file di proprietà e un file di definizione dei ruoli utilizzando il generatore di definizioni dei ruoli.

Per ulteriori informazioni, consultare *Connector Xpress Guide*.

3. Copiare il file .jar nella seguente posizione
 - (Windows) *app server home/iam_im.ear/user_console.war/WEB-INF/lib*
 - (UNIX) *app server home/iam_im.ear/user_console.war/WEB-INF/lib*

Nota: per WebSphere, copiare il file JAR in
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/Cell_name/applications/iam_im.ear/user_console.war/WEB-INF
4. Copiare il file delle proprietà nella seguente posizione:
 - (Windows) *app server home/iam_im.ear/custom/provisioning/resourceBundles*
 - (UNIX) *app server home/iam_im.ear/custom/provisioning/resourceBundles*

Nota: per WebSphere, copiare il file delle proprietà in
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/cell_name/applications/iam_im.ear/custom/provisioning/resourceBundles
5. Se si dispone di un cluster, ripetere le due operazioni appena descritte per ciascun nodo.
6. Riavviare il server applicazioni.
7. Importare il file di definizioni dei ruoli come segue:
 - a. Nella console di gestione selezionare un ambiente.
 - b. Selezionare le impostazioni relative a ruoli e attività.
 - c. Fare clic su Importa.
 - d. Selezionare il tipo di endpoint e fare clic su Fine.

Attività degli account

Nella console utente è possibile creare, modificare, visualizzare ed eliminare gli account degli endpoint associati con un utente Identity Manager. È inoltre possibile assegnare altri account di endpoint non associati con CA Identity Manager a un utente.

Esistono quattro tipi di account di endpoint:

Forniti

Account creati quando all'utente viene assegnato un ruolo di fornitura

Eccezioni

Account creati quando all'utente viene assegnato un modello di account

Orfani

Account creati sul sistema di endpoint e non associati a un utente CA Identity Manager

Sistema

Account creati sul sistema di endpoint, non associati con un utente CA Identity Manager e utilizzati per gestire il sistema di endpoint

Visualizzazione o modifica di account di endpoint

Le attività che consentono di visualizzare il profilo di un utente, ad esempio Visualizza utente o Modifica profilo personale, comprendono la scheda Account con l'elenco degli account di quell'utente sugli endpoint.

Dettagli account

Fare clic su un nome account per eseguire un'azione.

Seleziona	Nome	Tipo di endpoint	Endpoint	Sospeso	Bloccato
☒	 ken	Window NT	IM-term	Attivo	Sbloccato

Crea account

Azioni per gli account selezionati

Aggiorna account	Sospendi	Riprendi	Sblocca	Modifica password
Annulla assegnazione	Assegna	Elimina		

Per ciascun account, Identity Manager consente di visualizzare informazioni quali il nome dell'account, l'endpoint in cui esiste l'account e lo stato dell'account. Per un'attività di modifica, sono disponibili opzioni aggiuntive per modificare la password utente e bloccare o sospendere un account.

In questo esempio, la scheda Account comprende il pulsante di ricerca, pertanto la scheda è configurata con una schermata di ricerca. È possibile configurare la scheda per utilizzare una schermata di elenco, una schermata di ricerca o entrambe.

- Quando sono configurati entrambi i tipi di schermata, la schermata di ricerca determina i campi nei risultati della ricerca.
- Se è configurata solo la schermata di elenco, questa determina i campi nei risultati della ricerca.
- Se nessuna delle schermate è configurata, la scheda degli account utilizza una schermata di elenco statica, pertanto non è possibile personalizzarla per la visualizzazione di colonne.

Per ulteriori informazioni sulle altre opzioni disponibili nella scheda Account, consultare l'argomento relativo alla scheda Configura account nella Guida della console utente.

Creazione di un account fornito

Il metodo consigliato per creare un account di endpoint per un utente CA Identity Manager consiste nell'assegnare a tale utente un ruolo di provisioning. L'utente riceve l'account con gli attributi definiti nei modelli di account relativi a tale ruolo. Quando necessario, le modifiche apportate a tale modello di account, ad esempio dimensioni della cassetta postale per gli account Exchange, aggiornano l'account dell'endpoint.

Per creare un account fornito

1. Nella console utente, selezionare Gestisci utenti, Modifica utente.
2. Selezionare un utente da modificare.
3. Fare clic sulla scheda Fornitura Ruolo.
4. Fare clic su un ruolo di fornitura.
5. Seleziona ruolo.
6. Fare clic su Inoltra.

Creazione di un account di eccezione

È possibile creare un account direttamente nella scheda Account quando si utilizza Modifica utente per un utente. Questo account è denominato account di eccezione. Tuttavia, poiché nessun ruolo di fornitura riguarda questo account, la sincronizzazione dei ruoli con gli utenti non aggiorna l'account.

Per creare un account di eccezione

1. Nella console utente, selezionare Utenti, Modifica account endpoint utente.
2. Selezionare un utente da modificare.
3. Fare clic su Crea.
4. Selezionare un endpoint.
5. Selezionare un contenitore se necessario per il tipo di endpoint in questione.
6. Completare i campi in ciascuna scheda.
7. Fare clic su Inoltra.

Assegnazione di account orfani

Nella console utente è possibile gestire gli account orfani, cioè quelli non associati a un utente CA Identity Manager.

Per creare un utente predefinito per gli account orfani

Se la directory di provisioning è separata dall'archivio utenti di CA Identity Manager, creare l'utente predefinito del server di provisioning nell'archivio utenti di CA Identity Manager. L'utente predefinito viene usato per gli account orfani.

1. Nella console utente, fare clic su Utenti.
2. Fare clic su Gestisci utenti, Crea utente.
3. Denominare l'utente come segue, senza tralasciare le parentesi quadre:
[default user]

Ora è possibile assegnare account orfani agli utenti.

Per assegnare un account orfano

1. Nella console utente, fare clic su Endpoint.
2. Fare clic su Gestisci account orfani.
3. Cercare e selezionare un utente.
4. Fare clic su un utente per assegnare un account orfano.

Assegnazione di account di sistema

Nella console utente, è possibile gestire gli account di sistema, che sono account endpoint usati per gestire il sistema endpoint.

Per assegnare un account di sistema a un utente è necessario creare un'attività di amministrazione basata sull'attività Gestisci account di sistema. La nuova attività ha un utente CA Identity Manager specifico relativo a un determinato endpoint. È possibile creare un'attività per ciascun tipo di endpoint.

Per configurare un'attività in modo che assegni account di sistema

1. Nella console utente fare clic su Ruoli e attività, Attività di amministrazione, Crea attività di amministrazione.
2. La nuova attività deve basarsi su gestisci account di sistema.
Ad esempio è possibile creare un'attività denominata *Gestisci account di sistema Oracle* per assegnare gli account di sistema su un tipo di endpoint Oracle.
3. Nella scheda Ricerca, fare clic sul pulsante Sfoglia per modificare la schermata di ricerca. In questa schermata, includere un filtro di ricerca per individuare un utente da assegnare a questo account di sistema.
4. Inoltrare l'attività.
5. Includere l'attività in un ruolo.
6. Assegnare il ruolo a un utente incaricato di assegnare account di sistema per un endpoint a un utente.

L'utente con questo ruolo può eseguire la nuova attività per assegnare utenti di sistema a un utente CA Identity Manager.

Schermata attività Sposta account

Utilizzare questa schermata per spostare gli account da un contenitore o un endpoint all'altro. Di seguito sono descritti i campi presenti in questa schermata:

Sposta dettagli account

Consente di specificare l'account, il contenitore di livello superiore, il contenitore di destinazione, l'endpoint e il tipo di endpoint da spostare.

Pulsante Seleziona contenitore

Fare clic per cercare i contenitori account disponibili che appartengono all'endpoint.

Eliminazione di un account di un endpoint

Per eliminare un account di un endpoint esistono due metodi:

1. Mediante l'attività Modifica utente nella scheda Ruoli di fornitura è possibile rimuovere il ruolo che ha creato l'account.
2. Mediante l'attività Modifica account endpoint utente è possibile eliminare l'account.

Per eliminare un account con Modifica account endpoint utente

1. Nella console utente, selezionare Utenti, Modifica account endpoint utente.
2. Selezionare un utente da modificare.
3. Cercare gli account in base al tipo di endpoint.
4. Selezionare un account.
5. Fare clic sul pulsante Elimina.

Gli account eliminati vengono creati nuovamente quando si utilizza Manager fornitura, in questo modo:

- Sincronizza utenti con ruoli ricrea gli account forniti, ovvero gli account creati quando un utente ha un ruolo di fornitura.
- Sincronizza utenti con modelli di account ricrea gli account di eccezione (se l'account ha un modello di account) e gli account forniti.

Modifica della password di un account di un endpoint

È possibile modificare la password di un endpoint senza conoscere la password corrente.

Per modificare la password di un account di un endpoint

1. Nella console utente, selezionare Utenti, Modifica account endpoint utente.
2. Selezionare un utente da modificare.
3. Cercare gli account in base al tipo di endpoint.
4. Selezionare uno o più account.
5. Fare clic sul pulsante Modifica password.
6. Immettere una nuova password.

I criteri delle password di CA Identity Manager convalidano la nuova password.

7. Fare clic su Invia.

Esecuzione di azioni su più account

È possibile eseguire alcune azioni su uno o più account. È ad esempio possibile ripristinare un account sospeso, sbloccare un account nel caso in cui un utente abbia immesso una password errata, oppure assegnare o revocare l'assegnazione di un account a un utente. L'azione viene applicata a tutti gli account selezionati e la procedura è identica.

Per eseguire attività su più account

1. Nella console utente, selezionare Utenti, Modifica account endpoint utente.
2. Selezionare un utente da modificare.
3. Cercare gli account in base al tipo di endpoint.
4. Selezionare uno o più account.
5. Fare clic su uno dei pulsanti sotto Azioni per gli account selezionati.
6. Rispondere alle richieste della finestra di dialogo che viene visualizzata e fare clic su Inoltra.

Operazioni di account avanzate

In Manager di provisioning, è possibile eseguire alcune operazioni aggiuntive sugli account:

- Associare un account a utenti globali diversi
- Esplorare gli account automaticamente
- Eliminare gli account
- Utilizzare l'opzione In attesa di eliminazione
- Ricreare account eliminati

Modificare l'utente globale per un account

Di seguito sono descritti i casi in cui è opportuno associare un account a un utente globale diverso:

- Si hanno due utenti globali con lo stesso nome e CA Identity Manager correla l'account alla persona sbagliata
- CA Identity Manager ha correlato un account all'oggetto [utente predefinito] ma si desidera associarlo a un altro oggetto di tipo utente globale
- È stato creato un account con l'opzione Nuovo e ora si desidera associarlo a un utente globale

Per associare un account a un utente globale diverso in Manager di provisioning, trascinare l'account nell'utente globale corretto.

Funzionamento dell'esplorazione automatica

L'aggiunta o l'eliminazione di account o altri oggetti mediante strumenti nativi per l'endpoint non sono rilevate da CA Identity Manager finché non si esplora l'endpoint. Il processo di esplorazione rileva aggiunte ed eliminazioni (e in alcuni casi le modifiche) che si sono verificate e applica le modifiche alla rappresentazione di CA Identity Manager dell'oggetto nella directory di provisioning.

Tuttavia, se si utilizza Manager di provisioning per tentare di creare un oggetto con lo stesso nome prima dell'esplorazione, in CA Identity Manager viene rilevata l'esistenza di un oggetto con lo stesso nome e viene segnalato un errore. CA Identity Manager esplora quindi l'oggetto, creando una sua rappresentazione nella directory di provisioning. È possibile cominciare a utilizzare l'oggetto immediatamente. L'esplorazione automatica di un oggetto si verifica ogni volta che un'operazione di aggiunta, spostamento o rimozione genera un errore già esistente dall'endpoint, quando l'oggetto non esiste nella directory di provisioning.

È possibile combinare l'esplorazione automatica con il parametro di configurazione dominio di Sincronizzazione/Correlazione automatica descritto nella *Guida di riferimento sul provisioning*. Quando queste funzionalità operano insieme, per prima cosa provano a creare un account da un modello di account come tentativo per la creazione di un nuovo account. Questo processo comprende i seguenti passaggi:

- Rilevazione di un account inesplorato
- Esplorazione automatica dell'account
- Correlazione automatica dell'account all'utente globale
- Aggiunta di un modello di account all'account come se fosse un account esistente correlato a questo utente globale.

Eliminare gli account

Per eliminare un account, è possibile utilizzare i metodi seguenti in Manager di provisioning:

- Fare clic con il pulsante destro del mouse sull'account e selezionare Elimina
- Fare clic con il pulsante destro del mouse su un utente globale e selezionare Delete User and Accounts (Elimina utente e account)
- Eseguire la procedura guidata di eliminazione account
- Sincronizzare gli utenti globali con ruoli di provisioning e specificare che si desidera eliminare gli account aggiuntivi

Quando si rimuove un utente globale da un ruolo di provisioning, il Manager di provisioning fornisce queste opzioni di eliminazione account:

- Se si decide di eliminare questi account, CA Identity Manager rimuove gli account dalla directory di provisioning.
- Se si decide di non eliminare gli account, è possibile utilizzare l'opzione Sincronizza utente con ruolo e selezionare Elimina account.

Quando si rimuove un utente globale da un ruolo di provisioning prima di eliminare gli account, è possibile elencare gli account dell'utente globale. Fare clic con il pulsante destro del mouse sull'utente globale e selezionare List Accounts (Elenca account).

- Nell'elenco account vengono visualizzati i ruoli di provisioning ai quali appartiene ciascun account. Se un account appartiene a un ruolo di provisioning, viene eliminato quando si rimuove quell'utente dal ruolo e si accetta l'azione di sincronizzazione utente per eliminare gli account.
- Se un account non appartiene a un ruolo di provisioning, si tratta di un account aggiuntivo e verrà segnalato mediante la funzione Check User Synchronization (Verifica sincronizzazione utente). L'account viene eliminato selezionando la voce di menu Sincronizza utente con ruolo nell'utente globale.

Utilizzare l'opzione In attesa di eliminazione

È possibile configurare CA Identity Manager su base endpoint per endpoint in modo che gli account di un endpoint non vengano eliminati quando gli amministratori avviano azioni di eliminazione o sincronizzazione che normalmente causano la rimozione degli account. Gli account vengono posti invece nello stato In attesa di eliminazione in CA Identity Manager e nello stato Sospeso sull'endpoint gestito.

È possibile identificare gli account con stato In attesa di eliminazione in Manager di provisioning nella scheda Statistiche delle proprietà dell'account. Per ogni account sospeso viene indicato il motivo dello stato In attesa di eliminazione e la data e ora di ingresso in quello stato. L'archiviazione dello stato In attesa di eliminazione e l'indicazione di ora e data dello stato Sospeso consentono di scrivere un'utilità che identifica questi account con stato In attesa di eliminazione e li elimina dal server di provisioning e dall'endpoint gestito in seguito.

Ricreare gli account eliminati

Se si elimina un account su un endpoint gestito mediante uno strumento diverso da CA Identity Manager, la funzionalità Check Account Synchronization (Controllo sincronizzazione account) segnala l'account come mancante, perché quest'ultimo esiste già nella directory di provisioning ma non sull'endpoint gestito. In questo caso, ricreare l'account sull'endpoint mediante la funzione Synchronize Account with Account Templates (Sincronizza account con modelli account), che consente di ricreare l'account utilizzando un modello di account a esso associato.

Se gli account vengono ricreati, CA Identity Manager li registra come ricreati. È possibile identificare questi account separatamente dagli account che sono stati aggiornati perché gli amministratori devono essere a conoscenza del fatto che gli attributi diversi dagli attributi di compatibilità (ad esempio, le password) sono stati impostati sui valori dei modelli di account originali.

Capitolo 8: Ruoli di fornitura

Questa sezione contiene i seguenti argomenti:

[Ruoli di fornitura e modelli di account](#) (a pagina 203)

[Creazione di ruoli per assegnare account](#) (a pagina 204)

[Attività relative a ruoli e modelli](#) (a pagina 208)

[Attributi nei modelli di account](#) (a pagina 212)

[Espressioni delle regole avanzate](#) (a pagina 216)

[Prestazioni dei ruoli di provisioning](#) (a pagina 223)

[Attività di fornitura per ambienti esistenti](#) (a pagina 225)

Ruoli di fornitura e modelli di account

Per semplificare la gestione degli account, è possibile creare e gestire gli account utilizzando i modelli di account, che vengono utilizzati nelle regole di fornitura. Un ruolo di fornitura contiene uno o più modelli di account. Quando tale ruolo viene applicato a un utente, quest'ultimo riceve gli account definiti dai modelli.

Questi modelli vengono utilizzati come base per gli account in uno specifico tipo di endpoint. Offrono lo stesso tipo di funzionalità dei criteri di fornitura disponibili in eTrust Admin.

I modelli di account consentono di eseguire le operazioni seguenti:

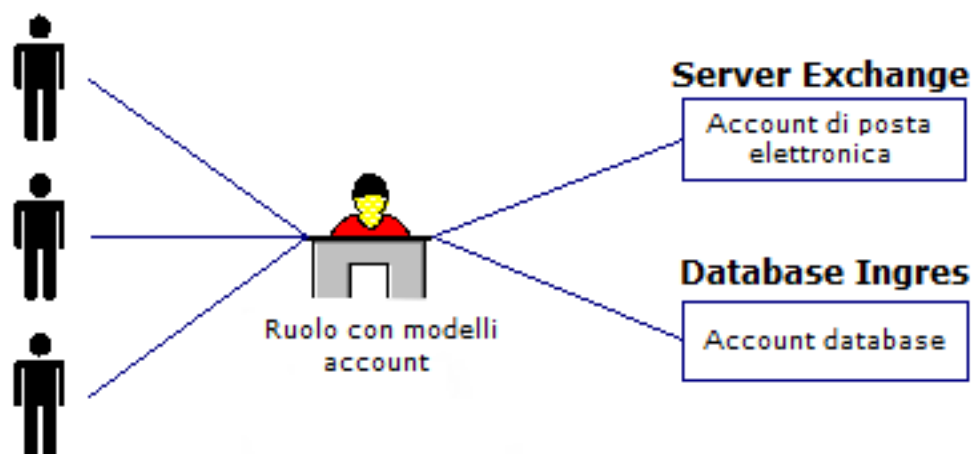
- Controllare di quali attributi di account dispongono gli utenti di CA Identity Manager in un endpoint durante la creazione degli account
- Definire gli attributi utilizzando stringhe o valori di regole
- Combinare gli attributi di account di diversi ruoli di fornitura, in modo che gli utenti dispongano di un solo account, in un determinato endpoint, con tutti gli attributi di account necessari
- Creare o aggiornare gli attributi di account quando gli utenti globali modificano i ruoli di fornitura
- Sincronizzare gli attributi di account in modo che gli utenti globali dispongano solo degli attributi di cui necessitano
- Eseguire query per stabilire quali account devono essere creati, aggiornati o eliminati durante un'operazione di sincronizzazione
- Determinare quali attributi di account possono o non possono essere sincronizzati con i ruoli di fornitura.

Creazione di ruoli per assegnare account

Nella maggior parte delle organizzazioni, fornire account di accesso agli utenti per i diversi sistemi e applicazioni è un'attività che richiede molto tempo agli amministratori. Per semplificare questa attività ripetitiva, è possibile creare ruoli di provisioning, che comprendono modelli di account. I modelli definiscono gli attributi presenti in un tipo di account. Ad esempio, un modello di account per un account Exchange definisce attributi quali le dimensioni della casella di posta elettronica. I modelli di account definiscono anche le modalità di mapping degli attributi utente sugli account.

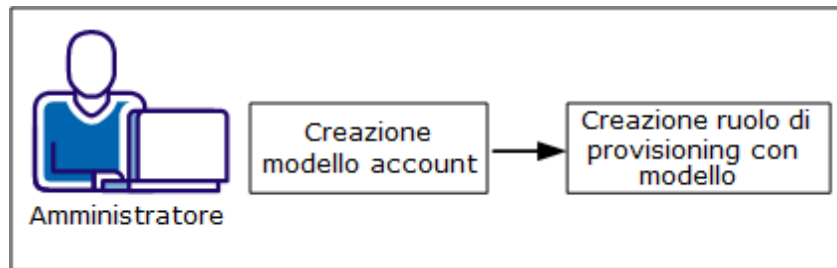
Ad esempio, ogni dipendente dell'azienda Forward, Inc. necessita dell'accesso a un database e alla posta elettronica. Un amministratore desidera evitare di creare un account di database e uno di posta elettronica alla volta per ogni dipendente. Perciò crea un ruolo di provisioning per quell'azienda. Il ruolo comprende un modello di account per il server Microsoft Exchange, per fornire account di posta elettronica e un modello di database Oracle. In questo esempio, il server Exchange e il database Oracle vengono denominati endpoint, ovvero sistemi o applicazioni in cui sono presenti gli account.

Nota: Forward, Inc. è un nome di azienda casuale, utilizzato solo a scopo puramente illustrativo senza alcun riferimento a un'azienda esistente.



Una volta creati i ruoli, gli amministratori aziendali, come i manager o gli addetti all'assistenza, possono assegnarli agli utenti per fornire loro un account negli endpoint. Dopo aver ricevuto il ruolo, gli utenti possono accedere all'endpoint.

La creazione di un ruolo di provisioning che comprende un modello di account è un processo diviso in due fasi, come segue:



Nelle sezioni seguenti si spiega come creare un ruolo che è possibile utilizzare per assegnare account:

1. [Creazione di un modello di account](#) (a pagina 206)
2. [Creazione di un ruolo di provisioning](#) (a pagina 207)

Creazione di un modello di account

Per semplificare la gestione degli account, è possibile creare e gestire gli account utilizzando i modelli di account, che vengono utilizzati nelle regole di fornitura. Un ruolo di fornitura contiene uno o più modelli di account. Quando tale ruolo viene applicato a un utente, quest'ultimo riceve gli account definiti dai modelli.

Questi modelli vengono utilizzati come base per gli account in uno specifico tipo di endpoint.

I modelli di account consentono di eseguire le operazioni seguenti:

- Controllare di quali attributi account dispongono gli utenti in un endpoint durante la creazione degli account
- Definire gli attributi utilizzando stringhe o valori di regole
- Combinare gli attributi di account di diversi ruoli di fornitura, in modo che gli utenti dispongano di un solo account, in un determinato endpoint, con tutti gli attributi di account necessari
- Creare o aggiornare gli attributi di account quando gli utenti globali modificano i ruoli di fornitura

Con il server CA Identity Manager viene installato un modello di account predefinito per ogni tipo di endpoint. In un ruolo di fornitura è possibile utilizzare il modello di account predefinito, oppure creare modelli di account personalizzati per qualsiasi endpoint configurato.

Per creare un modello di account

1. Accedere a Endpoint, il quale potrebbe trovarsi in Attività, quindi fare clic su Modelli account, Crea modello account.
2. Selezionare un tipo di endpoint per il modello.
3. Definire il Nome endpoint come nome di sistema dell'endpoint, oppure localhost, se opportuno.
4. Selezionare un endpoint da utilizzare nella scheda Endpoint.
5. Compilare i campi nelle schede oppure utilizzare i valori predefiniti.
Ogni tipo di endpoint presenta una serie di schede diverse. Fare clic su ? per la definizione dei campi.
6. Fare clic su Inoltra.

Nota: Se durante la ricerca di oggetti di endpoint nel modello account viene specificato più di un endpoint, viene restituito il sottoinsieme comune (intersezione) degli oggetti correlati. Un esempio è un gruppo Active Directory che esiste su ciascuno degli endpoint selezionati associati al modello di account. Se i risultati della ricerca mostrano attributi diversi dal nome oggetto, vengono visualizzati i valori di attributo degli oggetti associati al primo endpoint. Un esempio è l'attributo di descrizione dell'oggetto lingua in un connettore PeopleSoft.

Creazione di un ruolo di provisioning

È possibile creare un ruolo di provisioning dopo aver definito i relativi requisiti seguenti:

- Utenti per i quali è necessario creare altri account
- Account associati al ruolo
- Membri, amministratori e titolari del ruolo

Per creare un ruolo di provisioning

1. Nella console utente fare, accedere a Ruoli e attività, Ruoli di provisioning, Crea ruolo di provisioning.

Per ulteriori informazioni su ogni scheda, fare clic sul collegamento ? disponibile in ogni schermata.

2. Completare la scheda Profilo. Solo il campo Nome è obbligatorio.

Nota: nella scheda Profilo è possibile specificare attributi personalizzati con i quali specificare informazioni aggiuntive sui ruoli di provisioning. Tali informazioni aggiuntive sono utili per facilitare le ricerche di ruoli in ambienti che presentano un numero elevato di ruoli.

3. Completare la scheda Modelli di account.

- a. Fare clic su un tipo di endpoint, ad esempio Active Directory.
- b. Fare clic su un modello di account.

I modelli che è possibile scegliere si basano sul tipo di endpoint selezionato.

- c. Aggiungere il numero di modelli di account desiderato, a seconda dei diversi tipi di endpoint.

4. Completare la scheda Ruoli di provisioning per nidificare i ruoli di provisioning in questa scheda.

Questo passaggio richiede che sono stati attivati i [ruoli nidificati](#) (a pagina 212) per questo ambiente.

5. Completare la scheda Amministratori mediante l'aggiunta di regole di amministrazione che controllano gli utenti che gestiscono i membri e gli amministratori del ruolo corrente.

6. Completare la scheda Titolari aggiungendo regole di titolari che controllano gli utenti in grado di modificare il ruolo corrente.
7. Fare clic su Inoltra.
8. Per verificare che il ruolo sia stato creato, fare clic su Ruoli di provisioning, Visualizza ruolo di provisioning.

Attività relative a ruoli e modelli

Nella console utente è possibile creare e gestire ruoli di fornitura scegliendo Ruoli e attività e selezionando un'attività in Fornitura ruoli. Esistono attività per le operazioni standard, quali l'inclusione di un utente in un ruolo e la modifica o l'eliminazione di un ruolo.

Prima di creare un ruolo di fornitura è necessario un modello di account da includere in tale ruolo oppure un ruolo di fornitura da importare. È possibile importare ruoli creati in Gestore fornitura o in eTrust Admin. In CA Identity Manager, tuttavia, non sono supportati i ruoli nidificati creati in eTrust Admin.

Importazione di un ruolo di provisioning

Nonostante sia possibile gestire i ruoli di fornitura nella console utente, è possibile che alcuni ruoli di provisioning siano stati creati in Gestione provisioning oppure in un'applicazione esterna. Per questi ruoli di provisioning è possibile reimpostare il titolare del ruolo in modo che sia un amministratore di CA Identity Manager, così da poterlo gestire nella console utente.

Per importare un ruolo di provisioning

1. Accedere alla console utente come utente con il ruolo di Gestore di sistema. Fare clic su Attività, Ruoli e attività.
2. Fare clic sul provisioning dei ruoli, Reimposta titolari ruolo di provisioning, quindi selezionare un ruolo di provisioning creato in Gestione provisioning.
3. Completare la scheda Titolari aggiungendo regole di titolari che controllano gli utenti in grado di modificare il ruolo corrente.
4. Fare clic su Inoltra.

A questo punto, il ruolo può essere modificato, assegnato o visualizzato mediante l'aggiunta di attività nella categoria Fornitura Ruoli.

Assegnazione di nuovi titolari ai ruoli di provisioning

È possibile selezionare uno o più ruoli di provisioning e assegnare criteri di proprietà per controllare gli utenti autorizzati a modificare i ruoli.

Per assegnare nuovi titolari ai ruoli di provisioning

1. Accedere alla console utente come utente con il ruolo di Gestore di sistema.
2. Fare clic su Attività, Ruoli, oppure fare clic su Ruoli, quindi su Attività.
3. Fare clic su Ruoli di provisioning, Crea criteri di proprietà per i ruoli di provisioning.
4. Selezionare uno o più ruoli di provisioning.
5. Completare la scheda Titolari aggiungendo regole di titolari che controllano gli utenti in grado di modificare il ruolo corrente.
6. Fare clic su Inoltra.

Gli utenti che soddisfano i nuovi criteri di titolare possono modificare i ruoli di provisioning selezionati.

Password per gli account creati dai ruoli di provisioning

Quando a un utente viene assegnato un ruolo di provisioning, la creazione dell'account per tale utente non riesce se la password dell'utente CA Identity Manager non soddisfa i requisiti per le password dell'endpoint. Questa situazione include la creazione di un nuovo utente con una password temporanea.

Pertanto, impostare il criterio di password in modo che corrisponda o sia più rigido rispetto ai requisiti di password dell'endpoint. È possibile impostare il criterio di password mediante il campo Criteri di password o Provisioning Password Profile (Provisioning profilo password) di CA Identity Manager. Se si utilizzano entrambi i metodi, i criteri devono corrispondere.

Ordine di elaborazione degli eventi dei ruoli di provisioning

Alcune attività predefinite di CA Identity Manager includono *eventi*, cioè azioni eseguite da CA Identity Manager per portare a termine un'attività, che determinano l'appartenenza al ruolo di provisioning. Ad esempio, l'attività predefinita Modifica utente include gli eventi AssignProvisioningRoleEvent e RevokeProvisioningRoleEvent. L'assegnazione o la revoca di un ruolo di provisioning può causare l'aggiunta o la rimozione di un account in un endpoint. In alcuni casi, l'endpoint può richiedere che tutte le azioni di aggiunta vengano eseguite prima di quelle di rimozione.

Per imporre l'elaborazione prioritaria delle azioni di aggiunta in CA Identity Manager, abilitare l'impostazione Accumulation of Provisioning Role Membership Events (Accumulo eventi di appartenenza al ruolo di provisioning) nella console di gestione. Dopo aver abilitato questa impostazione, in CA Identity Manager tutte le azioni di aggiunta e rimozione verranno accumulate in un unico evento denominato AccumulatedProvisioningRolesEvent. Ad esempio, se l'attività Modifica utente assegna tre ruoli di provisioning a un utente e ne rimuove altri due, viene generato un evento AccumulatedProvisioningRolesEvent contenente cinque azioni, ossia tre di aggiunta e due di rimozione.

Quando l'evento viene eseguito, tutte le azioni di aggiunta vengono unite in un'unica operazione e inviate al server di provisioning per l'elaborazione. Una volta completata l'elaborazione delle azioni di aggiunta, CA Identity Manager unisce le azioni di rimozione in un'unica operazione che viene inviata al server di provisioning.

Questa impostazione, se abilitata, influisce sulle seguenti funzionalità di CA Identity Manager:

- **Scheda Ruoli di provisioning nelle attività utente**

Quando un amministratore aggiunge o rimuove un ruolo di provisioning per un utente tramite la scheda Ruoli di provisioning, in CA Identity Manager queste azioni vengono accumulate in un unico evento.

- **Criteri di identità**

Tutti gli eventi di appartenenza a un ruolo di provisioning (AssignProvisioningRoleEvent o RevokeProvisioningRoleEvent) generati per effetto di una valutazione dei criteri di identità vengono accumulati in un unico evento AccumulatedProvisioningRolesEvent. Questo evento viene eseguito in CA Identity Manager come qualsiasi altro evento secondario. Ad esempio, in un set di criteri di identità costituito da due criteri: il Criterio A revoca l'appartenenza al Ruolo di provisioning A e il Criterio B assegna agli utenti il Ruolo di provisioning B. Se in CA Identity Manager si determina che un utente non soddisfa più il Criterio A, mentre soddisfa il Criterio B, viene generato un evento AccumulatedProvisioningRolesEvent contenente due azioni, una di rimozione e una di aggiunta. L'azione di aggiunta viene eseguita per prima e in seguito viene eseguita quella di rimozione.

■ Visualizzazione delle attività inoltrate

Per visualizzare lo stato dell'evento AccumulatedProvisioningRolesEvent e lo stato di ciascuna delle singole azioni utilizzare l'attività Visualizza attività inoltrate per visualizzare i dettagli dell'evento.

Se una delle singole azioni non riesce, l'evento assume lo stato di non riuscito, che viene propagato anche all'attività.

■ Flusso di lavoro

È possibile associare un processo di flusso di lavoro all'evento AccumulatedProvisioningRolesEvent. In tal caso, un revisore potrà approvare o rifiutare l'intero evento, causando così l'approvazione o il rifiuto dei singoli eventi.

Per attivare il flusso di lavoro per singoli eventi in AccumulatedProvisioningRolesEvent è necessaria ulteriore configurazione.

■ Verifica

In CA Identity Manager vengono verificate le informazioni su AccumulatedProvisioningRolesEvent e sui singoli eventi.

Attivazione dell'accumulo degli eventi di appartenenza a un ruolo di fornitura

Nella console di gestione di CA Identity Manager è disponibile un'impostazione che consente di unire in un'unica operazione tutte le azioni di aggiunta e rimozione relative a un evento di appartenenza a un ruolo di fornitura. Una volta unite, le azioni di aggiunta vengono elaborate prima delle azioni di rimozione, come se si trattasse di un'unica operazione.

È in tal modo possibile creare le sequenze di eventi richieste da alcuni tipi di endpoint.

Nota: questa funzione è disattivata per impostazione predefinita.

Attivazione dell'accumulo degli eventi di appartenenza a un ruolo di fornitura

1. Accedere alla console di gestione di Identity Manager.
2. Fare clic su Environments (Ambienti).
3. Selezionare l'ambiente da configurare.
4. Aprire le impostazioni avanzate e selezionare Provisioning (Fornitura).
5. Selezionare la casella Enable Accumulation of Provisioning Role Membership Events (Attiva accumulo eventi di appartenenza ai ruoli di fornitura).
6. Riavviare il server applicazioni.

Abilitazione di ruoli nidificati in un ambiente

È possibile includere un ruolo di provisioning all'interno di un altro ruolo di provisioning. Il ruolo incluso si chiama ruolo nidificato.

Ad esempio, è possibile creare un ruolo di provisioning Dipendente. Il ruolo Dipendente potrebbe essere utilizzato per fornire ai dipendenti gli account necessari, ad esempio gli account di posta elettronica. È possibile inoltre includere il ruolo Dipendente in ruoli di provisioning specifici dei dipartimenti, quali un ruolo Finanza e un ruolo Vendite. In tal modo, i ruoli di provisioning del dipartimento forniscono gli account solo per il reparto assegnato. Questa combinazione di ruoli fornisce l'account corretto a ciascun utente.

Per abilitare i ruoli nidificati in un ambiente

1. Nella console di gestione selezionare un ambiente.
2. Fare clic su Role and Task Settings (Impostazioni ruolo e attività), Importa.
3. Selezionare Supporto ruoli di provisioning nidificati.
4. Fare clic su Fine.
5. Riavviare l'ambiente.

Inclusione di un ruolo in un ruolo di provisioning

Per includere un ruolo in un ruolo di provisioning

1. Fare clic su Ruoli e attività, Ruoli di provisioning, Modifica ruolo di provisioning.
2. Completare la scheda Ruoli di provisioning facendo clic su Aggiungi ruolo e selezionare un ruolo di provisioning.

Per motivi di prestazioni, si consiglia di limitare il ruolo a tre livelli di nidificazione. Ad esempio, si includano nel ruolo di provisioning corrente (il primo ruolo) un altro ruolo (il ruolo di secondo livello), che può contenere un ruolo di terzo livello. È consigliabile che il ruolo di terzo livello non contenga alcun ruolo.

3. Completare il criterio di titolarità modificando la regola di titolarità.
L'ambito deve essere uguale o più ampio rispetto all'ambito per il ruolo aggiunto.
4. Fare clic su Inoltra.

Attributi nei modelli di account

Nei modelli di account gli attributi determinano le modalità di definizione degli stessi nell'account.

Attributi di compatibilità e attributi iniziali

I modelli di account includono due tipi di attributi:

- *Gli attributi di compatibilità* rappresentano le informazioni dell'account, quali dimensioni di archiviazione, quantità, limiti di frequenza o appartenenza ai gruppi. Il manager di provisioning marca in grassetto gli attributi di compatibilità in tutti gli schermi dei modelli di account, per agevolarne l'identificazione.
- *Gli attributi iniziali* rappresentano tutte le informazioni impostate inizialmente per un account, quali nome account, password e stato dell'account, e le informazioni personali, quali nome, indirizzo e numeri di telefono.

Gli account sono considerati sincronizzati con i relativi modelli di account quando tutti gli attributi di compatibilità sono sincronizzati. Questi attributi variano a seconda del tipo di endpoint, ad esempio appartenenza ai gruppi, privilegi, quote e restrizioni di accesso, che determinano le operazioni che l'utente può effettuare quando accede all'account.

La sincronizzazione non aggiorna altri attributi dell'account, che vengono inizializzati dai modelli di account durante la creazione dell'account e che possono essere aggiornati con le funzioni di propagazione. Il server di provisioning dispone di due funzioni di propagazione: l'aggiornamento immediato degli account al momento della modifica del modello di account e l'aggiornamento degli account al momento della modifica degli attributi dell'utente globale.

Individuazione degli attributi di compatibilità e degli attributi iniziali

Per scoprire quali attributi sono definiti di compatibilità e quali sono attributi iniziali, è necessario generare il file eTACapability.txt. Immettere il comando seguente da un prompt dei comandi di Windows:

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

Specifica C:\Program Files\CA\Identity Manager\Provisioning Server\bin

Viene generata una versione del file per tutti i connettori installati.

Stringhe di regola nei modelli di account

Quando viene creato un modello di account, si utilizzano le stringhe di regola per definire il formato di molti attributi di account. Le stringhe di regola sono variabili del valore attuale. Le stringhe di regola si rivelano particolarmente utili quando vengono generati attributi per il passaggio da un account a un altro. Durante la valutazione delle regole, CA Identity Manager sostituisce le stringhe di regola immesse nei modelli di account con i dati specificati nell'oggetto utente.

Nota: la valutazione delle regole non viene eseguita sugli account creati durante esplorazione o senza ruoli di fornitura.

Nella tabella seguente sono elencate le stringhe di regole in CA Identity Manager:

Stringa regola	Descrizione
%AC%	Nome account
%D%	Data corrente nel formato <i>gg/mm/aaaa</i> (la data è un valore calcolato non contenente informazioni sull'utente globale). Questa regola stringa è equivalente a una delle seguenti: %\$\$DATE()% %\$\$DATE%
%EXCHAB%	Cassetta postale nascosta dall'elenco indirizzi Exchange
%EXCHS%	Nome server principale cassetta postale
%EXCMS%	Nome archivio cassette postali
%GENUID%	Identificatore utente UNIX/POSIX numerico. Questa variabile di regola è uguale a %UID% se è impostato il valore UID dell'utente globale. Se invece all'utente globale non è assegnato un valore UID ed è abilitata la generazione di UID (Global Properties (Proprietà globali) in System Task (Attività sistema)), si verificano alcune azioni. Il successivo valore UID disponibile viene allocato, assegnato all'utente globale e utilizzato come valore per questa variabile di regola.
%P%	Password
%U%	Nome utente globale
%UA%	Indirizzo completo (generato da via, città, stato e codice postale)
%UB%	Edificio
%UC%	Città
%UCOMP%	Nome società
%UCOUNTRY%	Paese

Stringa regola	Descrizione
%UCUxx% o %UCUxxx%	Campo personalizzato (xx o xxx rappresenta l'ID campo a 2 o 3 cifre specificato nella scheda Custom User Fields (Campi utente personalizzati) del frame System Task (Attività sistema))
%UD%	Descrizione
%UDEPT%	Reparto
%UE%	Indirizzo e-mail
%UEP%	Indirizzo di posta elettronica principale
%UES%	Indirizzi di posta elettronica secondari
%UF%	Nome
%UFAX%	Numero di fax
%UHP%	Pagina iniziale
%UI%	Iniziali
%UID%	Identificatore utente UNIX/POSIX numerico
%UL%	Cognome
%ULOC%	Posizione
%UMI%	Iniziale secondo nome
%UMN%	Secondo nome
%UMP%	Numero di cellulare
%UN%	Nome completo
%UO%	Nome ufficio
%UP%	Numero di telefono
%UPAGE%	Numero di cercapersone
%UPC%	Codice postale, CAP
%UPE%	Interno telefonico
%US%	Stato
%USA%	Indirizzo
%UT%	Professione

Stringa regola	Descrizione
%XD%	Genera l'indicatore orario corrente nel formato dateTimeValue XML, un formato di stringa a lunghezza fissa. In un attributo dateValue o timeValue, è possibile scrivere un'espressione di sottostringa (:offset,length) per estrarre le parti di dateTimeValue relative a data e ora. Ad esempio, il risultato di %XD:1,10% sarà AAAA-MM-GG e il risultato di %XD:12,8% sarà HH:MM:SS.

Valori per gli attributi

Per utilizzare uno specifico valore costante per un attributo account, immettere il valore nel campo del modello di account anziché in una stringa di regola. Ad esempio, è possibile definire valori per specificare limiti di frequenza o dimensioni di quantità.

Se il valore costante dell'attributo deve contenere più segni di percentuale, immettere due segni di percentuale (%%) ogni volta. Verranno convertiti in un segno di percentuale (%) al momento della generazione del valore dell'attributo account. Se il valore del modello di account contiene un solo segno di percentuale, non verrà generato un errore. La regola indica che se si desidera un valore letterale del 25%, è necessario specificare 25%%. Tuttavia, come caso particolare, il valore 25% verrà accettato.

Espressioni delle regole avanzate

Per assicurare una maggiore flessibilità rispetto alla semplice sostituzione degli attributi dell'utente globale, è possibile immettere espressioni delle regole avanzate, elencate qui di seguito:

- Sottostringhe di espressioni delle regole che utilizzano offset e lunghezza
- Combinazioni di stringhe e valori delle regole
- Espressioni delle regole per impostare più valori per attributi di account con più valori
- Variabili delle regole per altri attributi dell'utente globale
- Chiamata di funzioni incorporate
- Chiamata di funzioni di chiusura del programma scritte dal cliente

Combinazione di stringhe e valori delle regole

È possibile combinare stringhe di regole e valori costanti in un valore di attributo di modello di account. Ad esempio, se non vi fossero stringhe di regole %UI%, sarebbe possibile ottenere lo stesso effetto concatenando più espressioni delle regole, come segue:

```
%UF: ,1%%UMI: ,1%%UL: ,1%
```

La stringa della regola %UA% equivalente a una delle seguenti:

```
%USA%, %UC%, %US%, %UPC%
```

È inoltre possibile combinare una stringa della regola con un valore costante per creare un attributo di endpoint principale UNIX come segue:

```
/u/home/%AC%
```

Sottostringhe delle regole

La sintassi per la creazione di un valore di sottostringa di una variabile della regola è la seguente:

```
%variabile[:offset, lunghezza]%
```

variabile

Rappresenta il nome della variabile della regola predefinita, specificata nella tabella sopra riportata.

offset

(Facoltativo) Specifica l'offset iniziale del suffisso della sottostringa. Il numero 1 rappresenta il primo carattere.

lunghezza

(Facoltativo) Specifica la posizione finale del suffisso della sottostringa. Il simbolo di asterisco (*) indica fino alla fine del valore.

Ad esempio, per impostare un attributo di account sui primi 4 caratteri di un attributo Edificio di un utente globale, utilizzare la seguente espressione per definire la variabile:

```
%UB:1,4%
```

Se l'attributo Edificio è vuoto o contiene meno di quattro caratteri, il valore dell'attributo dell'account risultante conterrà meno di quattro caratteri.

Espressioni delle regole con più valori

La maggior parte delle espressioni delle regole hanno un valore singolo. Iniziano da un valore di attributo utente (possibilmente vuoto) e il risultato è un valore di attributo account (a sua volta possibilmente vuoto). Talvolta però può essere necessario considerare un attributo utente vuoto come avente valore 0. Talvolta può essere inoltre necessario generare valori multipli per compilare un valore di attributo account con più valori.

La sintassi sotto indicata consente di lavorare con valori zero o con più valori di quanto un attributo utente possa contenere:

`%*var%`

L'asterisco (*), che costituisce un flag con più valori facoltativo, posto immediatamente dopo il primo segno di percentuale (%) di un'espressione di una regola, indica che il risultato di questa espressione deve essere 0, 1 o più di 1 valore a seconda di quanti valori sono contenuti nell'attributo utente a cui viene fatto riferimento.

La maggior parte dei valori dell'attributo utente sono valori singoli, quindi possono contenere solo 0 o 1 valore. Gli attributi personalizzati (da CustomField01 a CustomField99), invece, sono attributi con più valori, quindi una variabile della regola che fa riferimento a questi attributi può contenere 0, 1 o più di 1 valore.

Se un attributo utente ha più di 1 valore ma non viene specificato l'asterisco (*) nell'espressione della regola, il risultato del calcolo della regola sarà quello del primo valore. In genere, tuttavia, i valori dell'attributo non sono ordinati e quindi non è dato sapere quale valore CA Identity Manager considererà primo.

Se un attributo utente ha più di un valore e si include l'asterisco nell'espressione della regola, vengono generati valori multipli per l'attributo account. Tale espressione della regola con più valori non va definita in un modello di account se l'attributo account impostato dall'attributo del modello account non è a sua volta con più valori.

È possibile definire un attributo account esteso nel tipo di endpoint ADS in modo che abbia più valori e utilizzare questa sintassi di espressione della regola con più valori in modo che imposti tale attributo. Si consideri ad esempio un ambiente che definisce un attributo account ADS esteso denominato brevetti e un attributo utente personalizzato numero 3 denominato a sua volta brevetti.

Un modello di account ADS potrebbe definire, per l'attributo brevetti, la stringa della regola `%*UCU03%`. In seguito si potrebbe modificare l'attributo brevetti dell'utente aggiungendo uno o più valori. Quando si applicano le modifiche all'utente, selezionare l'opzione di aggiornamento degli account dell'utente. Grazie a tale opzione il modello di account dell'account viene esaminato, quindi viene individuata la variabile della regola `%*UCU03%` e tutti i brevetti dell'utente vengono copiati nell'attributo utente denominato brevetti.

Allo stesso modo, durante la creazione degli account, le stringhe delle regole vengono calcolate. Inoltre, nel corso della modifica dell'account, se la stringa della regola è stata modificata, è possibile ricalcolare la regola per tutti gli account associati al modello di account.

La sintassi `%*var%` è valida anche per le variabili *var* che fanno riferimento agli attributi utente con valore singolo. Ciò vale solo quando è richiesta la concatenazione e nel caso in cui gli attributi a cui si fa riferimento non sono impostati per gli utenti.

L'asterisco flag con più valori facoltativo indica che la regola contenente una variabile della regola `%*var%` non calcola alcun valore se l'attributo utente non ha valori.

L'espressione `%var%` invece calcola sempre un valore singolo, anche se si tratta di una stringa vuota.

Per capire la differenza, si considerino le seguenti stringhe di regola:

```
(310)%UP%  
(310)%*UP%
```

Sembrerebbe che entrambe aggiungano il prefisso 310 al numero di telefono, e invece sono diverse perché se l'utente non ha un valore per il numero di telefono, la prima genera il valore (310) mentre la seconda non genera alcun valore e lascia l'attributo account non impostato.

Si considerino invece le seguenti stringhe che parrebbero aggiungere l'interno del numero di telefono al numero di telefono:

```
%UP% %UPE%  
%UP% %*UPE%
```

Se tutti hanno un numero di telefono ma alcuni non hanno interno, la prima stringa della regola genera un valore che comprende il numero di telefono per ciascun utente senza interno, invece la seconda non genera valori. In questo caso, utilizzare la prima regola con `%UPE%`.

Regole esplicite dell'Attributo utente globale

Ciascun utente ha molti più attributi di quelli elencati nella precedente tabella delle regole. Probabilmente non sarà necessario creare espressioni di regole con riferimenti a tali attributi, tuttavia, qualora ciò risultasse necessario, è necessario usare la seguente sintassi per fare riferimento a un determinato attributo dell'utente:

`%#attributo-ldap%`

Ad esempio, se è necessario determinare il valore del campo Sospeso dell'utente, bisognerà determinare il corrispondente nome di attributo LDAP per questo campo (che è eTSuspended) e creare l'espressione della regola che calcola 0 o 1, come eTSuspended:

`%#eTSuspended%`

Per fare un altro esempio, è possibile ottenere i ruoli di fornitura assegnati dell'utente con la seguente espressione della regola:

`%*#eTRoleDN%`

Questi ruoli di fornitura sono valori di nomi LDAP distinti. Forse, in associazione con la funzione incorporata RDNVALUE (vedere tabella qui di seguito), i valori ottenuti potrebbero risultare più utili. Si noti che l'asterisco (*) è il segno che indica più valori e che quindi, nell'esempio di cui sopra, consente di ottenere tutti i ruoli di fornitura assegnati dell'utente come valori molteplici.

Anche la sintassi delle sottostringhe è applicabile a queste espressioni delle regole, quindi si potrebbe ad esempio utilizzare `%#eTTelephone:6,*%` per indicare `%UP:6,*`. Entrambe chiedono a CA Identity Manager di eliminare i primi cinque caratteri del campo Telephone dell'utente.

Funzioni delle regole incorporate

Nelle espressioni delle regole è possibile utilizzare funzioni incorporate che consentono di eseguire determinate operazioni sui valori. Il formato generico della chiamata di funzione della regola incorporata è

`%[*]$$funzione(arg[,...])[:offset, lunghezza]%`

dove l'asterisco (*) indica più valori e offset e lunghezza sono, anche in questo caso, facoltativi.

Le funzioni incorporate riconosciute sono le seguenti:

Funzione delle regole incorporata	Descrizione
ALLOF	Unisce tutti i parametri in un attributo con più valori. L'ordine viene mantenuto e i duplicati vengono eliminati. Se ad esempio gli attributi utente sono impostati come segue: eTCustomField01: { A, B } eTCustomField02: { A, C } Quindi, la regola <code>%*ALLOF(%*UCU01%,%*UCU02%)%</code> calcola tre valori { A, B, C }.
DATE	Calcola la data corrente in formato <i>gg/mm/aaaa</i>. L'espressione della regola <code>%D%</code> è equivalente a una delle seguenti: <code>\$\$\$DATE()%</code> <code>\$\$\$DATE%</code>
FIRSTOF	Restituisce il primo valore di uno qualsiasi dei parametri. Utilizzata per inserire un valore predefinito se un attributo non è impostato: <code>\$\$\$FIRSTOF(%UCU01%, 'unknown')%</code> <code>\$\$\$FIRSTOF(%LN%, %UCU01%, %U%)%</code> Se nessuno dei valori è impostato, il risultato è nessun valore. Per immettere una stringa costante in un argomento, racchiuderla tra virgolette semplici.
INDEX	Restituisce un valore di un attributo con più valori. Indice 1 è il primo valore. Se l'indice supera il numero di valori, il risultato è il valore vuoto. Le seguenti regole equivalgono a quanto segue: <code>\$\$\$INDEX(%*UCU01%, 1)%</code> <code>\$\$\$FIRSTOF(%*UCU01%)%</code>

Funzione delle regole incorporata	Descrizione
NOTEMPTY	Restituisce il singolo valore del suo unico argomento, ma segnala un errore se questo valore di attributo non è impostato. Esempio 1 La creazione o l'aggiornamento dell'account non vengono eseguiti se l'utente non ha un attributo UID assegnato: <pre>%%\$NOTEMPTY(%UID%)%</pre> Esempio 2 Utilizza il nome, ma se questo non è impostato utilizza il cognome. Se nessuno dei due è impostato, la creazione o l'aggiornamento dell'account non vengono eseguiti. <pre>%%\$NOTEMPTY(%%\$FIRSTOF(%UF%, %UL%)%)%</pre>
PRIMARYEMAIL	Restituisce l'indirizzo di posta elettronica principale estratto da più indirizzi di posta elettronica. L'espressione %UE% è equivalente a quanto segue: <pre>%%\$PRIMARYEMAIL(%UEP%)%</pre>
RDNVALUE	Tratta il valore dell'attributo come nome LDAP distinto ed estrae il nome comune dell'oggetto dal DN in questione: <pre>%%\$RDNVALUE(%#eTRoleDN%)%</pre> Vengono restituiti i nomi comuni di tutti i ruoli di fornitura assegnati. Se l'utente appartiene a due ruoli di fornitura aventi lo stesso nome comune, il nome del ruolo viene elencato una sola volta.
TOLOWER	Converte le maiuscole in minuscole: <pre>%%\$TOLOWER(%AC%)%</pre>
TOUPPER	Converte le minuscole in maiuscole: <pre>%%\$TOUPPER(%U%)%</pre>

Funzione delle regole incorporata	Descrizione
TRIM	Rimuove i caratteri di spazio iniziali e finali dal valore di un attributo. Ad esempio “%UF %UL%” genera un valore con un nome e un cognome separati da uno spazio. Se però l'utente non ha un attributo nome, questa regola genera un valore che termina con uno spazio. Tuttavia, utilizzando “%\$\$TRIM(%UF% %UL%)%” nessuno spazio viene lasciato nel valore dell'attributo dell'account anche se uno Nome o Cognome non sono impostati.

Prestazioni dei ruoli di provisioning

Quando si utilizza CA Identity Manager con un server di provisioning, è possibile migliorare alcuni aspetti legati alle prestazioni di provisioning.

Cache oggetto JIAM

Identity Manager comunica con il server di fornitura mediante l'API Java IAM (JIAM). Per migliorare le prestazioni di comunicazione, è necessario configurare una cache per gli oggetti reperiti dal server di fornitura.

Attivazione della cache JIAM

Per attivare la cache JIAM

1. Accedere alle impostazioni ambientali mediante la console di gestione. Selezionare Impostazioni avanzate, Varie.
 2. Configurare le proprietà definite dall'utente per la cache JIAM.
 - **Proprietà:** JIAMCache
 - **Valore:** true
 3. Fare clic su Aggiungi.
 4. Fare clic su Salva.
- La proprietà definita dall'utente viene salvata.

Definizione del TTL (Time-to-live) della cache JIAM

La cache JIAM memorizza le informazioni per un periodo di tempo specificato prima che i dati scadano. Tale periodo è detto time-to-live (TTL). Per definire per quanto tempo i dati devono rimanere nella cache, è necessario impostare un valore in secondi.

Per ottenere il massimo vantaggio dai dati in una cache locale, è necessario bilanciare prestazioni potenziate e tempestività. Si raccomanda di utilizzare un valore TTL minimo di 1 giorno e massimo di 7 giorni. Per sapere quale valore TTL utilizzare, consultare la seguente tabella:

Durata desiderata	Impostazioni TTL (secondi)
24 ore (1 giorno)	86.400
72 ore (3 giorni)	259.200
120 ore (5 giorni)	432.000
168 ore (7 giorni)	604.800

Per definire il TTL della cache JIAM TTL

1. Accedere all'ambientale mediante la console di gestione. Selezionare Impostazioni avanzate, Varie.
2. Configurare le proprietà definite dall'utente per il TTL della cache JIAM.
 - **Proprietà:** JIAMCacheTTL
 - **Valore:** numero di secondi per i quali i dati permangono nella cache JIAM
3. Fare clic su Aggiungi.
4. Fare clic su Salva.

Impostazione predefinita: 300

La proprietà definita dall'utente viene salvata.

Pooling di sessione

Per migliorare le prestazioni, Identity Manager può pre-assegnare un numero di sessioni che verranno sottoposte a pooling durante la comunicazione con il server di fornitura.

Per ulteriori informazioni sul pooling di sessione, consultare la *Guida in linea della console di gestione*.

Attività di fornitura per ambienti esistenti

Se si importano definizioni di ruoli personalizzati e si desidera attivare la fornitura in un ambiente, è necessario importare *anche* le definizioni del ruolo di solo provisioning nella console di gestione. Tali definizioni si trovano nella cartella:

`iam_im.ear\management_console.war\WEB-INF\Template\environment`

Nota: per ulteriori informazioni sull'importazione delle definizioni dei ruoli, consultare la *Guida alla configurazione*.

Capitolo 9: Servizi gestiti (richieste di accesso di base)

Questa sezione contiene i seguenti argomenti:

[Creazione di un servizio](#) (a pagina 228)

[Procedura per rendere i servizi disponibili agli utenti](#) (a pagina 239)

[Modifica di un servizio](#) (a pagina 242)

[Aggiunta di una ricerca all'accesso e visualizzazione dell'accesso](#) (a pagina 244)

[Eliminazione di un servizio](#) (a pagina 245)

[Rinnovo dell'accesso a un servizio](#) (a pagina 247)

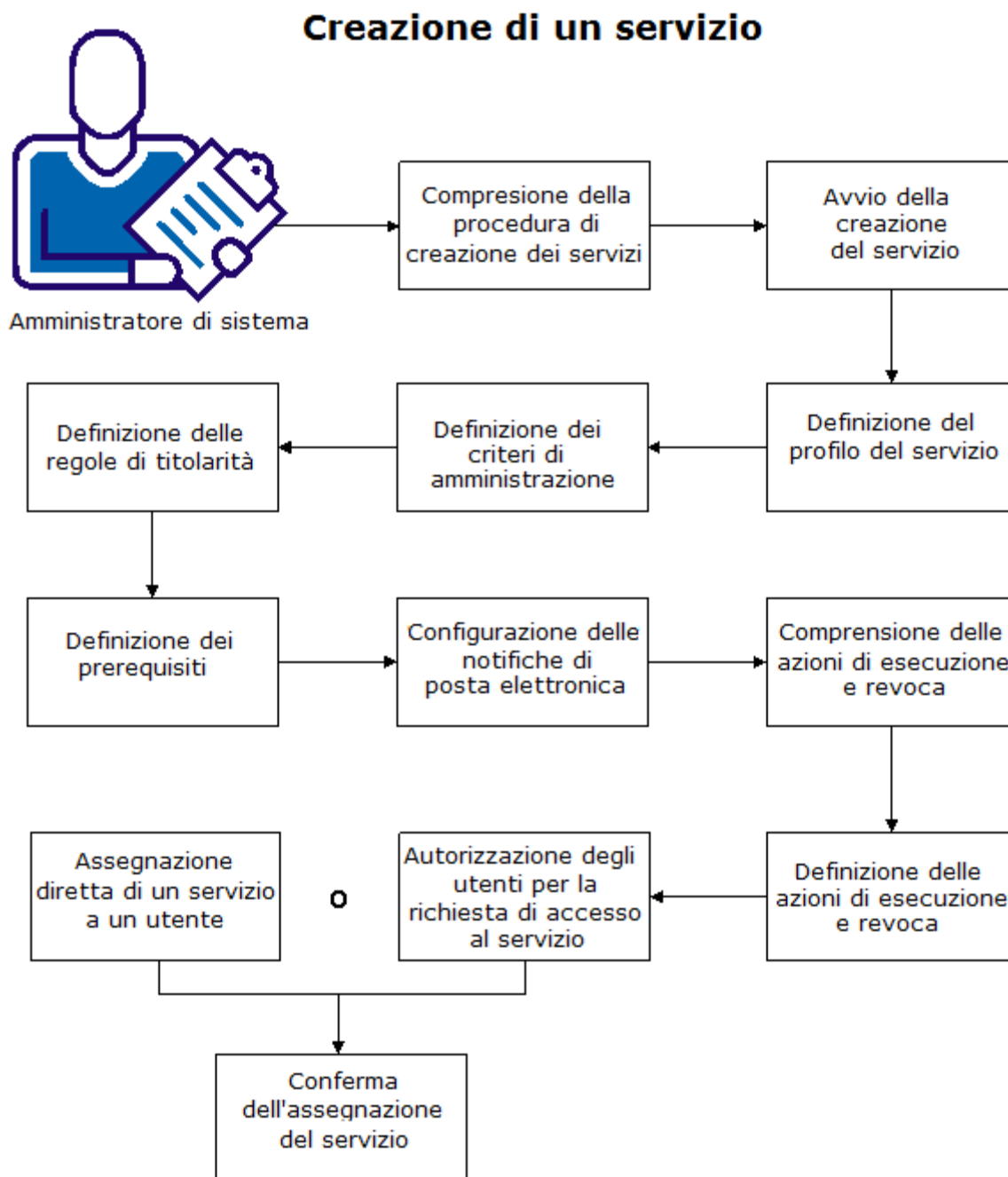
Creazione di un servizio

I servizi semplificano la gestione dei diritti. Un servizio raggruppa insieme tutti i diritti (attività, ruoli, gruppi e attributi) necessari a un utente per un dato ruolo aziendale. I servizi sono disponibili tramite le attività Richiesta di accesso nella console utente di CA CloudMinder. Le attività Richiesta di accesso consentono a un utente o amministratore di richiedere, assegnare, revocare e rinnovare un servizio.

I servizi consentono a un amministratore di associare i diritti dell'utente in un unico pacchetto, che vengono così gestiti come un insieme. Ad esempio, tutti i nuovi dipendenti del reparto Vendite devono accedere a un insieme definito di attività, account su determinati sistemi endpoint. Inoltre, devono aggiungere informazioni specifiche ai loro profili di account utente. Un amministratore crea un servizio denominato Amministrazione vendite, contenente ogni attività, ruolo, gruppo e informazioni di attributo del profilo richiesto per un nuovo dipendente del reparto Vendite. Quando un amministratore assegna il servizio Amministrazione vendite a un utente, costui riceve l'insieme intero di ruoli, attività, gruppi e attributi di account definiti dal servizio.

Un altro modo per gli utenti di accedere ai servizi consiste nel richiedere l'accesso da sé. Nella console utente, ciascun utente dispone di un elenco di servizi disponibili su richiesta. I servizi elencati sono stati contrassegnati dalla voce Sottoscrizione automatica, generalmente impostata da un amministratore con i privilegi appropriati in fase di creazione del servizio. Dall'elenco dei servizi disponibili gli utenti possono richiedere l'accesso ai servizi necessari. Quando l'utente richiede l'accesso a un servizio, la richiesta viene eseguita automaticamente e i diritti associati vengono assegnati immediatamente all'utente. Un amministratore con i privilegi adeguati può configurare, per l'esecuzione di un servizio, la necessità di approvare il flusso di lavoro o la generazione di notifiche di posta elettronica.

Nel diagramma seguente sono illustrate le informazioni utili e le fasi per la creazione di un servizio.



Nelle sezioni seguenti viene spiegata la procedura per creare un servizio e renderlo disponibile agli utenti:

1. [Introduzione alla creazione del servizio](#) (a pagina 230).
2. [Fasi iniziali nella creazione del servizio](#) (a pagina 231).
3. [Definizione del profilo di servizio](#) (a pagina 231).
4. [Definire i criteri di amministrazione per il servizio](#) (a pagina 233).
5. [Definizione delle regole di titolarità per il servizio](#) (a pagina 234).
6. [Definizione dei prerequisiti per il servizio](#) (a pagina 234).
7. [Configurare le notifiche di posta elettronica per il rinnovo del servizio.](#) (a pagina 235)
8. [Introduzione alle azioni di esecuzione e revoca](#) (a pagina 236).
9. [Definizione delle azioni di esecuzione e revoca per il servizio.](#) (a pagina 236)
10. Procedura per consentire agli utenti di richiedere l'accesso a servizi.
Nella console utente, facendo clic su Accesso personale, quindi su Richiedi e Visualizza accesso, viene visualizzato un elenco dei servizi che è possibile richiedere. I servizi riportati in elenco sono quelli contrassegnati dalla voce Sottoscrizione automatica, che in genere viene impostata dall'amministratore con i privilegi appropriati in fase di creazione del servizio.
11. [Assegnazione diretta di un servizio a un utente](#) (a pagina 87).
12. Conferma dell'assegnazione di servizio.

Introduzione alla creazione dei servizi

Prima di creare un servizio, considerare le informazioni relative ai prerequisiti e i diritti necessari per la creazione e l'esecuzione del servizio.

Considerare le domande seguenti:

1. A quale esigenza aziendale è rivolto il servizio? Ad esempio, è possibile creare un servizio che mette a disposizione un account su Salesforce.com a tutti i dipendenti nuovi.
2. I membri del servizio necessitano di ruoli di amministrazione? In tal caso, creare o identificare i ruoli di amministrazione richiesti.
3. I membri del servizio devono avere accesso a uno o più endpoint? In tal caso, creare o identificare gli endpoint richiesti.
4. Se i membri del servizio devono accedere a endpoint, creare o identificare i ruoli di provisioning associati e i modelli di account.

5. I membri del servizio devono essere membri di determinati gruppi? In tal caso, creare o identificare i gruppi richiesti.
6. È necessario fare riferimento o modificare determinati attributi utente quando un utente diventa membro del servizio? Ad esempio, quando un utente riceve il servizio Salesforce.com, è necessario confermare se l'attributo di dipartimento per quell'utente è impostato su Vendite? In tal caso, creare o identificare gli attributi utente richiesti.

Una volta creati o identificati i prerequisiti, è possibile [iniziare la creazione del servizio](#) (a pagina 231).

Fasi iniziali nella creazione del servizio

Un servizio viene creato dalla console utente.

Procedere come descritto di seguito:

1. Accedere a un account con privilegi di gestione del servizio.
Ad esempio, il primo utente di un ambiente è associato al ruolo Manager di sistema, che dispone dell'attività Crea servizio.
2. Dal menu di navigazione, selezionare Servizi. L'opzione potrebbe essere contenuta in Attività.
3. Fare clic su Gestione servizi, Crea servizio.
4. Definire il profilo di servizio.

Definizione del profilo del servizio

Nella scheda Profilo è possibile definire le caratteristiche di base del servizio.

Procedere come descritto di seguito:

1. Immettere un nome e un tag. Un tag è un identificatore univoco del servizio.
Nota: i tag possono contenere solo caratteri alfanumerici e di sottolineatura e non possono iniziare con un numero. Una volta creato, non è possibile modificare o riutilizzare un nome tag, anche se in seguito il servizio viene eliminato.
2. Selezionare Attivato per rendere disponibile il servizio subito dopo la creazione.
3. Selezionare Sottoscrizione automatica se si desidera visualizzare il servizio nell'elenco dei servizi disponibili su richiesta. Quando l'opzione Sottoscrizione automatica è abilitata, gli utenti possono richiedere l'accesso al servizio tramite la console utente.

4. (Facoltativo) Aggiungere una o più categorie. Immettere il nome della categoria e fare clic sulla freccia Su per aggiungerlo al servizio.

Le categorie offrono informazioni aggiuntive a un servizio. Tali informazioni aggiuntive sono utili per facilitare le ricerche di servizi in ambienti che presentano un numero elevato di servizi.

5. Specificare l'opzione Schermata dati utente per l'esecuzione del servizio se si desidera raccogliere altri dati utente quando viene richiesto il servizio.

Utilizzare la schermata dati utente per l'esecuzione del servizio per assicurarsi che sul sistema siano presenti tutti i dati utente necessari all'esecuzione del servizio. Ad esempio, è necessario un indirizzo di posta elettronica valido per eseguire un servizio che crea un account in Google Apps. Se nell'archivio utenti di CA CloudMinder non esiste l'indirizzo di posta elettronica di un utente, è necessario fornirlo alla richiesta del servizio.

- a. Fare clic su Sfoglia.

Viene visualizzato un elenco delle schermate di profilo disponibili. Queste schermate vengono generalmente utilizzate per raccogliere i dati dell'utente.

- b. Selezionare una schermata di profilo contenente i dati utente che si desidera raccogliere. Selezionare una delle seguenti opzioni:

- Fare clic su Seleziona per raccogliere tutti i dati utente contenuti in quella schermata.

O

- Fare clic su Copia per personalizzare i dati utente che si desidera raccogliere. Specificare un nome e un tag univoco per la nuova schermata. Aggiungere, modificare o rimuovere elementi di dati utente e fare clic su OK.

O

- Fare clic su Modifica per cambiare i dati utente contenuti in quella schermata. Aggiungere, modificare o rimuovere elementi di dati utente e fare clic su OK.

Importante. Se si modifica una schermata dati utente, le modifiche si applicano in qualsiasi ambito di utilizzo della schermata nella console utente. Valutare piuttosto la procedura di copia e personalizzazione della schermata di profilo.

- c. Fare clic su Seleziona.

Gli elementi di dati utente selezionati vengono raccolti alla richiesta del servizio.

Nota: se i dati necessari sono già presenti nel sistema quando un utente richiede il servizio, i dati vengono prepopolati nella schermata di profilo.

6. [Definire i criteri di amministrazione per il servizio](#) (a pagina 233).

Definizione dei criteri di amministrazione per il servizio

Nella scheda Amministratori viene definito chi può aggiungere o rimuovere utenti come membri e amministratori del servizio. I criteri di amministrazione contengono regole di ambito e amministrazione e almeno un privilegio di amministratore (Gestione membri o Gestione amministratori).

Le regole di amministrazione definiscono chi può amministrare il servizio. Le regole di ambito limitano quali utenti possono diventare amministratori. Ad esempio, una regola di amministrazione può consentire a tutti i membri del gruppo Vendite di amministrare un servizio. Una regola di ambito può limitare l'amministrazione solo ai membri del gruppo Vendite di Boston, MA.

Procedere come descritto di seguito:

1. Nella scheda Amministratori, fare clic su Aggiungi.
Viene visualizzata la schermata Criterio di amministrazione.
2. Definire una regola di amministrazione per cui gli utenti possono amministrare il servizio. Ad esempio, è possibile specificare utenti membri del gruppo Vendite o con l'attributo di profilo per la professione Responsabile delle vendite.
Fare clic sulla freccia sinistra per modificare una parte specificata in precedenza di una regola.
3. Definire una regola di ambito per limitare quali utenti possono amministrare il servizio. Ad esempio, se nella regola di amministrazione sono stati indicati gli utenti membri del gruppo Vendite, è possibile limitare l'ambito di quella regola solo agli utenti la cui città è Boston, MA.
Nota: è possibile aggiungere molti criteri di amministrazione con regole e privilegi differenti per ciascun servizio.
4. Se si desidera consentire agli amministratori di aggiungere o rimuovere membri del servizio, fare clic su "È possibile gestire membri di questo servizio".
5. Fare clic su OK.
6. Per ulteriori modifiche al criterio, fare clic sull'icona Modifica. Per rimuovere un criterio, fare clic sull'icona con il segno meno.
7. [Definire le regole di titolarità per il servizio.](#) (a pagina 234)

Definizione delle regole di titolarità per il servizio

Nella scheda Titolari si definiscono le regole riguardanti chi può essere titolare del servizio. Un titolare è un utente che può modificare il servizio.

Procedere come descritto di seguito:

1. Nella scheda Titolari, fare clic su **Aggiungi**.
Viene visualizzata la schermata Regola di titolarità.
2. Definire una regola di titolarità per cui gli utenti possono essere titolari del servizio. Ad esempio, è possibile specificare utenti membri del gruppo Vendite o con l'attributo di profilo per la professione Responsabile delle vendite.
Fare clic sulla freccia sinistra per modificare una parte specificata in precedenza di una regola.
3. Fare clic su **OK**.
4. [Definire i prerequisiti per il servizio](#). (a pagina 234)

Definizione dei prerequisiti per il servizio

Nella scheda Prerequisiti si definiscono i servizi che gli utenti devono possedere prima di richiedere un altro servizio. Un servizio è riportato nell'elenco dei servizi disponibili per un dato utente solo se quest'ultimo è membro di tutti i servizi necessari come prerequisiti.

Se viene impostata una durata per un servizio che rientra nei prerequisiti, quella durata si applica al servizio in corso di definizione. Ad esempio, il Servizio A è un prerequisito per il Servizio B. Il Servizio A dura una settimana. Anche il Servizio B scade in una settimana.

Procedere come descritto di seguito:

1. Nella scheda Prerequisiti, fare clic su **Add Service** (Aggiungi servizio).
Viene visualizzata una schermata di ricerca.
2. Cercare un servizio che si desidera scegliere come prerequisito per il servizio.
Per visualizzare un elenco di tutti i servizi per i quali si dispone di privilegi amministrativi, fare clic su **Cerca** senza modificare i criteri di ricerca.
3. Selezionare un servizio e fare clic su **Seleziona**.
Viene visualizzato un elenco aggiornato dei prerequisiti per il servizio.

Configurazione delle notifiche di posta elettronica per il rinnovo del servizio

Alcuni servizi scadono dopo un certo periodo.

Nella scheda Posta elettronica è possibile configurare una notifica di posta elettronica in modo da ricordare ai membri del servizio di rinnovare l'appartenenza prima della scadenza. I membri possono così utilizzare l'attività Rinnova servizio per rinnovare l'accesso.

CA CloudMinder fornisce un modello di messaggio di posta elettronica predefinito con contenuti dinamici. Questi contenuti sono popolati automaticamente all'invio del messaggio di posta elettronica. I contenuti dinamici, racchiusi tra parentesi graffe ({ }) nell'editor della notifica di posta elettronica, consentono di aggiungere al messaggio di posta elettronica il nome utente, il nome del servizio e la data di scadenza.

Nell'editor è possibile modificare il contenuto della notifica di posta elettronica. Ad esempio, è possibile modificare il corpo del messaggio o il testo dell'oggetto, il carattere oppure rimuovere i contenuti dinamici.

Fare attenzione agli elementi seguenti durante la configurazione delle notifiche di posta elettronica:

- Se si includono contenuti dinamici nella notifica di posta elettronica, non modificare il testo tra le parentesi graffe ({ }).
- Se il servizio comprende un prerequisito che scade, le notifiche di posta elettronica vengono inviate solo per il prerequisito, anche quando le notifiche di posta elettronica sono configurate per entrambi i servizi.

Procedere come descritto di seguito:

1. Nella scheda Posta elettronica, selezionare la casella di controllo Notifica di posta elettronica da inviare agli utenti prima della scadenza del servizio per abilitare le notifiche.
2. (Facoltativo) Personalizzare la notifica di posta elettronica con i comandi dell'editor.
L'editor della notifica di posta elettronica supporta l'HTML. È possibile aggiungere contenuti in HTML al testo della notifica di posta elettronica facendo clic sul pulsante Toggle HTML Source (<>) nella barra degli strumenti.
3. [Comprensione delle azioni di esecuzione e revoca](#). (a pagina 236)

Comprensione delle azioni di esecuzione e revoca

Nella scheda Azioni si definiscono i diritti e le informazioni (attività, ruoli, gruppi e attributi) da aggiungere, modificare o rimuovere quando un servizio viene assegnato o revocato. In altre parole, le azioni di un servizio definiscono le azioni svolte dal servizio.

CA CloudMinder utilizza un criterio di Policy Xpress per definire le circostanze in cui si verificano le azioni di esecuzione e revoca. CA CloudMinder preconfigura questo criterio in modo che quando un utente richiede un servizio, esistano le condizioni e i dati esatti. Il servizio viene eseguito o revocato automaticamente.

Un amministratore deve definire le azioni che il sistema compie durante l'esecuzione o la revoca di un servizio. Ad esempio, durante la creazione di un servizio, un amministratore può specificare che i membri del servizio ricevano il ruolo di amministrazione Responsabile delle vendite, il ruolo di provisioning di Salesforce.com e il gruppo Vendite. Allo stesso modo, l'amministratore può specificare che questi diritti siano rimossi alla revoca del servizio.

Definizione delle azioni di esecuzione e revoca per il servizio

Nella scheda Azioni è possibile definire i diritti e le informazioni aggiungete, modificate o rimosse dal sistema nel caso in cui un servizio venga assegnato o rimosso da un utente.

Procedere come descritto di seguito:

1. Fare clic sulla scheda Azioni.

Viene visualizzata la schermata per le azioni di esecuzione e revoca.

2. Fare clic sul pulsante Gestisci azioni di esecuzione o Gestisci azioni di revoca.

Viene visualizzata la schermata Crea criterio Policy Xpress.

I campi seguenti sono predefiniti per creare una regola di azione:

Nome

Consente di specificare un nome descrittivo per la regola di azione. Il nome deve essere univoco.

Descrizione

Consente di specificare il significato della regola di azione.

Priorità

Consente di specificare la regola di azione eseguita, nel caso in cui esista una corrispondenza per più regole di azione. Questo campo risulta utile per definire le azioni predefinite. Se ad esempio si dispone di più regole, ognuna per uno specifico nome di dipartimento, è possibile impostare un'azione predefinita aggiungendo un'ulteriore regola senza condizioni, ma con priorità più bassa (ad esempio 10 se tutte le altre hanno priorità 5). Se non esiste una corrispondenza per nessuna delle regole del dipartimento, viene utilizzata l'azione predefinita.

3. In Condizioni regola di azione, specificare i criteri da allineare.
4. Fare clic sul pulsante Aggiungi azione quando esiste una corrispondenza in Aggiungi azioni

Viene visualizzata la schermata Aggiungi azione quando esiste una corrispondenza. In questa schermata si definiscono le azioni che il sistema esegue quando viene trovata una corrispondenza per la regola.

5. Immettere un nome descrittivo che definisce lo scopo dell'azione.

Ad esempio, immettere Aggiungi il ruolo di amministrazione Responsabile delle vendite.

6. Selezionare la categoria di azione da far svolgere al sistema.

Ad esempio, per aggiungere un ruolo, selezionare la categoria Ruoli.

7. Selezionare il tipo di azione da far svolgere al sistema.

Ad esempio, per aggiungere o rimuovere un ruolo di amministrazione, selezionare il tipo Imposta ruolo di amministrazione.

8. Selezionare la funzione da far svolgere al sistema.

Ad esempio, per aggiungere un ruolo di amministrazione, selezionare la funzionalità Aggiungi.

Nota: quando si seleziona una funzionalità, viene visualizzata la descrizione. Questa descrizione può servire per determinare se la funzionalità selezionata produce il comportamento desiderato del sistema.

9. Definire l'azione specifica da far svolgere al sistema.

Ad esempio, per aggiungere un ruolo di amministrazione denominato Responsabile delle vendite, immettere il nome del ruolo o fare clic sul pulsante Sfoglia e selezionare Responsabile delle vendite dall'elenco dei ruoli di amministrazione disponibili.

10. Fare clic su OK.

Ripetere questa procedura finché sono state aggiunte tutte le azioni desiderate per questo servizio.

11. Fare clic su OK.

Il sistema associa le azioni di esecuzione e revoca definite con il servizio. Quando un utente riceve il servizio, vengono aggiunti, modificati o rimossi le informazioni e i diritti associati.

12. A questo punto è possibile [assegnare un servizio a un utente](#) (a pagina 87).

Assegnazione diretta di un servizio a un utente

È possibile assegnare un servizio direttamente a un singolo utente. L'utente diviene *membro* del servizio.

Procedere come descritto di seguito:

1. Accedere a Servizi, Richiedi e Visualizza accesso.

Viene visualizzato un elenco dei servizi che è possibile amministrare.

2. Selezionare il servizio che si desidera assegnare all'utente e fare clic su Seleziona.

Viene visualizzato un elenco di utenti assegnati al servizio.

3. Fare clic su Richiedi accesso.

4. Cercare un utente cui si desidera assegnare il servizio.

Per visualizzare un elenco di tutti gli utenti per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.

5. Selezionare un utente e fare clic su Seleziona.

Viene visualizzato un elenco aggiornato degli utenti cui è assegnato il servizio.

6. Fare clic su Salva modifiche.

L'utente riceve il servizio specificato. L'utente riceve quindi tutte le applicazioni, ruoli, gruppi e attributi inclusi nel servizio.

Conferma dell'assegnazione del servizio

Una volta assegnato un servizio a un utente, confermare il corretto completamento di tutte le attività associate al servizio.

Procedere come descritto di seguito:

1. Accedere a Servizi, Visualizza cronologia richieste di accesso servizio.
Viene visualizzata una schermata di ricerca.
2. Cercare il servizio assegnato a un utente.
Per visualizzare un elenco di tutti i servizi per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.
Viene visualizzato un elenco dei servizi che è possibile amministrare.
3. Selezionare il servizio assegnato e fare clic su Seleziona.
Viene visualizzata la cronologia delle azioni associate al servizio.
4. Fare clic su Ultima modifica per visualizzare prima le azioni più recenti.
5. Confermare che l'utente in questione ha ricevuto correttamente il servizio.
6. Fare clic su Chiudi.

Procedura per rendere i servizi disponibili agli utenti

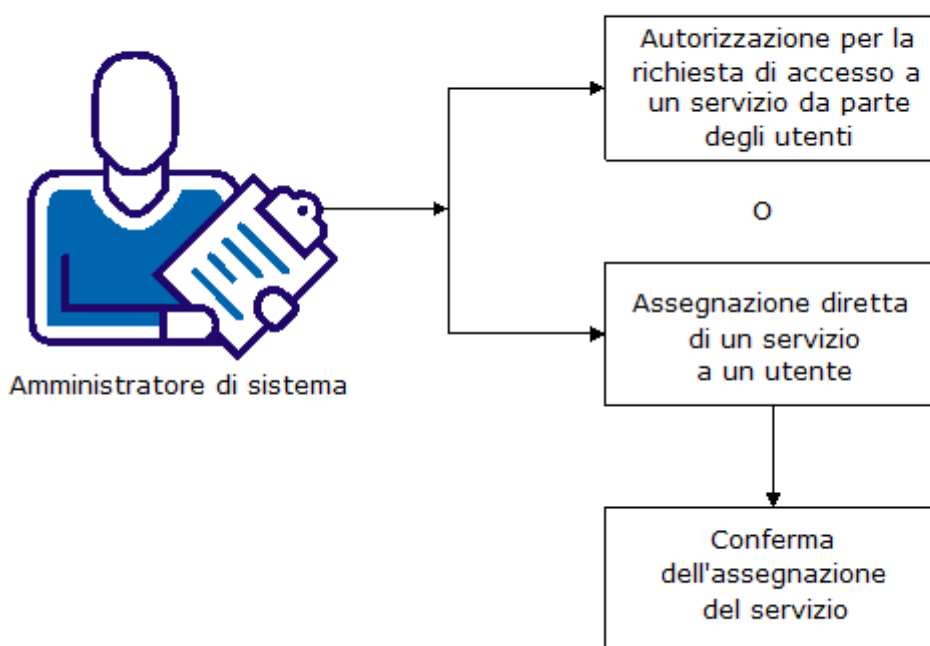
I servizi semplificano la gestione dei diritti. Un servizio raggruppa tutti i diritti necessari a utente per un dato ruolo aziendale. I servizi sono disponibili tramite le attività Richiesta di accesso nella console utente. Le attività Richiesta di accesso consentono a un utente o amministratore di richiedere, assegnare, revocare e rinnovare un servizio attraverso l'interfaccia utente.

I servizi consentono a un amministratore di sistema di associare le attività e le informazioni utente (attività, ruoli, gruppi e attributi) in un pacchetto singolo, gestito come un insieme. Ad esempio, tutti i nuovi dipendenti del reparto vendite devono accedere a un insieme definito di attività, account su determinati sistemi endpoint e informazioni specifiche aggiunte ai loro profili di account utente. Un amministratore di sistema crea un servizio denominato "Amministrazione vendite", contenente ogni attività, ruolo, gruppo e informazioni di attributo del profilo richiesto per un nuovo dipendente del reparto vendite. Quando un amministratore assegna il servizio Amministrazione vendite a un utente, costui riceve l'insieme intero di ruoli, attività, gruppi e attributi di account definiti dal servizio.

Un altro modo per gli utenti di accedere ai servizi consiste nel richiedere l'accesso da sé. Nella console utente, ciascun utente dispone di un elenco di servizi disponibili su richiesta. I servizi elencati sono stati contrassegnati dalla voce Sottoscrizione automatica, generalmente impostata dall'amministratore di sistema con i privilegi appropriati in fase di creazione del servizio. Dall'elenco dei servizi disponibili gli utenti possono richiedere l'accesso ai servizi necessari. Quando l'utente richiede l'accesso a un servizio, la richiesta viene eseguita automaticamente. Le attività, i ruoli, i gruppi e gli attributi associati vengono assegnati immediatamente all'utente. Un amministratore di CA CloudMinder con i privilegi adeguati può configurare, per l'esecuzione di un servizio, la necessità di approvare il flusso di lavoro o la generazione di notifiche di posta elettronica.

Il diagramma seguente illustra le informazioni utili e i passaggi da seguire per rendere i servizi disponibili agli utenti.

Procedura per rendere i servizi disponibili agli utenti



È possibile rendere i servizi disponibili agli utenti con i metodi seguenti:

1. Consentire agli utenti di richiedere l'accesso da sé.

Nella console utente di CA CloudMinder, facendo clic su Accesso personale, quindi su Richiedi e Visualizza accesso, viene visualizzato un elenco dei servizi disponibili su richiesta. I servizi riportati in elenco sono quelli contrassegnati dalla voce Sottoscrizione automatica, che in genere viene impostata dall'amministratore di CA CloudMinder con i privilegi appropriati in fase di creazione del servizio.

Quando un utente richiede l'accesso, il sistema assegna il servizio all'utente. L'utente riceve quindi tutte le applicazioni, ruoli, gruppi e attributi associati al servizio. Se il servizio include un ruolo di avvio per un'applicazione, nella pagina principale della console utente viene visualizzata un'icona e un collegamento a tale applicazione.

2. [Assegnazione diretta di un servizio a un utente](#) (a pagina 87).
3. Se si assegna un servizio direttamente a un utente, [confermare l'assegnazione del servizio](#) (a pagina 242).

Assegnazione diretta di un servizio a un utente

È possibile assegnare un servizio direttamente a un singolo utente. L'utente diviene *membro* del servizio.

Procedere come descritto di seguito:

1. Accedere a Servizi, Richiedi e Visualizza accesso.
Viene visualizzato un elenco dei servizi che è possibile amministrare.
2. Selezionare il servizio che si desidera assegnare all'utente e fare clic su Seleziona.
Viene visualizzato un elenco di utenti assegnati al servizio.
3. Fare clic su Richiedi accesso.
4. Cercare un utente cui si desidera assegnare il servizio.
Per visualizzare un elenco di tutti gli utenti per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.
5. Selezionare un utente e fare clic su Seleziona.
Viene visualizzato un elenco aggiornato degli utenti cui è assegnato il servizio.
6. Fare clic su Salva modifiche.
L'utente riceve il servizio specificato. L'utente riceve quindi tutte le applicazioni, ruoli, gruppi e attributi inclusi nel servizio.

Conferma dell'assegnazione del servizio

Una volta assegnato un servizio a un utente, confermare il corretto completamento di tutte le attività associate al servizio.

Procedere come descritto di seguito:

1. Accedere a Servizi, Visualizza cronologia richieste di accesso servizio.
Viene visualizzata una schermata di ricerca.
2. Cercare il servizio assegnato a un utente.
Per visualizzare un elenco di tutti i servizi per i quali si dispone di privilegi amministrativi, fare clic su Cerca senza modificare i criteri di ricerca.
Viene visualizzato un elenco dei servizi che è possibile amministrare.
3. Selezionare il servizio assegnato e fare clic su Seleziona.
Viene visualizzata la cronologia delle azioni associate al servizio.
4. Fare clic su Ultima modifica per visualizzare prima le azioni più recenti.
5. Confermare che l'utente in questione ha ricevuto correttamente il servizio.
6. Fare clic su Chiudi.

Modifica di un servizio

L'amministratore di sistema può modificare un servizio creato in precedenza. Ad esempio, può modificare i diritti concessi ai membri del servizio con l'aggiunta di un ruolo al servizio. È possibile modificare anche le regole di amministrazione e titolarità per il servizio, i prerequisiti di servizio e altri dettagli amministrativi.

Se CA CloudMinder ha eseguito un servizio per un dato utente, qualsiasi modifica apportata al servizio non si propaga all'utente. Se si decide di modificare un servizio, gli utenti che hanno ricevuto il servizio prima delle modifiche conservano i diritti originali. Gli utenti che ricevono il servizio dopo le modifiche hanno i diritti concessi dal servizio modificato. Ad esempio, considerare lo scenario seguente:

Un amministratore di sistema può creare un servizio di Responsabile vendite che assegna il ruolo Responsabile vendite e il gruppo Vendite ai membri del servizio. Gli utenti richiedono il servizio Responsabile vendite e CA CloudMinder adempie al servizio concedendo il ruolo e il gruppo appropriati agli utenti. È possibile decidere di modificare il servizio Responsabile vendite in modo che includa il ruolo di responsabile dei dipendenti. I membri esistenti del servizio non ricevono quindi il ruolo di responsabile dei dipendenti. Solo i nuovi membri del servizio Responsabile vendite ricevono il ruolo di responsabile dei dipendenti, oltre al ruolo di Responsabile vendite e al gruppo Vendite.

Per questo motivo si consiglia di modificare un servizio solo se questo non ha alcun membro. Cioè, modificare un servizio solamente se nessun utente ha richiesto e ricevuto il servizio e nessun amministratore ha assegnato il servizio a un utente.

È possibile modificare le informazioni amministrative, le regole di amministratori e titolari, i prerequisiti del servizio e i diritti (attività, ruoli, gruppi e attributi) per il servizio.

Procedere come descritto di seguito:

1. Accedere a un account CA CloudMinder dotato di privilegi di gestione del servizio.
Ad esempio, il primo utente di un ambiente è associato al ruolo di manager di sistema, che dispone dell'attività Modifica servizio.
2. Dal menu di navigazione, selezionare Attività, Servizi.
3. Fare clic su Gestione servizi, quindi Modifica servizio.
Viene visualizzata una schermata di ricerca.
4. Cercare il servizio che si desidera modificare.
Per visualizzare un elenco di tutti i servizi per cui si dispongono i privilegi di amministrazione, fare clic su Cerca, senza modificare i criteri di ricerca.
5. Selezionare un servizio e fare clic su Seleziona.
Viene visualizzato un messaggio di conferma.
6. Fare clic su Sì.
7. Fare clic su Inoltra.
CA CloudMinder applica le modifiche al servizio.

Aggiunta di una ricerca all'accesso e visualizzazione dell'accesso

L'attività Richiedi e visualizza accesso mostra un elenco di servizi. Tenere tuttavia presente che non esistono campi per la ricerca di più servizi. Per aggiungere un campo di ricerca:

1. Fare clic su Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
2. Cercare l'attività Richiedi e visualizza accesso.
3. Selezionare l'attività nella categoria Servizio.
4. Fare clic su Schede.
5. Nella scheda, fare clic sull'icona di modifica situata a sinistra dell'opzione Gestione accesso.
6. Fare clic su Sfoglia della riga Schermata elenco.
7. Configurare l'opzione applicabile per aggiungere la ricerca appropriata.
8. Selezionare la schermata desiderata, quindi fare clic sul pulsante Modifica per modificare la schermata.
9. In Configure Standard List Screen (Configurare schermata di elenco standard), accedere alla sezione Selezione dei campi di ricerca da parte dell'utente.
10. Selezionare i campi di ricerca e configurare i nomi corrispondenti.
11. Fare clic su OK per salvare le modifiche.

Le informazioni sulle richieste di servizio, come ad esempio la durata della richiesta di servizio e i dati utente vengono visualizzate nell'elemento del flusso di lavoro di approvazione della richiesta di servizio. Queste informazioni vengono inoltre inviate via posta elettronica se il flusso di lavoro basato sul criterio AddServiceToUserEvent viene assegnato all'attività Richiedi e visualizza accesso.

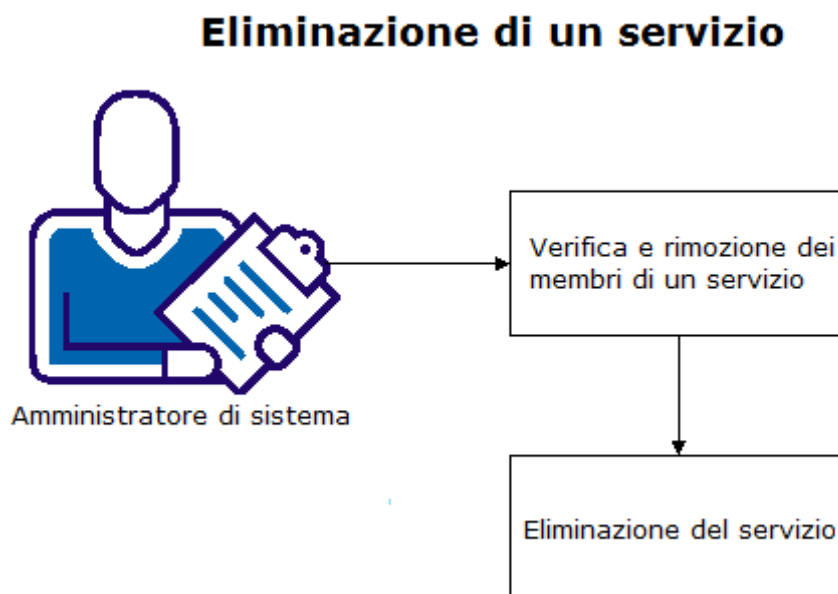
Eliminazione di un servizio

Un amministratore di sistema può eliminare un servizio. Un servizio eliminato viene rimosso completamente dal sistema.

Se gli utenti vengono assegnati a un servizio, non è possibile eliminarlo. Prima di eliminare un servizio, controllare e rimuovere tutti gli utenti o i *membri* assegnati.

Nota: allo stesso modo, se un utente è membro di un servizio, non è possibile eliminarlo. Prima di tutto, rimuovere l'utente come membro del servizio, quindi eliminare l'utente.

L'immagine seguente mostra le informazioni necessarie e i passaggi da eseguire per eliminare un servizio.



I seguenti argomenti spiegano come eliminare un servizio:

1. [Verifica e rimozione dei membri di un servizio](#) (a pagina 246)
2. [Eliminazione del servizio](#) (a pagina 246)

Verifica e rimozione dei membri di un servizio

Prima di eliminare un servizio, controllare e rimuovere gli eventuali membri esistenti.

Procedere come descritto di seguito:

1. Accedere a un account CA CloudMinder dotato di privilegi di gestione del servizio.
Ad esempio, il primo utente di un ambiente è associato al ruolo di manager di sistema, che dispone dell'attività Modifica servizio.
2. Selezionare Attività, Servizi, Richiedi e visualizza accesso.
Viene visualizzato un elenco dei servizi che è possibile amministrare.
3. Selezionare il servizio che si desidera eliminare, quindi fare clic su Seleziona.
Viene visualizzato un elenco di utenti assegnati al servizio.
4. Se sono presenti membri collegati al servizio, deselezionare le caselle di controllo accanto a tutti gli utenti.
5. Fare clic su Salva modifiche.
Viene visualizzato un messaggio di conferma.
6. Fare clic su Sì.
CA CloudMinder rimuove i membri dal servizio.

Eliminazione di un servizio

È possibile eliminare un servizio privo di membri del servizio.

Per eliminare un servizio

1. Accedere a CA CloudMinder con un account dotato di privilegi di gestione del servizio.
Ad esempio, il primo utente di un ambiente è associato al ruolo Manager di sistema, che dispone dell'attività Elimina servizio.
2. Accedere a Servizi dal riquadro sinistro oppure selezionare le attività.
3. Fare clic su Gestione servizi, Elimina servizio.
Viene visualizzata una schermata di ricerca.
4. Individuare il servizio da eliminare.
Per visualizzare un elenco di tutti i servizi per cui si dispongono i privilegi di amministrazione, fare clic su Cerca, senza modificare i criteri di ricerca.
5. Selezionare il servizio e fare clic su Seleziona.
Viene visualizzato un messaggio di conferma.

6. Fare clic su Sì.

Il servizio viene eliminato.

Rinnovo dell'accesso a un servizio

Alcuni servizi scadono dopo un certo periodo di tempo. Gli amministratori possono rinnovare un servizio per gli utenti, per prevenire un'interruzione dell'accesso.

Per rinnovare un servizio utilizzare uno dei metodi seguenti:

- Selezionare il servizio, quindi selezionare l'accesso utente da rinnovare.
- Selezionare l'utente, quindi selezionare il servizio da rinnovare

Nota: a seconda del modo in cui un ambiente viene configurato, gli utenti finali possono rinnovare il proprio accesso anche mediante l'attività Rinnova accesso.

La procedura seguente descrive come rinnovare l'accesso selezionando prima il servizio. Se si desidera selezionare per prima cosa l'utente, utilizzare l'attività Richieste di accesso dell'utente, Gestisci richieste di rinnovo dell'utente nella categoria Utenti.

Procedere come descritto di seguito:

1. Fare clic su Servizi, Rinnova accesso nella Console utente.
2. Cercare e selezionare il servizio che si desidera rinnovare.

La console utente visualizza un elenco di utenti che attualmente hanno accesso al servizio selezionato e la data di scadenza di tale accesso.

3. Selezionare la durata del periodo di rinnovo nella colonna Richiesta di accesso, quindi fare clic su OK.

Le opzioni nel campo Durata vengono stabilite quando il servizio viene creato.

4. Fare clic su Salva modifiche.

È possibile visualizzare lo stato del rinnovo del servizio mediante Visualizza cronologia richieste di accesso servizio nella console utente.

Capitolo 10: Sincronizzazione

Questa sezione contiene i seguenti argomenti:

[Sincronizzazione utente tra server](#) (a pagina 249)

[Sincronizzare gli utenti nelle attività di creazione o modifica utente](#) (a pagina 252)

[Attività di sincronizzazione](#) (a pagina 253)

Sincronizzazione utente tra server

Si configura la sincronizzazione in Identity Manager per assicurare che i dati degli utenti della directory aziendale e della directory di provisioning corrispondano. Per gestire le modifiche da entrambe le directory, è necessario configurare la sincronizzazione in entrata e in uscita.

Sincronizzazione in entrata

La *sincronizzazione in entrata* mantiene gli utenti di CA Identity Manager aggiornati rispetto alle modifiche effettuate nella directory di provisioning. Le modifiche apportate alla directory di provisioning includono quelle effettuate mediante sistemi con connettori al server di provisioning. La sincronizzazione utilizza i mapping definiti nella schermata di provisioning della console di gestione.

Failover della sincronizzazione in entrata

Si verifica un failover su un URL del server di Identity Manager alternativo solo se il server applicazioni denominato dall'URL non è in esecuzione. Se il server applicazioni è in esecuzione e accetta la notifica ma in seguito si verifica un errore di configurazione, come ad esempio un errore di ambiente sconosciuto o ambiente non avviato, tali errori bloccano la consegna delle notifiche. È necessario risolvere questi problemi perché le notifiche in entrata funzionino correttamente.

Sincronizzazione in uscita

La *sincronizzazione in uscita* implica l'utilizzo di Identity Manager per la creazione e l'aggiornamento degli utenti nella directory di provisioning.

Creare utenti globali da Identity Manager

La creazione di un utente nella directory di provisioning si verifica solo per gli eventi relativi al provisioning, come ad esempio l'assegnazione di un ruolo di provisioning a un utente. Se si utilizza un'attività di amministrazione per creare un utente, nella directory di provisioning non viene creato nessun utente, a meno che tale attività non assegni un ruolo o includa un criterio di identità che assegna il ruolo.

Quando la creazione di un utente in Identity Manager attiva la creazione utente nella directory di provisioning, Identity Manager invia un messaggio di posta elettronica con una password temporanea all'indirizzo e-mail del nuovo utente definito nella directory di provisioning. L'utente può accedere alla console utente con questa password, ma verrà richiesto di crearne una nuova. Di conseguenza, la password viene sincronizzata tra l'archivio utenti e la directory di provisioning.

Se l'utente non dispone di un indirizzo e-mail, non può accedere alla console utente fino a che non cambia la password dell'archivio utenti o finché un amministratore di CA Identity Manager non modifica la password dell'utente in Manager di provisioning.

Nota: per inviare una password temporanea via e-mail, è necessario abilitare le notifiche di posta elettronica per l'ambiente e configurare `CreateProvisioningUserNotificationEvent` per tali notifiche. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Aggiornare gli utenti globali mediante Identity Manager

Gli aggiornamenti degli utenti nella directory di provisioning si verificano quando si utilizza un'attività di amministrazione che modifica gli utenti. Se non esistono utenti globali, non si verifica alcuna sincronizzazione.

I mapping in uscita allineano gli eventi utente di Identity Manager a un evento in uscita che influisce sulla directory di provisioning.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

Se un utente esiste nella directory di provisioning ma non in Identity Manager, è possibile creare l'utente nella console utente. È stato eseguito il mapping degli attributi per l'attività di creazione e gli utenti hanno lo stesso ID utente, gli attributi dell'utente di provisioning vengono aggiornati nella directory di provisioning. A questo punto è possibile gestire l'utente da Identity Manager.

Nota: se un evento aggiorna gli attributi utente e si desidera che i valori vengano sincronizzati in CA Identity Manager, è necessario eseguire il mapping degli eventi all'evento in uscita: POST_MODIFY_GLOBAL_USER.

Eliminare gli utenti globali mediante Identity Manager

Per impostazione predefinita, la sincronizzazione in uscita viene configurata per l'evento Elimina utente. Quando si elimina un utente in Identity Manager, questo viene eliminato anche nella directory di provisioning e in tutti gli account di endpoint.

Se CA Identity Manager non è in grado di eliminare un account utente in un endpoint gestito, elimina l'utente dagli account restanti, ma non lo elimina dalla directory di provisioning.

Ad esempio, l'utente A dispone di un account UNIX e di un account Exchange, che vengono gestiti nel server di provisioning. Quando l'utente A viene eliminato in Identity Manager, il server di provisioning tenta di eliminare gli account dell'utente. Se il server di provisioning non riesce a eliminare l'account Exchange a causa di un errore di comunicazione, elimina l'account UNIX dell'utente A, ma non elimina l'utente dalla directory di provisioning. Tuttavia, l'utente A non viene ripristinato nell'archivio utenti.

Abilitare la sincronizzazione di password

Il server di provisioning consente la sincronizzazione di password tra utenti di Identity Manager e gli account utente degli endpoint associati. Per abilitare le modifiche iniziate dagli endpoint, sono necessarie due configurazioni:

- È necessario configurare gli endpoint per l'acquisizione delle modifiche iniziate dagli endpoint e per il loro inoltro al server di provisioning.

Nota: per ulteriori informazioni sulla configurazione degli endpoint per la sincronizzazione della password, consultare la *Guida per l'amministratore di CA Identity Manager*.

- L'attributo Enable Password Synchronization Agent (Attiva agente sincronizzazione password) deve essere attivato per l'utente globale.

Per abilitare la sincronizzazione di password

1. Nella console di gestione, Selezionare Impostazioni avanzate, Provisioning.
2. Selezionare Enable Password Changes (Abilita modifiche password) da Endpoint Accounts (Account endpoint).
3. Fare clic su Save (Salva).
4. Riavviare il server applicazioni.

Sincronizzare gli utenti nelle attività di creazione o modifica utente

Nella scheda di profilo di un'attività che crea o modifica utenti, i controlli di sincronizzazione assicurano che le modifiche apportate a Identity Manager vengano applicate anche all'utente globale. Se si creano attività di amministrazione che creano o modificano utenti e si dispone dei criteri di identità, impostare i controlli di sincronizzazione nel modo seguente:

- Impostare Sincronizzazione utente su Al completamento dell'attività.
- Impostare Sincronizzazione account su Al completamento dell'attività.

Nota: per ottimizzare le prestazioni, selezionare l'opzione Al completamento dell'attività. Tuttavia, se si seleziona l'opzione Al completamento dell'attività per un'attività che include più eventi, Identity Manager non esegue la sincronizzazione finché tutti gli eventi nell'attività non sono stati completati. Se uno o più di tali eventi richiedono l'approvazione del flusso di lavoro, tale processo potrebbe impiegare diversi giorni. Per evitare che Identity Manager attenda il completamento di tutti gli eventi per applicare i criteri di identità o sincronizzare gli account, selezionare l'opzione A ogni evento.

Se si aggiungono attributi ad attività di amministrazione che gestiscono gli utenti, è necessario aggiornare i mapping di attributo nella schermata di provisioning della console di gestione. Per ciascun attributo utente in Identity Manager, esiste un attributo di provisioning predefinito.

User Attribute	Provisioning Attribute
☐ %ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
☐ %EMAIL%	%EMAIL%
☐ %ENABLED_STATE%	%ENABLED_STATE%
☐ %FIRST_NAME%	%FIRST_NAME%
☐ %FULL_NAME%	%FULL_NAME%
☐ %IDENTITY_POLICY%	%IDENTITY_POLICY%
☐ %LAST_NAME%	%LAST_NAME%
☐ %PASSWORD%	%PASSWORD%
☐ %PASSWORD_DATA%	%PASSWORD_DATA%
☐ %USER_ID%	%USER_ID%

Attività di sincronizzazione

È possibile eseguire i seguenti tipi di sincronizzazione:

Sincronizzazione utente

Assicura che ciascun utente disponga degli account necessari sugli endpoint gestiti appropriati, e che ciascun account venga assegnato ai modelli di account appropriati in base a quanto richiesto nei ruoli di provisioning dell'utente.

Sincronizzazione account

Assicura che i valori di attributo di compatibilità degli account siano i valori appropriati in base a quanto indicato nei modelli di account assegnati dell'account. La sincronizzazione di account può essere sicura o minima. Una sincronizzazione minima assicura che gli attributi di compatibilità degli account abbiano almeno la compatibilità minima richiesta dai relativi modelli di account. Una sincronizzazione sicura assicura che gli attributi di compatibilità degli account abbiano la compatibilità esatta richiesta dai relativi modelli di account. La sincronizzazione di account è sicura se l'account appartiene ad almeno un modello di account in cui la casella di controllo Sincronizzazione sicura è selezionata.

L'opzione Sincronizzazione utente non è controllata da una casella di controllo Sincronizzazione sicura corrispondente, ma un concetto simile esiste. Quando si invia la voce di menu Sincronizza utente con ruolo a un utente, si presentano due opzioni di sincronizzazione:

- Aggiungere account mancanti e assegnazioni di modelli di account.
- Eliminare account extra e assegnazioni di modelli di account.
- Selezionando solo la casella di verifica Aggiungi, similmente alla sincronizzazione account minima, si richiede che gli utenti globali abbiano come minimo tutti gli account richiesti dai propri ruoli di provisioning assegnati, ma si consente agli utenti di disporre di account aggiuntivi non specificati da ruoli di provisioning attuali.

Selezionando entrambe le caselle di verifica Aggiungi ed Elimina, similmente alla sincronizzazione account sicura, si ottiene che i ruoli di provisioning definiscano esattamente di quali account l'utente deve disporre. Eventuali account aggiuntivi vengono eliminati.

Scegliere l'opzione Weak/Strong Account Synchronization (Sincronizzazione account minima/sicura) o Weak/Strong User Synchronization (Sincronizzazione utente minima/sicura) in base alla precisione con cui i ruoli di provisioning sono definiti. Se gli utenti rientrano in ruoli di provisioning chiaramente definiti dove l'accesso all'account è legato a questi ruoli, utilizzare la sincronizzazione sicura.

Nota: alcuni tipi di endpoint impostano la sincronizzazione sicura come opzione predefinita. Per ulteriori informazioni, consultare la guida *Connectors Guide*.

La sincronizzazione utente e la sincronizzazione di account sono attività separate che devono essere eseguite individualmente. Generalmente, per assicurare che tutti gli account necessari vengano creati, si esegue innanzitutto la sincronizzazione utente, mentre la sincronizzazione di account viene eseguita in un secondo momento, in modo che il server di provisioning assegni o modifichi i valori degli attributi di account.

Il server di provisioning fornisce due gruppi di opzioni del menu di sincronizzazione per gli oggetti:

- Le opzioni del menu di verifica della sincronizzazione verificano la sincronizzazione e restituiscono un elenco degli account che non rispettano i ruoli di provisioning o i modelli di account.
- Le opzioni del menu di sincronizzazione consentono di sincronizzare gli utenti globali con i relativi ruoli di provisioning o gli account con i relativi modelli di account.

Se si eseguono per prime le funzioni di verifica della sincronizzazione, il server di provisioning segnala quali correzioni verranno eseguite dalle funzioni di sincronizzazione. Se le funzioni di verifica della sincronizzazione non rilevano alcun problema, le funzioni di sincronizzazione non vengono eseguite.

Perché gli utenti perdono la sincronizzazione

Di seguito vengono descritte alcune cause della perdita di sincronizzazione tra gli utenti e i rispettivi ruoli di provisioning o modelli di account:

- I precedenti tentativi di creare gli account necessari non sono riusciti per problemi di hardware o software della rete, causando la perdita di account.
- I ruoli di provisioning e i modelli di account possono avere subito delle modifiche, causando di conseguenza, la creazione di account extra o la perdita di account.
- Gli account sono stati assegnati a modelli di account dopo la loro creazione, e per questo motivo esistono account che non sono stati sincronizzati con i rispettivi modelli di account.
- La creazione di un nuovo account viene ritardata, in quanto era stato specificato che l'account sarebbe stato creato successivamente.
- È stato acquisito un endpoint. Durante l'esplorazione e la correlazione, il server di provisioning non assegna ruoli di provisioning agli utenti in automatico, e per questo motivo è necessario aggiornare il ruolo per indicare quali utenti devono disporre di account sul nuovo endpoint. Qualsiasi account messo in correlazione con un utente viene classificato come account extra quando l'utente viene sincronizzato.
- Un account esistente è stato assegnato a un utente copiando l'account nell'utente. In questo modo si esegue una correlazione manuale e si stabilisce un account extra.
- È stato creato un account per un utente, invece di assegnare l'utente a un ruolo. Ad esempio, se si copia un utente in un modello di account che non si trova in nessuno dei ruoli di provisioning dell'utente, l'account viene classificato come account extra o come account con un modello di account extra. Se si copia l'utente in un endpoint per creare un account utilizzando il modello di account predefinito, tale account potrebbe essere un account extra.

Sincronizzazione utente

La sincronizzazione utente crea, aggiorna o elimina gli account, in modo che siano conformi ai ruoli di provisioning assegnati a un utente. In questo modo, se gli amministratori aggiungono o eliminano account su un endpoint gestito mediante strumenti nativi e non è stata eseguita una ri-esplorazione recente dell'endpoint per aggiornare la directory di provisioning, è possibile che la sincronizzazione utente non rilevi problemi quando in realtà un utente può avere account extra o mancanti.

Utente con ruoli di sincronizzazione

È possibile verificare la sincronizzazione negli utenti per elencare account extra, modelli di account e account mancanti. Quando si richiede la sincronizzazione di un utente con i ruoli, il server di provisioning assicura che l'utente disponga di tutti gli account richiesti dai ruoli di provisioning della persona e che ciascun account appartenga ai modelli di account corretti.

- Con questa attività, è possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account nei ruoli di provisioning dell'utente prescrive lo stesso account, l'account viene creato unendo tutti i modelli di account interessati.
- Durante la sincronizzazione tra utente e ruoli, è disponibile l'opzione per l'eliminazione degli account extra. È possibile determinare che gli utenti abbiano ragioni legittime per avere account diversi da quelli richiesti dai ruoli di provisioning. In questo caso, non è necessario selezionare l'opzione di eliminazione.

Se un account che viene eliminato risiede su un endpoint gestito per il quale sono state disabilitate le eliminazioni di account, l'account non viene veramente eliminato.

Creare account

Poiché i ruoli di provisioning contengono modelli di account e i modelli di account sono associati agli endpoint, è opportuno che un utente abbia gli account elencati su ciascun endpoint con gli attributi di account corretti.

Con questa attività, è possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account nei ruoli di provisioning dell'utente prescrive lo stesso account, l'account viene creato unendo tutti i modelli di account interessati.

Questo account viene assegnato ai modelli di account attualmente non sincronizzati con l'account. La sincronizzazione dell'account non è necessaria sugli account appena creati.

Eliminare gli account

Durante la sincronizzazione tra utente e ruoli, è disponibile l'opzione per l'eliminazione degli account extra. È possibile determinare che gli utenti abbiano ragioni legittime per avere account diversi da quelli richiesti dai ruoli di provisioning. In questo caso, non è necessario selezionare l'opzione di eliminazione.

Se un account che viene eliminato risiede su un endpoint gestito per il quale sono state disabilitate le eliminazioni di account, l'account non viene veramente eliminato.

Aggiungere modelli di account agli account

Se in un account mancano una o più assegnazioni di modelli di account, l'utente con la sincronizzazione di modelli di account assegna un account esistente a questi modelli di account. Quando un account viene assegnato a uno o più nuovi modelli di account, la sincronizzazione di account viene eseguita automaticamente per aggiornare gli attributi di compatibilità dell'account con le compatibilità specificate nei modelli di account.

Dopo l'aggiornamento di account da parte di un utente con la sincronizzazione dei modelli di account, l'account può essere o meno in sincronia con i relativi modelli di account. Se uno dei modelli di account aggiunti era un modello di account con sincronizzazione sicura o se due o più modelli di account sono stati aggiunti a un account, l'utente con la sincronizzazione dei ruoli avvierà una sincronizzazione di account completa sull'account. Tuttavia, se è stato aggiunto un modello di account con sincronizzazione minima, la sincronizzazione utente con la sincronizzazione dei modelli di account avvia una sincronizzazione di account che coinvolge solamente questo modello di account. Se, prima di questo aggiornamento, l'account non era sincronizzato con i relativi modelli di account, è possibile che anche dopo l'aggiornamento sia ancora non sincronizzato.

Rimozione dei modelli di account dagli account

È possibile utilizzare un utente con la sincronizzazione dei ruoli anche per rimuovere modelli di account extra da un account. Ciò è possibile solo se si seleziona l'opzione di eliminazione. Se la sincronizzazione utente determina che un account debba essere aggiornato per rimuovere uno o più modelli di account extra, la sincronizzazione di account viene eseguita automaticamente sull'account per sincronizzare gli attributi di compatibilità con i modelli di account che rimangono sull'account.

La sincronizzazione di account che si verifica quando si rimuovono i modelli di account da un account utilizzerà la sincronizzazione sicura se uno qualsiasi dei modelli di account rimanenti è contrassegnato per la sincronizzazione sicura, mentre utilizzerà la sincronizzazione minima se tutti i modelli di account rimanenti sono contrassegnati per la sincronizzazione minima.

La scelta di utilizzare la sincronizzazione minima o sicura determina se le compatibilità degli account concesse quando un modello di account viene assegnato all'account vengono revocate nel momento in cui viene rimosso il modello di account. Con la sincronizzazione sicura, una compatibilità concessa da un modello di account, come ad esempio l'appartenenza a un gruppo o una quota più alta, verrà revocata (ovvero l'appartenenza di gruppo verrà rimossa o la quota abbassata) se nessuno dei modelli di account rimasti nell'account stabilisce tale compatibilità. Tuttavia, con la sincronizzazione minima, generalmente l'account rimane immutato, in quanto il server di provisioning non distingue tra compatibilità aggiuntive su richiesta e compatibilità concesse mediante i modelli di account.

Un'eccezione a questa regola sono sicuramente gli attributi di compatibilità multivalore designati come attributi SyncRemoveValues. Un attributo multivalore semplice che rappresenta una raccolta di valori assegnata all'account (ad esempio, un elenco di appartenenza al gruppo), generalmente verrà classificato come attributo SyncRemoveValues. Per questi attributi, l'azione di sincronizzazione minima che si verifica rimuovendo un modello di account da un account, rimuoverà i valori prescritti dal modello di account che viene rimosso, a condizione che quel valore non sia stabilito anche da uno dei modelli di account restanti.

Ad esempio, se si creano modelli di account in cui ciascun modello di account assegna un'appartenenza al gruppo univoca per il proprio account, la funzionalità SyncRemoveValues determina che, quando si modificano i ruoli di provisioning di un utente globale per far sì che un modello di account particolare non sia più necessario, l'account verrà aggiornato e non apparterrà più al gruppo stabilito da quel modello di account. Si noterà che questa azione non è esattamente come la sincronizzazione sicura, dal momento che le appartenenze al gruppo concesse al di là di quanto stabilito per i modelli di account vengono mantenute.

Per tutti gli attributi di valore singolo e alcuni attributi multivalore che non sono designati come attributi SyncRemoveValues, l'azione di sincronizzazione minima, con la rimozione di un modello di account da un account, ha lo stesso effetto di un'azione di sincronizzazione minima normale: le compatibilità non vengono mai rimosse.

Se si desidera che le compatibilità non vengano mai rimosse dalla sincronizzazione minima, disabilitare la funzionalità SyncRemoveValues impostando il parametro di configurazione dominio Synchronize/Remove Account Template Values from Accounts (Sincronizza/Rimuovi valori di modelli di account dagli account) su No.

Sincronizzazione dei modelli di account

Le modifiche effettuate ai modelli di account condizionano gli account esistenti nel modo seguente:

- Se si modifica il valore di un attributo di compatibilità, l'attributo account corrispondente viene aggiornato, se necessario, in modo da sincronizzarlo con il valore dell'attributo del modello di account. Consultare la descrizione di sincronizzazione minima e sicura.
- Alcuni attributi account vengono designati dal connettore come non aggiornati in caso di modifiche al modello di account, ad esempio l'attributo Password e determinati attributi che possono essere impostati dal tipo di endpoint unicamente durante la creazione dell'account.

Aggiornamento degli attributi

Quando vengono modificati gli attributi di compatibilità in un modello di account, è possibile che l'attributo corrispondente negli account venga modificato. Questa modifica ha un impatto sugli attributi dell'account. L'impatto si basa sui seguenti fattori:

- Se la definizione del modello di account prevede l'utilizzo della sincronizzazione minima o sicura.
- Se l'account appartiene a più modelli di account.

Sincronizzazione minima

La sincronizzazione minima assicura che gli utenti dispongano degli attributi di compatibilità minimi richiesti per i relativi account. Si tratta della sincronizzazione predefinita nella maggior parte dei tipi di endpoint. Se si aggiorna un modello che utilizza la sincronizzazione minima, CA Identity Manager aggiorna gli attributi di capacità nel modo seguente:

- Se viene aggiornato un campo numerico in un modello di account e il nuovo numero è maggiore di quello nell'account, il valore nell'account viene modificato in modo che corrisponda al nuovo numero.
- Se una casella di controllo in un modello di account non era selezionata e successivamente viene selezionata, la casella di controllo viene aggiornata in tutti gli account in cui non è selezionata.
- Se viene modificato un elenco in un modello di account, vengono aggiornati tutti gli account per includere tutti i valori presenti nel nuovo elenco che non erano inclusi nell'elenco di valori dell'account.

Se un account appartiene ad altri modelli di account, a prescindere dal fatto che tali modelli utilizzino la sincronizzazione minima o sicura, in CA Identity Manager viene consultato solo il modello modificato. Questa procedura risulta più efficiente rispetto al controllo di tutti i modelli di account. Poiché con la sincronizzazione minima vengono solo aggiunte compatibilità agli account, in genere non è necessario consultare altri modelli di account.

Nota: in caso di propagazione da un modello di account con sincronizzazione minima, le modifiche che comportano la rimozione o la riduzione di compatibilità possono lasciare alcuni account privi di sincronizzazione. Tenere presente che la sincronizzazione minima non determina mai la rimozione o la riduzione di compatibilità. Senza consultare altri modelli per un account, la propagazione non considera se la sincronizzazione minima è sufficiente.

In questa situazione, utilizzare Sincronizza utente con modelli account per sincronizzare l'account con i rispettivi modelli di account.

Sincronizzazione sicura

La sincronizzazione sicura garantisce che gli account presentino gli stessi attributi account specificati nel modello di account.

Ad esempio, a un modello di account UNIX esistente è stato aggiunto un gruppo. All'inizio, il modello di account inseriva gli account nel gruppo del personale. Adesso si desidera inserire gli account nei gruppi del personale e del sistema. Tutti gli account associati al modello di account si considerano sincronizzati quando ciascuno è inserito in entrambi i gruppi del personale e del sistema (e in nessun altro gruppo). Gli account non presenti nel gruppo del personale sono aggiunti a entrambi i gruppi.

Tra gli altri fattori da considerare vi sono le seguenti situazioni:

- Se il modello di account utilizza la sincronizzazione sicura, qualsiasi account che appartiene ad altri gruppi, diversi da quelli del personale e del sistema, viene rimosso da quei gruppi extra.
- Se il modello di account utilizza la sincronizzazione minima, gli account vengono aggiunti ai gruppi del personale e del sistema. Qualsiasi account con gruppi aggiuntivi definiti resta inserito in questi gruppi.

Nota: Sincronizzare regolarmente gli account con i relativi modelli per far sì che gli account rimangano sincronizzati con i relativi modelli di account.

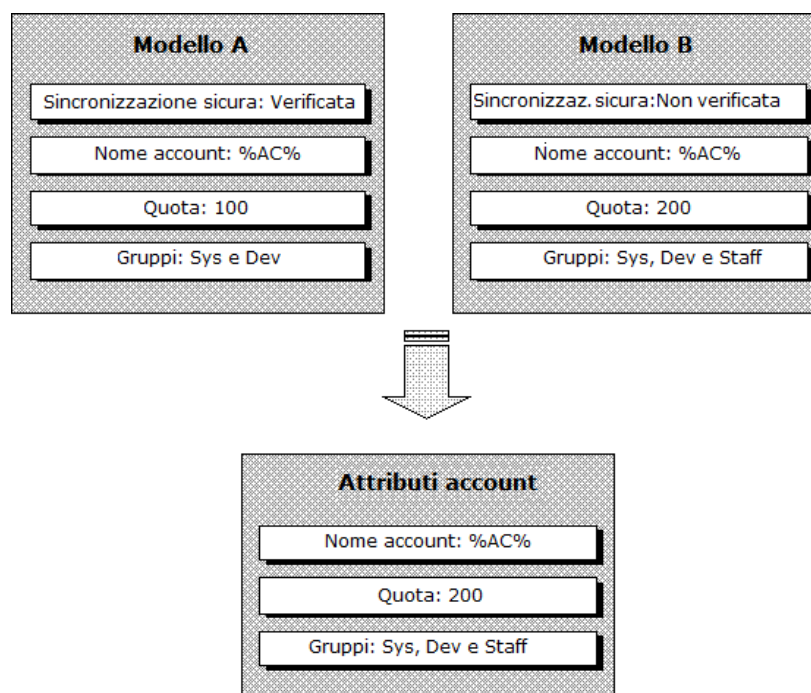
Account con più modelli

La sincronizzazione dipende anche se l'account appartiene a più modelli di account. Se un account ha un solo modello di account che utilizza la sincronizzazione sicura, ogni attributo viene aggiornato in modo che corrisponda esattamente a quanto restituito dal valore dell'attributo del modello di account. Si ottiene lo stesso risultato come se l'attributo fosse un attributo iniziale.

Un account può appartenere a più modelli di account, come nel caso di un utente che appartiene a più ruoli di provisioning, ognuno dei quali prevede un certo livello di accesso sullo stesso endpoint gestito. In questo caso, CA Identity Manager associa quei modelli di account in un unico modello di account valido che definisce il soprainsieme di compatibilità prese dai singoli modelli di account. Questo modello di account utilizza una sincronizzazione minima se tutti i singoli modelli di account sono minimi, oppure la sincronizzazione sicura se un singolo modello di account è sicuro.

Nota: in genere viene utilizzata solo la sincronizzazione minima o solo quella sicura per i modelli di account che controllano un account, a seconda se i propri ruoli aziendali definiscono completamente gli accessi necessari per gli utenti. Se gli utenti non rientrano in ruoli ben precisi ed è richiesta flessibilità per concedere compatibilità aggiuntive agli account utente, utilizzare la sincronizzazione minima. Se è possibile definire ruoli per specificare esattamente gli accessi necessari agli utenti, utilizzare la sincronizzazione sicura.

L'esempio seguente mostra l'associazione di più modelli di account in un singolo modello di account valido. In questo esempio, un modello di account viene contrassegnato per la sincronizzazione minima e l'altro per la sincronizzazione sicura. Di conseguenza, il modello di account valido creato combinando i due modelli di account viene considerato come un modello di account con sincronizzazione sicura. L'attributo Quota, espresso con un numero intero, adotta il valore maggiore dai due modelli di account, mentre l'attributo Gruppi con più valori adotta l'unione dei valori tratti dai due criteri.



Attributi solo per i nuovi account

In un modello di account, alcuni attributi vengono applicati solo durante la creazione dell'account. Ad esempio, l'attributo Password è un'espressione di regola che definisce la password per i nuovi account. Questa espressione di regola non aggiorna mai la password di un account. Le modifiche apportate all'espressione di regola per la password interessano solo sugli account creati successivamente all'impostazione di tale espressione.

Analogamente, un'espressione di regola modello per un attributo di account di sola lettura interessa solo gli account creati successivamente all'impostazione di tale espressione. La sua modifica non incide sugli account esistenti.

Sincronizzazione account

La sincronizzazione di account aggiorna gli attributi di compatibilità per assicurare che l'account disponga delle compatibilità specificate nel modello di account. La sincronizzazione non influisce sugli attributi iniziali dell'account.

Per sincronizzare le modifiche agli attributi di compatibilità di un modello di account con i relativi account, utilizzare una delle opzioni del menu di sincronizzazione descritte in questa sezione.

Verificare la sincronizzazione degli account

È possibile verificare la sincronizzazione di account per endpoint e utenti. Questa azione restituisce un elenco di account non conformi ai modelli di account. Nella tabella seguente vengono descritte le conseguenze della sincronizzazione degli account su ciascun oggetto:

Oggetto	Sincronizza
Endpoint	Gli attributi di account per ciascun account in un endpoint e assicura che siano conformi ai modelli di account associati.
Utente globale	Gli attributi di account per ciascun account utente e assicura che siano conformi ai modelli di account associati.

Sincronizzare gli account

È possibile eseguire la sincronizzazione degli account su endpoint, utenti e modelli di account. Nella tabella seguente vengono elencati gli effetti della sincronizzazione su ciascun oggetto:

Oggetto	Sincronizza
Endpoint	Ciascun account in un endpoint con i modelli di account associati.
Utente globale	Ciascun account di un utente globale con tutti i modelli di account associati.

Capitolo 11: Flusso di lavoro

Questa sezione contiene i seguenti argomenti:

[Panoramica del flusso di lavoro](#) (a pagina 263)

[Utilizza il controllo del flusso di lavoro - metodo basato su modelli](#) (a pagina 266)

[Utilizzo del metodo WorkPoint](#) (a pagina 286)

[Visualizzazione di processi Workpoint](#) (a pagina 318)

[Flusso di lavoro basato su criterio](#) (a pagina 319)

[Richieste in linea](#) (a pagina 338)

[Comandi operazione del flusso di lavoro](#) (a pagina 342)

[Elenchi ed elementi di lavoro](#) (a pagina 347)

Panoramica del flusso di lavoro

La funzionalità del flusso di lavoro di CA Identity Manager consente la gestione di un'attività di CA Identity Manager da parte di un processo del flusso di lavoro. Un *processo del flusso di lavoro* è composto da uno o più passaggi che devono essere eseguiti prima che CA Identity Manager possa completare un'attività gestita dal flusso di lavoro stesso. Un *processo* è un'istanza runtime di un processo del flusso di lavoro.

WorkPoint Designer è un software sviluppato da Workpoint LLC, una consociata di Planet Group, Inc., che è integrato in CA Identity Manager. WorkPoint Designer consente di gestire i processi e le singole attività del flusso di lavoro.

Un processo del flusso di lavoro è composto da uno o più passaggi, denominati *attività*, che devono essere eseguiti per il complemento di attività aziendali specifiche, ad esempio la creazione o la modifica di un account utente per i dipendenti. In genere, un processo del flusso di lavoro contiene una o più attività manuali che richiedono l'approvazione o il rifiuto da parte di un utente o partecipante autorizzato.

Un *partecipante* è una persona autorizzata ad eseguire un'attività del flusso di lavoro. In CA Identity Manager, i partecipanti sono definiti anche *revisori*, in quanto devono approvare o rifiutare l'attività gestita dal flusso di lavoro. Un *resolver partecipanti* è una regola o un insieme di criteri per determinare i partecipanti.

Le singole attività manuali all'interno di un flusso di lavoro sono definite *elementi di lavoro* in CA Identity Manager.

Un *elenco di lavoro* è un elenco generato dal flusso di lavoro contenente le attività di approvazione, o *elementi di lavoro*, visualizzati nella console utente del partecipante autorizzato ad approvare l'attività.

Diagramma del processo di WorkPoint

In generale, le attività di CA Identity Manager attivano eventi di CA Identity Manager. Ad esempio, per creare un utente, un amministratore seleziona l'attività Crea utente. Quando questa attività viene avviata, viene attivato l'evento CreateUserEvent.

Nel diagramma seguente viene illustrato un esempio del processo del flusso di lavoro, ovvero il processo predefinito CreateUserApproveProcess, come viene visualizzato in WorkPoint Designer. Il processo viene richiamato da un evento CreateUserEvent se l'attività Crea utente viene gestita dal flusso di lavoro.

Il processo include un'attività manuale (Approva Crea utente), che corrisponde a un'attività di approvazione del flusso di lavoro di CA Identity Manager avente lo stesso nome. Il partecipante deve approvare o rifiutare l'attività di approvazione, in genere facendo clic su un pulsante nella console utente, prima che l'attività gestita dal flusso di lavoro possa essere eseguita e completata.

Flusso di lavoro e notifiche via posta elettronica

Quando viene avviata un'attività, questa viene inoltrata per l'elaborazione e viene visualizzato un messaggio di conferma simile a quello riportato di seguito:

Conferma: Attività completata.

Tuttavia, se l'attività è gestita mediante il flusso di lavoro e richiede l'approvazione, il messaggio sarà analogo al seguente:

Avviso: In attesa di attività.

Oltre ai messaggi visualizzati sulla schermata, CA Identity Manager può generare automaticamente notifiche di posta elettronica nei seguenti casi:

- Un evento o un'attività che richiede l'approvazione o il rifiuto da parte del revisore del flusso di lavoro risulta in sospeso.
- Un revisore approva un evento o un'attività.
- Un revisore rifiuta un evento o un'attività.
- Un evento o un'attività vengono completati.

Ulteriori informazioni:

[Notifiche di posta elettronica](#) (a pagina 361)

Documentazione di WorkPoint

Per informazioni generali di base relative al flusso di lavoro e per istruzioni su processi ed attività del flusso di lavoro in WorkPoint Designer, consultare la documentazione di WorkPoint. A tale scopo, aprire la seguente pagina HTML:

`admin_tools\WorkPoint\docs\designer\default.htm`

admin_tools

Corrisponde alla directory di installazione degli strumenti di amministrazione di CA Identity Manager. La directory di installazione predefinita è la seguente:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Nota: Workpoint è un prodotto di terze parti installato con CA Identity Manager. CA Identity Manager supporta un sottoinsieme di funzionalità utilizzate in Workpoint. Ad esempio, CA Identity Manager non supporta WpConsole. Tuttavia, la documentazione di Workpoint descrive tutte le funzionalità del prodotto. Parti della documentazione di Workpoint non sono applicabili per gli utenti di CA Identity Manager.

Metodi per il controllo del flusso di lavoro

In CA Identity Manager sono disponibili due metodi per impostare il controllo delle attività da parte del flusso di lavoro.

Metodo basato su modelli

In CA Identity Manager sono disponibili modelli di processo del flusso di lavoro che è possibile utilizzare per impostare il controllo delle attività da parte del flusso di lavoro. Il *metodo basato su modelli* consente di utilizzare questi modelli per configurare e gestire il flusso di lavoro interamente dalla console utente. Questi modelli di processo generici, introdotti in CA Identity Manager r12, possono essere configurati per controllare la maggior parte delle attività e degli eventi di CA Identity Manager.

Il metodo basato su modelli rende disponibili le seguenti nuove funzionalità:

- Controllo del flusso di lavoro sia a livello di attività che a livello di evento
- Configurazione semplificata dei resolver partecipanti per i revisori del flusso di lavoro
- Delega degli elementi di lavoro, che supporta scenari "fuori sede" consentendo a un utente di delegare a un altro utente l'approvazione degli elementi di lavoro
- Riassegnazione degli elementi di lavoro, che consente la riassegnazione di un'attività in corso a un altro utente per l'approvazione

Metodo WorkPoint

In CA Identity Manager è inoltre disponibile un insieme di processi del flusso di lavoro predefiniti con mapping di eventi predefiniti corrispondenti a specifiche attività di CA Identity Manager. Il *metodo WorkPoint* richiede la configurazione e la personalizzazione di questi processi all'interno di WorkPoint Designer. Questi processi predefiniti sono compatibili con le versioni di CA Identity Manager precedenti alla r12.

Il metodo WorkPoint rende anche disponibili le seguenti nuove funzionalità:

- Controllo del flusso di lavoro sia a livello di attività che a livello di evento
- Delega degli elementi di lavoro, che supporta scenari "fuori sede" consentendo a un utente di delegare a un altro utente l'approvazione degli elementi di lavoro
- Riassegnazione degli elementi di lavoro, che consente la riassegnazione di un'attività in corso a un altro utente per l'approvazione

Nota: per ottimizzare la flessibilità e semplificarne l'utilizzo, CA consiglia di utilizzare il metodo basato su modelli, laddove possibile.

Ulteriori informazioni:

[Utilizza il controllo del flusso di lavoro - metodo basato su modelli](#) (a pagina 266)

Utilizza il controllo del flusso di lavoro - metodo basato su modelli

Il metodo basato su modelli, introdotto in CA Identity Manager r12, consente di configurare i modelli dei processi del flusso di lavoro nella console utente senza dover aprire WorkPoint Designer.

I vantaggi del metodo basato su modelli sono riportati di seguito:

- I modelli di processi in più fasi possono soddisfare la maggior parte delle esigenze a livello di flusso di lavoro senza la necessità di interventi di personalizzazione in WorkPoint Designer.
- I modelli supportano il controllo del flusso di lavoro sia a livello di attività che a livello di evento.
- Lo stesso modello di processo del flusso di lavoro può essere configurato per l'utilizzo con diverse attività mentre la stessa struttura del processo rimane invariata.

- È inoltre possibile specificare i resolver partecipanti in modo semplice e rapido nella console utente.
- La delega degli elementi di lavoro può essere eseguita nella console utente.

Prerequisito: Attiva flusso di lavoro

È innanzitutto necessario attivare il flusso di lavoro prima di poterlo utilizzare per gestire le attività di CA Identity Manager. Per impostazione predefinita, il flusso di lavoro è disattivato.

Procedere come descritto di seguito:

1. Nella console di gestione selezionare un ambiente.
2. Passare a Impostazioni avanzate, Flusso di lavoro.
3. Selezionare la casella di controllo Attivato, quindi fare clic su Salva.

Nota: i mapping degli eventi visualizzati in questa schermata sono validi solo se si utilizza il metodo WorkPoint per configurare il flusso di lavoro. Se si utilizza il metodo basato su modelli (opzione consigliata), non eseguire il mapping degli eventi ai processi utilizzando questa console di gestione.

4. Riavviare il server applicazioni.
5. (Facoltativo) [Configurare gli strumenti di amministrazione di WorkPoint](#) (a pagina 288).

Ulteriori informazioni:

[Mapping di un processo ad un evento a livello globale](#) (a pagina 295)

[Metodi per il controllo del flusso di lavoro](#) (a pagina 265)

Colloca le attività di amministrazione sotto il controllo del flusso di lavoro - metodo basato su modelli

In qualità di amministratori, mediante il metodo basato su modelli, è possibile collocare le attività di amministrazione sotto il controllo del flusso di lavoro.



Procedere come descritto di seguito:

1. Nella console utente selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione o Crea attività di amministrazione.
2. Cercare l'attività per la quale impostare il controllo da parte del flusso di lavoro, quindi fare clic su Seleziona.
3. Eseguire *una* delle seguenti operazioni:
 - [Implementare il flusso di lavoro a livello di evento](#) (a pagina 269) facendo clic sul pulsante di modifica Processo del flusso di lavoro sulla scheda Profilo.
 - [Implementare il flusso di lavoro a livello di evento](#) (a pagina 272) selezionando uno o più eventi sulla scheda Eventi.
4. [Selezionare un modello di processo](#) (a pagina 275).
5. [Configurare i resolver partecipanti](#) (a pagina 279).
6. Selezionare la modalità di approvazione del flusso di lavoro.
7. [\(Facoltativo\) Impostare un criterio di posta elettronica per il processo del flusso di lavoro](#) (a pagina 284).

Nota: Se si seleziona il processo EscalationApproval, viene visualizzato un campo denominato Timeout approvazione (min). Il campo è specificato il minuti e non può essere vuoto. Per impostazione predefinita, il valore è impostato su 60 minuti.

Al termine della configurazione del controllo del flusso di lavoro, un utente con il ruolo appropriato esegue l'attività di amministrazione e il partecipante al flusso di lavoro designato approva o rifiuta l'attività o l'evento.

Flusso di lavoro basato sull'evento o sull'attività

CA Identity Manager consente di associare i processi del flusso di lavoro ad attività o eventi. Ciò significa che i partecipanti possono approvare o rifiutare un'intera attività di CA Identity Manager oppure un evento specifico all'interno di un'attività.

Alcune attività di CA Identity Manager, ad esempio, generano diversi eventi e un revisore potrebbe avere l'esigenza di esaminare tutti gli eventi prima di decidere se approvare o rifiutare una richiesta. Ciò è possibile in un flusso di lavoro a livello di attività. Quando un processo del flusso di lavoro viene associato ad un evento specifico all'interno di un'attività, un revisore non può visualizzare il contesto complessivo dell'attività all'interno del quale è stata presentata una richiesta.

Flusso di lavoro a livello di attività

Il flusso di lavoro a livello di attività consente ai revisori di rivedere tutti gli eventi prima di decidere se approvare o rifiutare una richiesta. Il flusso di lavoro a livello di attività si verifica prima che un'attività specifica venga elaborata. Prima dell'inizio del processo di elaborazione del flusso di lavoro non verrà eseguito alcun evento o alcuna attività nidificata.

Se il flusso di lavoro a livello di attività viene rifiutato, l'attività non verrà eseguita né parzialmente né globalmente.

Nota: Un'attività configurata per il controllo del flusso di lavoro a livello di attività può contemporaneamente essere configurata anche per il controllo del flusso di lavoro a livello di evento. Il flusso di lavoro concorrente a livello di evento può essere applicato globalmente oppure ad un'attività specifica.

Ulteriori informazioni

[Flusso di lavoro a livello di evento](#) (a pagina 272)

[Mapping globale processi/eventi](#) (a pagina 293)

Attributo del processo a livello di attività

I processi del flusso di lavoro compatibili con il flusso di lavoro a livello di attività hanno tutti un attributo speciale definito all'interno di WorkPoint Designer. Questo attributo relativo ai dati dell'utente a livello di processo, chiamato TASK_LEVEL, viene impostato in modo predefinito su true nei seguenti modelli di processo:

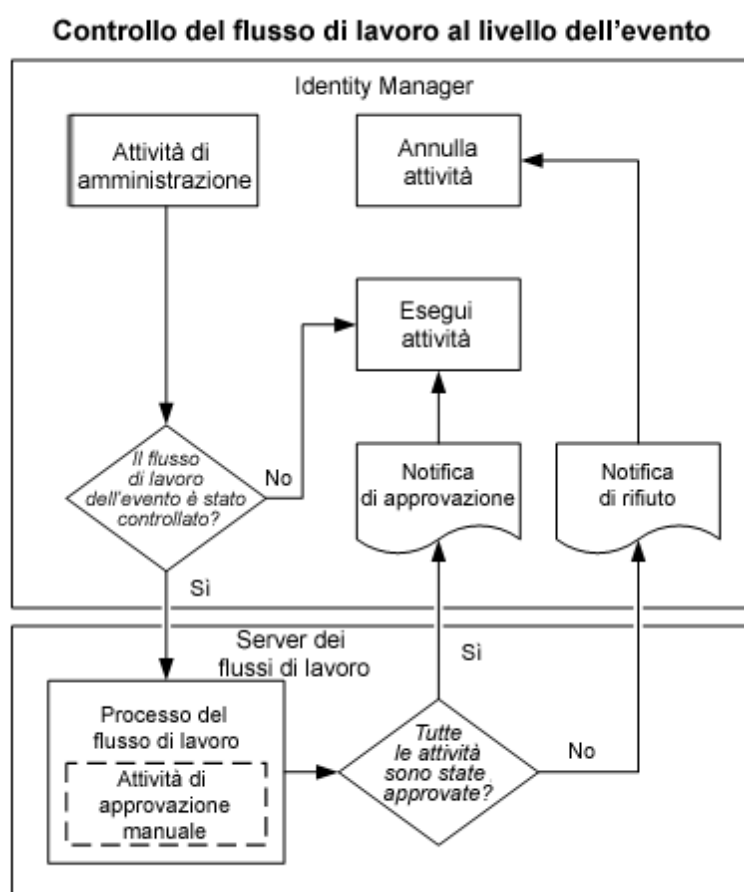
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

Quando si seleziona un'attività di amministrazione per il flusso di lavoro a livello di attività, sono disponibili solamente questi modelli di processo.

Nota: Nonostante TASK_LEVEL sia impostato su true, è comunque possibile utilizzare i modelli di processo per il flusso di lavoro a livello di evento. Non modificare il valore dell'attributo TASK_LEVEL.

Diagramma del controllo a livello di attività

Nel seguente diagramma viene illustrata l'interazione tra CA Identity Manager e il server del flusso di lavoro quando viene avviato un comune processo del flusso di lavoro a livello di attività.



Ulteriori informazioni:

[Diagramma del controllo a livello di evento](#) (a pagina 273)

Procedura di configurazione del flusso di lavoro a livello di attività

Il flusso di lavoro a livello di attività si verifica prima che un'attività specifica venga elaborata. Prima dell'inizio del processo di elaborazione del flusso di lavoro non verrà eseguito alcun evento o alcuna attività nidificata.

Configurazione del flusso di lavoro a livello di attività

1. Nella console utente selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione o Crea attività di amministrazione.
Viene visualizzato la schermata Selezionare attività di amministrazione.
2. Cercare l'attività per la quale impostare il controllo da parte del flusso di lavoro, quindi fare clic su Seleziona.
Viene visualizzato la schermata Modifica attività di amministrazione o Crea attività di amministrazione.
3. Nella scheda Profilo, verificare che l'opzione Attiva flusso di lavoro sia selezionata.
4. Nella scheda Profilo fare clic sul pulsante Processo del flusso di lavoro.
Viene visualizzata la scheda Configurazione del flusso di lavoro del livello attività.
5. Selezionare uno dei seguenti modelli di processo nell'elenco Processo del flusso di lavoro:
 - SingleStepApproval
 - TwoStageApprovalProcessLa scheda Configurazione del flusso di lavoro del livello attività verrà ingrandita.
6. Configurare i resolver partecipanti in modo conforme al modello di processo.
Le richieste dei partecipanti verranno aggiunte al processo.
7. Fare clic su OK.
La configurazione del flusso di lavoro a livello di attività viene salvata.
8. Fare clic su Invia.
La modifica all'attività viene elaborata in CA Identity Manager.

Flusso di lavoro a livello di evento

È possibile mappare un evento su un processo del flusso di lavoro. Quando viene attivato un evento mappato ad un processo del flusso di lavoro, tale processo inizia. L'attività che ha attivato l'evento viene collocata in uno stato In sospeso e viene considerata sotto il controllo del flusso di lavoro.

Un processo del flusso di lavoro può richiedere che un partecipante approvi o rifiuti un evento o un'attività prima che il processo possa essere completato. Il completamento di un'attività che richiede l'approvazione manuale del flusso di lavoro da parte di un partecipante richiede più tempo rispetto ad un'attività non sottoposta al controllo del flusso di lavoro.

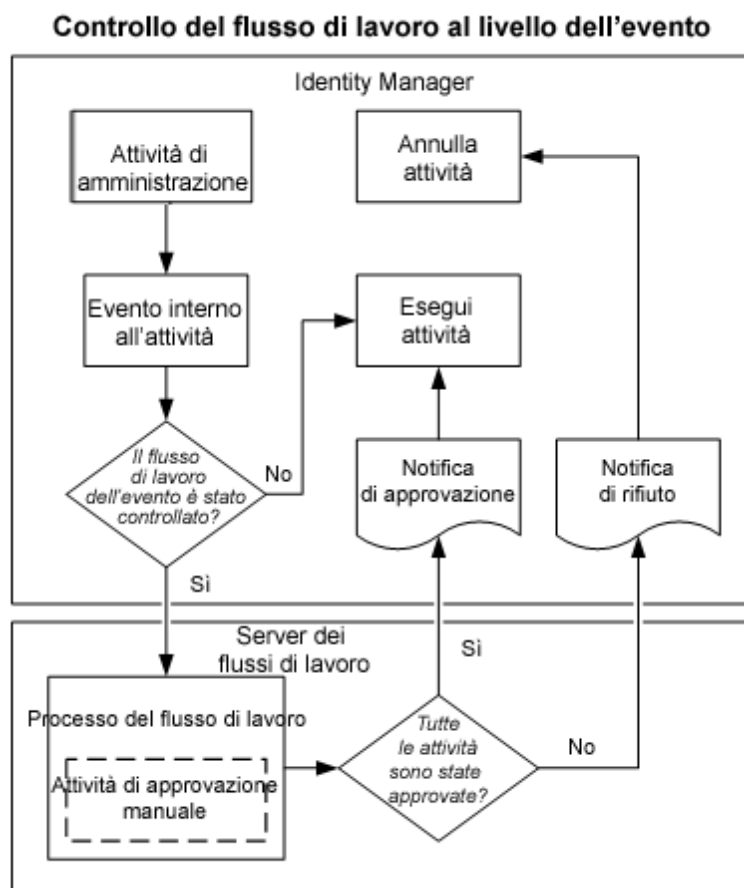
Dopo il completamento di tutte le attività incluse in un processo del flusso di lavoro, l'evento mappato a tale processo viene rilasciato dal controllo del flusso di lavoro. Quando tutti gli eventi attivati da una determinata attività vengono rilasciati dal controllo del flusso di lavoro, l'attività controllata da tale flusso è completa.

Mentre l'attività si trova sotto il controllo del flusso di lavoro, il contenuto delle schermate relative a tale attività viene memorizzato nel database di persistenza delle attività. Lo stato del processo del flusso di lavoro (dati rilevanti a livello del flusso di lavoro) viene archiviato nel database di WorkPoint.

Nota: nella scheda Eventi sono elencati gli eventi generati da ogni scheda in un'attività. Dopo avere aggiunto una nuova scheda a un'attività, è necessario inoltrare e quindi riaprire l'attività utilizzando Modifica attività di amministrazione prima che i nuovi eventi vengano visualizzati nella scheda Eventi.

Diagramma del controllo a livello di evento

Nel seguente diagramma viene illustrata l'interazione tra CA Identity Manager e il server del flusso di lavoro quando viene avviato un tipico processo del flusso di lavoro a livello di evento.



Ulteriori informazioni:

[Diagramma del controllo a livello di attività](#) (a pagina 270)

Procedura di configurazione del flusso di lavoro a livello di evento

Il flusso di lavoro a livello di evento viene avviato quando un evento viene mappato ad un processo del flusso di lavoro. Lo stato dell'attività che ha attivato l'evento viene impostato su In sospeso fino al momento in cui il partecipante approva o rifiuta l'attività.

Configurazione del flusso di lavoro a livello di evento

1. Nella console utente selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione o Crea attività di amministrazione.
Viene visualizzato la schermata Selezionare attività di amministrazione.
2. Cercare l'attività per la quale impostare il controllo da parte del flusso di lavoro, quindi fare clic su Seleziona.
Viene visualizzato la schermata Modifica attività di amministrazione o Crea attività di amministrazione.
3. Nella scheda Profilo, verificare che l'opzione Attiva flusso di lavoro sia selezionata.
4. Nella scheda Eventi selezionare un evento da mappare ad un modello di processo.
Verrà visualizzato la schermata del mapping del flusso di lavoro.
5. Selezionare uno dei seguenti modelli di processo nell'elenco Processo del flusso di lavoro:
 - SingleStepApproval
 - TwoStageApprovalProcessLa schermata del mapping del flusso di lavoro verrà ingrandito.
6. Configurare i resolver partecipanti in modo conforme al modello di processo.
Le richieste dei partecipanti verranno aggiunte al processo.
7. Fare clic su OK.
La configurazione del flusso di lavoro a livello di evento viene salvata.
8. Ripetere i passaggi 3-6 per ogni evento che si desidera sottoporre al controllo del flusso di lavoro.
9. Fare clic su Invia.
La modifica all'attività viene elaborata in CA Identity Manager.

Nota: nell'elenco Processo del flusso di lavoro sono inclusi i processi da utilizzare sia con il metodo basato su modelli che con il metodo WorkPoint:

- Quando si seleziona un processo del metodo basato su modelli (SingleStepApproval oppure TwoStageApprovalProcess), la pagina verrà ingrandita in modo da consentire la configurazione dei resolver partecipanti.
- Se invece si seleziona un metodo WorkPoint, la pagina non verrà ingrandita. I resolver partecipanti vengono configurati in WorkPoint Designer.

Tipi di modelli di processi

Un modello di processo del flusso di lavoro è caratterizzato da quanto segue:

- È definito in WorkPoint Designer.
- Contiene attività manuali, che corrispondono alle attività di approvazione di CA Identity Manager.
- Include attributi speciali contenenti informazioni per l'identificazione dei partecipanti (denominati anche responsabili dell'approvazione).

Nei modelli di processo del flusso di lavoro non sono incluse informazioni per la selezione di partecipanti specifici. Tali informazioni vengono fornite da CA Identity Manager in seguito alla configurazione di un flusso di lavoro e dei relativi resolver partecipanti da parte di un utente. Per queste informazioni viene eseguito il mapping ad un evento per il controllo del flusso di lavoro del livello evento, ed il mapping ad un'attività per il controllo del flusso di lavoro del livello attività.

Se si utilizza il metodo basato su modelli, l'intero processo di configurazione del flusso di lavoro e dei partecipanti viene eseguito all'interno della console utente.

Sono disponibili due modelli di processo da utilizzare nel metodo basato su modelli:

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

Funzionamento di un modello di processo

Un modello di processo del flusso di lavoro contiene una serie di punti in cui vengono richiesti elenchi di partecipanti. Quando il modello è mappato a un'attività o un evento di CA Identity Manager, è necessario configurare i resolver partecipanti per tali elenchi.

In fase di runtime, come illustrato nella figura seguente, gli elenchi di partecipanti vengono passati al processo del flusso di lavoro in base alle informazioni configurate.

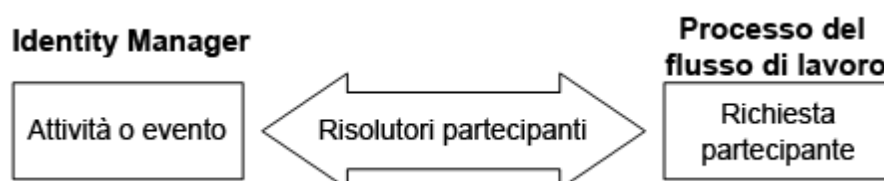


Diagramma del modello a fase singola

Nel seguente diagramma viene illustrato il modello di processo SingleStageApproval come viene visualizzato in WorkPoint Designer. Il modello di processo include due attività manuali:

- Un nodo di approvazione per il partecipante primario. Se tale utente approva o rifiuta la richiesta, l'esecuzione del processo viene completata.
- Un nodo di approvazione per il partecipante predefinito. Questo utente può approvare o rifiutare l'attività se il partecipante primario non è disponibile oppure se non risponde.

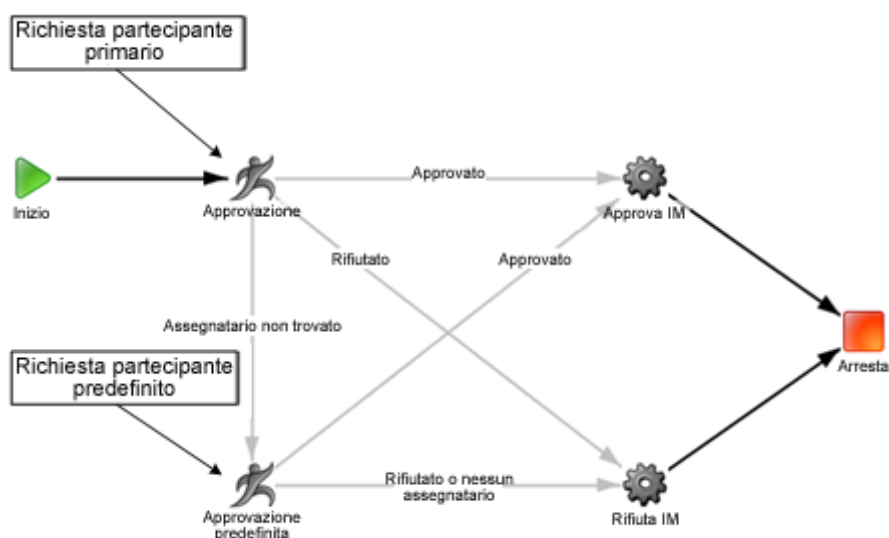


Diagramma del modello a due fasi

Nel seguente diagramma viene illustrato il modello di processo TwoStageApproval come viene visualizzato in WorkPoint Designer. Il modello di processo TwoStageApproval include tre attività manuali:

- Un nodo di approvazione per il partecipante aziendale. Se tale utente approva o rifiuta la richiesta, il processo passa al revisore tecnico.

- Un nodo di approvazione per il partecipante tecnico. Se tale utente approva o rifiuta la richiesta, l'esecuzione del processo viene completata.
- Un nodo di approvazione per il partecipante predefinito. Questo utente può approvare o rifiutare l'attività se il partecipante aziendale o tecnico non è disponibile oppure se non risponde.

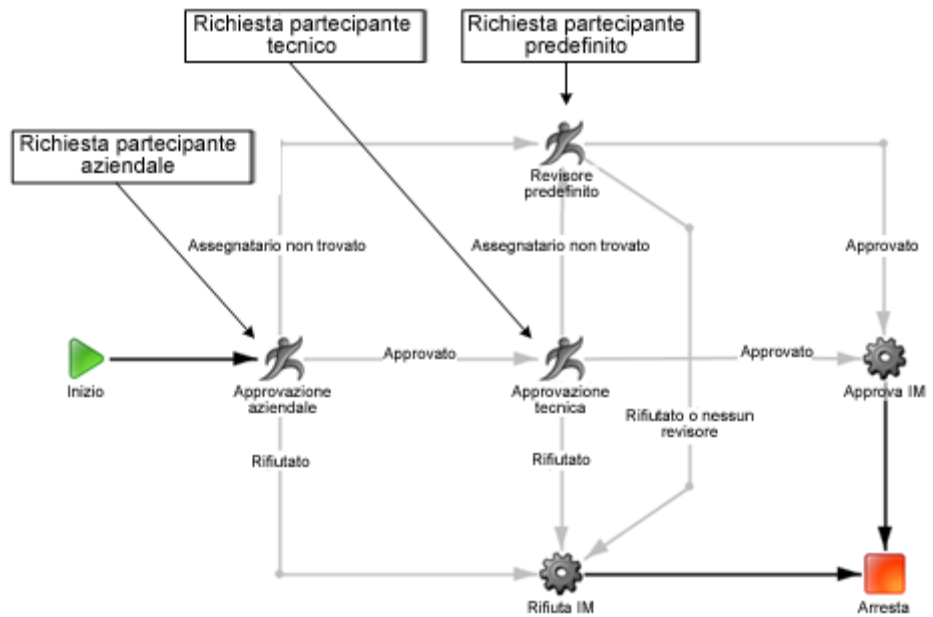
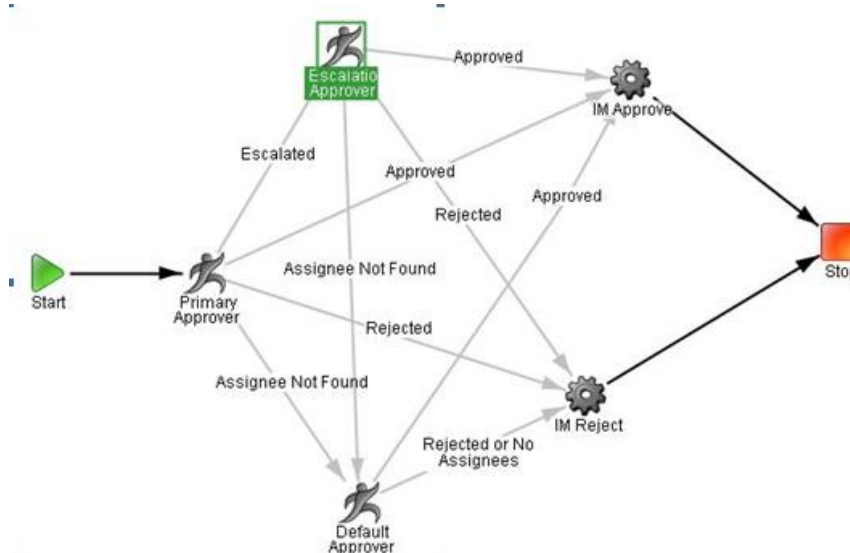


Diagramma del modello EscalationApproval

Nel seguente diagramma viene illustrato il modello di processo EscalationApproval come viene visualizzato in WorkPoint Designer. Il modello di processo include le seguenti attività manuali:

- Un nodo di approvazione per il partecipante primario. Se tale utente approva o rifiuta la richiesta, l'esecuzione del processo viene completata.
- Un nodo di approvazione per il partecipante predefinito. Questo utente può approvare o rifiutare l'attività se il partecipante primario non viene individuato.

- Un nodo di approvazione di transizione programmato dal responsabile dell'approvazione primario al responsabile della riassegnazione. Questo utente può approvare o rifiutare la richiesta se il partecipante primario è disponibile ma non risponde nell'intervallo di tempo predefinito.



Nota: per aggiungere l'opzione di timeout a un processo esistente, aggiungere il campo dei dati utente PARTICIPANT_TIMEOUT al nodo dell'attività e aggiungere la transizione Escalated al nodo desiderato per l'escalation dell'elemento.

Utilizzo del modello di approvazione riassegnazione

Per utilizzare il modello di approvazione riassegnazione è necessario importare manualmente il seguente file durante l'aggiornamento dalla versione r12.5 alla versione r12.5 SP1:

Workflow 12.5 to 12.5 SP1 upgrade.zip

Il file si trova nella cartella workflowScripts, nella cartella degli strumenti di amministrazione.

. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Tipi di resolver partecipanti

Per il metodo basato su modelli, sono disponibili sette tipi di resolver partecipanti:

Membri del ruolo attività di approvazione

Consente di specificare che i partecipanti sono membri dei ruoli che concedono l'accesso all'attività di approvazione.

Elenco utenti

Consente di specificare che i partecipanti sono inclusi in un determinato elenco di utenti.

Membri del gruppo

Consente di specificare che i partecipanti sono membri di un determinato elenco di gruppi.

Membri del ruolo di amministrazione

Consente di specificare che i partecipanti sono membri di un determinato elenco di ruoli di amministrazione.

Membri dell'attività di amministrazione

Consente di specificare che i partecipanti sono membri dei ruoli di amministrazione associati a un determinato elenco di attività di amministrazione.

Resolver dinamico

Consente di specificare che i partecipanti vengono selezionati in modo dinamico in base all'attività o all'evento in fase di approvazione.

Resolver nullo

Viene restituito un elenco nullo non contenente alcun utente.

Personalizzato

Consente di specificare che i partecipanti vengono determinati da un resolver partecipanti personalizzato.

Business Owner Resolver (Resolver del titolare di business)

Specifica l'elenco di partecipanti configurati nella regola di catalogo in qualità di titolari di business di un'entità.

Admin Owner Resolver (Resolver del titolare di amministrazione)

Specifica l'elenco di partecipanti configurati nella regola di catalogo in qualità di proprietari di amministrazione di un'entità.

Manager Resolver (Resolver di gestione)

Specifica il partecipante impostato come manager dell'oggetto Utente.

Membri del ruolo attività di approvazione

Questo resolver assegna l'attività a tutti i membri di tutti i ruoli di CA Identity Manager che concedono l'accesso all'attività di approvazione. Questo tipo di resolver non richiede ulteriori interventi di configurazione.

Elenco di utenti

Questo resolver assegna l'elemento di lavoro a un elenco specifico di utenti.

L'ambito non viene applicato Gli utenti che dispongono dell'accesso alla schermata di configurazione del flusso di lavoro possono aggiungere o rimuovere utenti dall'elenco.

Il resolver prevede le seguenti regole di convalida:

- È necessario fornire almeno un nome utente.
- I nomi utente devono corrispondere agli utenti attualmente esistenti.

Membri del gruppo

Questo resolver assegna l'elemento di lavoro a tutti i membri di tutti i gruppi specificati nell'elenco del gruppo.

La valutazione dei membri del gruppo viene eseguita al momento della creazione dell'elemento di lavoro e non al momento della definizione del resolver dei partecipanti.

L'ambito non viene applicato Gli utenti che dispongono dell'accesso alla schermata di configurazione del flusso di lavoro possono aggiungere o rimuovere gruppi dall'elenco.

Il resolver prevede le seguenti regole di convalida:

- È necessario specificare almeno un gruppo
- I nomi dei gruppi devono corrispondere ai gruppi attualmente esistenti

Membri del ruolo di amministrazione

Questo resolver assegna l'elemento di lavoro a tutti i membri dei ruoli di amministrazione specificati nell'elenco dei ruoli di amministrazione.

La definizione dei membri del ruolo viene eseguita durante la creazione dell'elemento di lavoro e non al momento della definizione del resolver dei partecipanti.

L'ambito non viene applicato Gli utenti che dispongono dell'accesso alla schermata di configurazione del flusso di lavoro possono aggiungere o rimuovere ruoli dall'elenco.

Il resolver prevede le seguenti regole di convalida:

- È necessario specificare almeno un ruolo di amministrazione.
- I nomi del ruolo di amministrazione devono corrispondere ai nomi dei ruoli di amministrazione esistenti.

Membri dell'attività di amministrazione

Questo resolver assegna l'elemento di lavoro a tutti i membri di tutti i ruoli di amministrazione associati alle attività di amministrazione specificate nell'elenco delle attività di amministrazione.

L'ambito non viene applicato. Gli utenti che dispongono dell'accesso alla schermata di configurazione del flusso di lavoro possono aggiungere o rimuovere attività nell'elenco.

La valutazione dei membri del ruolo e dei ruoli presenti nelle attività viene eseguita al momento della creazione dell'elemento di lavoro e non al momento della definizione del resolver dei partecipanti.

Il resolver prevede le seguenti regole di convalida:

- È necessario specificare almeno un'attività di amministrazione.
- I nomi delle attività di amministrazione devono corrispondere alle attività di amministrazione attualmente esistenti.

Resolver dinamico

Questo resolver restituisce un elenco di utenti a seconda della regola dinamica risolta al momento dell'esecuzione. Utilizzare le opzioni descritte di seguito per impostare i vincoli della regola dinamica:

Responsabili dell'approvazione

Consente di specificare il tipo di utente per l'approvazione dell'attività corrente.

Nota: visualizza solo gli oggetti che possono contenere utenti (o revisori).

Utente o oggetto

Consente di specificare l'utente o l'oggetto in cui si trovano i responsabili dell'approvazione.

- Oggetto associato all'evento: evento sottoposto al controllo del flusso di lavoro.
- Iniziatore di questa attività: utente che ha avviato l'attività di amministrazione.
- Oggetto primario di questa attività: oggetto creato/modificato dall'attività.
- Responsabile dell'approvazione dell'attività precedente: il precedente responsabile dell'approvazione di questa attività.

Utente associato con questo account

Aggiorna il campo Attributo utente o oggetto per elencare gli attributi dell'utente CA Identity Manager anziché gli attributi dell'account di endpoint. Il resolver elimina gli attributi al livello di utente CA Identity Manager. Questa casella di controllo si applica quando si seleziona un oggetto dell'account di endpoint, ad esempio un account Active Directory.

Attributo

Consente di specificare l'attributo contenente i responsabili dell'approvazione.

Nota: L'elenco di attributi viene organizzato in ordine alfabetico e contiene un elenco di nomi di visualizzazione univoci. Gli attributi estesi vengono esclusi dall'elenco.

Tipo oggetto evento

Consente di specificare il tipo di oggetto dell'evento.

Nota: questa opzione è visualizzata solo se viene selezionata l'opzione "Oggetto associato all'evento".

Nota: Il resolver dinamico con Crea gruppo richiede l'esistenza dell'oggetto. Le informazioni su amministratori/appartenenza al gruppo possono essere utilizzate solo con resolver dinamici/della corrispondenza dell'attributo per i gruppi esistenti.

Il resolver dinamico è stato potenziato per poter aggiungere il responsabile dell'approvazione precedente all'elenco degli oggetti supportati. Se è selezionato l'attributo fisico che contiene le informazioni sul manager, la configurazione consente l'inoltro dell'approvazione a un manager.

Per configurare il resolver per il resolver dell'approvazione manager:

- Impostare i responsabili dell'approvazione su Utenti
- Selezionare Responsabile dell'approvazione dell'attività precedente dall'elenco a discesa Utente o Oggetto
- Impostare l'attributo sull'attributo fisico che contiene le informazioni sul manager

Resolver di corrispondenza attributi

Questo resolver funziona solo sugli oggetti di tipo Utente. Un valore di qualsiasi oggetto disponibile viene fatto corrispondere ad un campo nell'oggetto utente. Utilizzare le opzioni descritte di seguito per impostare i vincoli della regola di corrispondenza attributi:

Responsabili dell'approvazione

Consente di specificare il tipo di utente per l'approvazione dell'attività corrente.

Utente o oggetto

Specifica il valore che i responsabili dell'approvazione troveranno per l'attributo selezionato di seguito.

Nota: il valore recuperato dall'utente o dall'oggetto deve essere un valore accettabile per una ricerca sull'utente per l'attributo selezionato.

- Oggetto associato all'evento: evento sottoposto al controllo del flusso di lavoro.
- Iniziatore di questa attività: utente che ha avviato l'attività di amministrazione.
- Oggetto primario di questa attività: oggetto creato/modificato dall'attività (disponibile solo per il mapping degli eventi a livello di attività).
- Responsabile dell'approvazione dell'attività precedente: il precedente responsabile dell'approvazione di questa attività.

Utente associato con questo account

Aggiorna il campo Attributo utente o oggetto per elencare gli attributi dell'utente CA Identity Manager anziché gli attributi dell'account di endpoint. Il resolver elimina gli attributi al livello di utente CA Identity Manager. Questa casella di controllo si applica quando si seleziona un oggetto dell'account di endpoint, ad esempio un account Active Directory.

Attributo Utente o oggetto

Specifica l'attributo che contiene il valore da utilizzare nella ricerca dei responsabili dell'approvazione.

Attributo di ricerca del responsabile dell'approvazione

Consente di specificare l'attributo da utilizzare nella ricerca per la corrispondenza al valore identificato in precedenza.

Nota: Quando si imposta l'attività Approva Crea utente come resolver della corrispondenza dell'attributo che funzioni su utenti e resolver partecipanti, è necessario modificare la firma del metodo perché lo script imApprovers in WorkPoint Designer punti al nome univoco di TwoStageProcessDefinition.

Resolver nullo

Il resolver nullo non restituisce alcun utente. A seconda della progettazione del processo del flusso di lavoro, il processo può evitare interamente l'approvazione. Il resolver nullo non richiede alcuna ulteriore configurazione.

Resolver partecipanti personalizzato

Il resolver partecipanti personalizzato è un oggetto Java che determina i partecipanti dell'attività del flusso di lavoro e restituisce un elenco a CA Identity Manager. Tale elenco viene quindi passato al motore del flusso di lavoro. In genere, viene sviluppato un resolver partecipanti personalizzato solo se i criteri partecipanti standard non sono in grado di fornire l'elenco di partecipanti richiesti da un'attività.

Nota: Creare un resolver partecipanti personalizzato utilizzando l'API relativa ai resolver partecipanti. Per ulteriori informazioni, consultare la *Programming Guide for Java*.

Impostazione di un criterio di posta elettronica per un processo del flusso di lavoro

È possibile specificare un criterio di posta elettronica per ciascuna fase del processo del flusso di lavoro. In base al criterio di posta elettronica definito, viene inviato messaggio di posta elettronica quando un processo raggiunge la fase o l'attività corrispondente. Per le notifiche di posta elettronica relative al processo del flusso di lavoro, è possibile selezionare unicamente il tipo *Invia messaggi con stato: Indirizzo di posta elettronica - Flusso di lavoro in sospeso*.

Nota: Per ulteriori informazioni sui criteri di posta elettronica, consultare la sezione Creazione di criteri della notifica di posta elettronica.

Esempio di flusso di lavoro: creazione di utenti

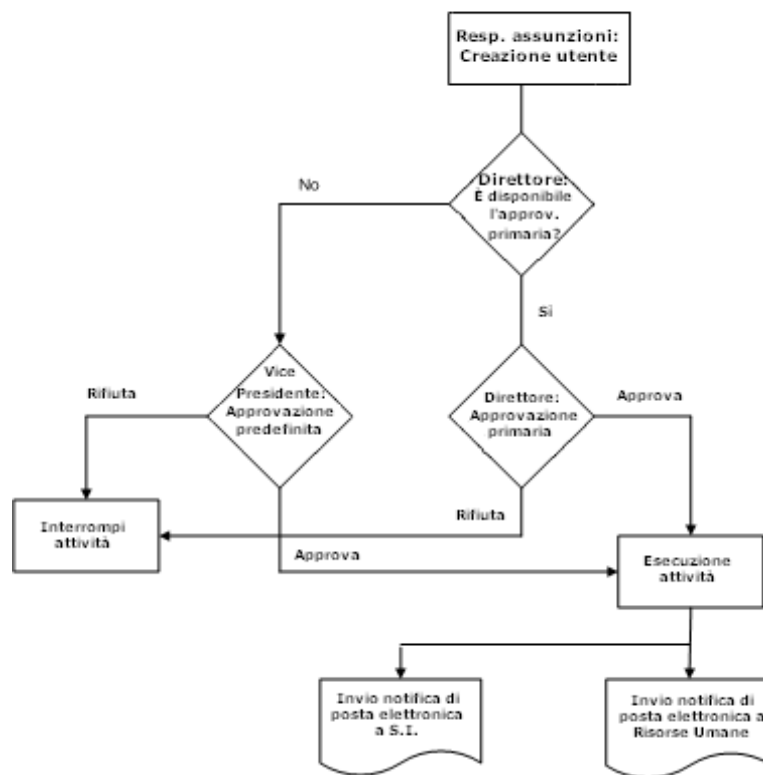
L'amministrazione di CA Identity Manager di una società deve definire un flusso di lavoro ed i ruoli utente per la gestione del seguente scenario:

- Il responsabile vendite della società assume un nuovo rappresentante. Il responsabile vendite deve essere in grado di creare un utente CA Identity Manager per questa nuova assunzione.
- Per semplificare il processo di assunzione, i partecipanti devono eseguire un unico elemento di lavoro per approvare (o rifiutare) l'attività.
- Il direttore vendite deve essere il revisore primario di tutte le nuove assunzioni. Se il direttore vendite non è in grado di eseguire questa attività per qualsiasi motivo, il vicedirettore vendite viene impostato come revisore predefinito.
- Se la nuova assunzione viene approvata, ai reparti Risorse umane (HR) e Servizi informativi (IS) viene inviata tramite posta elettronica una notifica di creazione di un nuovo utente.

Diagramma di controllo relativo alla creazione di utenti

Nel seguente diagramma viene illustrato il flusso logico dello scenario di creazione degli utenti.

Esempio di flusso di lavoro del livello attività: Creazione utente



Implementazione dell'esempio di flusso di lavoro

Per implementare questo scenario di esempio, l'amministratore deve eseguire le seguenti attività:

- Accertarsi che l'iniziatore dell'attività sia membro del ruolo di amministrazione richiesto.

Il responsabile vendite deve essere membro del ruolo di amministrazione Gestore utente. Questo ruolo conferisce al responsabile vendite l'autorità necessaria per avviare l'attività di amministrazione Crea utente per la nuova assunzione di un rappresentante.

- Attivare il flusso di lavoro a livello di attività per l'attività di amministrazione Crea utente.

Il flusso di lavoro a livello di attività garantisce la generazione di un unico elemento di lavoro per il completamento dell'attività Crea utente. Poiché all'attività Crea utente sono associati numerosi eventi specifici, il flusso di lavoro a livello di evento genererà più elementi di lavoro e risulterà pertanto più complesso da configurare.

- Configurare i resolver partecipanti.

Il numero di possibili resolver partecipanti è determinato dal modello di processo del flusso di lavoro selezionato. Il modello SingleStageApproval include revisori primari e predefiniti, mentre gli altri modelli ne prevedono un numero maggiore.

Poiché questo scenario ne prevede solo due, il resolver partecipanti Elenco utenti rappresenta la soluzione più semplice. Questo resolver consente la selezione di singoli revisori per nome, anziché la selezione di più utenti in base al ruolo o al gruppo.

- Configurare le notifiche tramite posta elettronica.

La console di gestione consente di configurare la notifica via posta elettronica per attività ed eventi specifici. Per questo scenario, i messaggi di posta elettronica relativi all'attività sono abilitati. Vengono pertanto inviate notifiche via posta elettronica non appena l'attività Crea utente viene completata.

È necessario utilizzare un modello di posta elettronica personalizzato per inviare le notifiche via posta elettronica ai dipartimenti HR ed IS con una riga dell'oggetto ed il testo del messaggio appropriati.

Ulteriori informazioni

[Notifiche di posta elettronica](#) (a pagina 361)

[Colloca le attività di amministrazione sotto il controllo del flusso di lavoro - metodo basato su modelli](#) (a pagina 268)

[Procedura di configurazione del flusso di lavoro a livello di attività](#) (a pagina 271)

Utilizzo del metodo WorkPoint

Il metodo WorkPoint è valido per le versioni precedenti alla r12 di CA Identity Manager. Sono disponibili 14 processi predefiniti del flusso di WorkPoint che per impostazione predefinita sono mappati a eventi di CA Identity Manager specifici. È necessario utilizzare WorkPoint Designer per configurare i resolver partecipanti e modificare eventualmente i processi del flusso di lavoro.

Il metodo WorkPoint richiede inoltre l'utilizzo della console di gestione per il mapping di un processo del flusso di lavoro su un evento di approvazione per impostare il controllo dell'attività corrispondente da parte del flusso di lavoro a livello globale all'interno dell'ambiente specifico.

In questa sezione vengono descritte le procedure avanzate per impostare il controllo delle attività di amministrazione da parte del flusso di lavoro mediante l'utilizzo del metodo WorkPoint.

Nota: per ottimizzare la flessibilità e semplificarne l'utilizzo, CA consiglia di utilizzare il metodo basato su modelli, laddove possibile.

Per utilizzare il metodo WorkPoint

1. [Configurare gli strumenti di amministrazione di WorkPoint.](#) (a pagina 288)
2. Nella console di gestione:
 - a. Assicurarsi che il flusso di lavoro sia abilitato per l'ambiente selezionando la casella di controllo Attivato in Impostazioni avanzate, Flusso di lavoro.
Nota: i mapping degli eventi visualizzati in questa schermata sono validi solo se si utilizza il metodo WorkPoint per configurare il flusso di lavoro. Se si utilizza il metodo basato su modelli (opzione consigliata), non eseguire il mapping degli eventi ai processi utilizzando questa console di gestione.
 - b. (Facoltativo) Per il mapping globale degli eventi, associare uno o più eventi al processo del flusso di lavoro predefinito appropriato.
 - c. Se necessario, riavviare l'ambiente CA Identity Manager.
3. Nella console utente:
 - a. Per il mapping a livello di attività degli eventi, associare uno o più eventi al processo del flusso di lavoro predefinito appropriato. (facoltativo).
4. In WorkPoint Designer:
 - a. Associare un'attività di approvazione ad un processo del flusso di lavoro (facoltativo).
 - b. Configurare i resolver partecipanti con un processo del flusso di lavoro (facoltativo).
5. Nella console utente:
 - a. Dopo aver configurato il controllo del flusso di lavoro, l'utente associato al ruolo appropriato esegue l'attività di amministrazione.
 - b. Il partecipante del flusso di lavoro designato approva o rifiuta l'evento.

Ulteriori informazioni:

[Mapping dei processi agli eventi](#) (a pagina 294)

[Associazione di un'attività del flusso di lavoro ad un'attività di approvazione](#) (a pagina 299)

[Resolver partecipanti: metodo WorkPoint](#) (a pagina 300)

Configurazione degli strumenti di amministrazione di WorkPoint

WorkPoint Designer è un software sviluppato da Workpoint LLC, una consociata di Planet Group, Inc., che è integrato in CA Identity Manager. WorkPoint Designer consente di gestire i processi e le singole attività del flusso di lavoro. Gli strumenti di amministrazione di WorkPoint includono WorkPoint Designer e WorkPoint Archive. Per configurare gli strumenti di amministrazione di WorkPoint, installare Strumenti di amministrazione di CA Identity Manager. Se gli strumenti di amministrazione di CA Identity Manager non sono installati, è possibile eseguire il programma di installazione e selezionare l'opzione Strumenti di amministrazione di CA Identity Manager.

Nota: per utilizzare Strumenti di amministrazione per il flusso di lavoro, è necessario che sia installato un JDK supportato nel sistema in cui sono installati gli strumenti di amministrazione. Per un elenco completo delle piattaforme e delle versioni supportate, vedere la Matrice di supporto di CA Identity Manager sul [sito del Supporto tecnico di CA Identity Manager](#).

Gli strumenti del client del flusso di lavoro sono posti nella directory WorkPoint degli strumenti amministrativi di CA Identity Manager. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Gli strumenti in questa directory consentono di effettuare le operazioni seguenti:

- Creare lo schema di database del flusso di lavoro
- Caricare gli script predefiniti del flusso di lavoro
- Progettare e monitorare i processi del flusso di lavoro

Configurazione degli strumenti di amministrazione WorkPoint in JBoss

Per configurare gli strumenti di amministrazione WorkPoint in JBoss, modificare i file `init.bat/sh` e `workpoint-client.properties`.

Modifica di init.bat/init.sh

Per modificare init.bat/init.sh

1. In un editor di testo modificare uno dei file seguenti:
 - **Windows:**
`admin_tools\Workpoint\bin\init.bat`
 - **UNIX:**
`admin_tools/Workpoint/bin/init.sh`
2. Rimuovere il commento dalla riga EJB_CLASSPATH nella sezione JBoss del file.
Nota: verificare che tutte le sezioni per altri server di applicazioni siano prive di commenti.
3. Copiare jbossall-client.jar da `jboss_home\client\` a:
`admin_tools\Workpoint\lib`

Modifica di workpoint-client.properties

Modificare il file workpoint-client.properties in base al tipo di server di applicazioni selezionato durante l'installazione di CA Identity Manager.

Configurazione del file workpoint-client.properties

1. Aprire `admin_tools\Workpoint\conf\workpoint-client.properties` in un editor di testo.
`admin_tools` è la directory in cui sono installati gli strumenti amministrativi. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:
 - **Windows:** `C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools`
 - **UNIX:** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`
2. Individuare la sezione intitolata JBOSS SETTINGS.
3. Rimuovere i commenti da tutti i valori di proprietà in tale sezione.
Ad esempio:
`java.naming.provider.url=localhost`
`java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory`
`java.naming.factory.url.pkgs=org.jboss.naming`
Nota: può essere necessario modificare il valore della proprietà `java.naming.provider.url`. Ad esempio, sostituire `localhost` con `jnp://nome_server o ip:porta`. Assicurarsi di utilizzare il numero di porta jnp 1099.
4. Salvare il file.

Configurazione degli strumenti di amministrazione WorkPoint in WebLogic

Per configurare gli strumenti di amministrazione WorkPoint in WebLogic, modificare i file `init.bat/sh` e `workpoint-client.properties`.

Modifica di `init.bat/init.sh`

Per modificare `init.bat/init.sh`

1. In un editor di testo modificare uno dei file seguenti:
 - **Windows:**
`admin_tools\Workpoint\bin\init.bat`
 - **UNIX:**
`admin_tools/Workpoint/bin/init.sh`
2. Rimuovere i commenti da `EJB_CLASSPATH` nella sezione WebLogic del file:
Nota: verificare che tutte le sezioni per altri server di applicazioni siano prive di commenti.
3. Copiare il file `wlclient.jar` da `directoryprincipale_weblogic\server\lib` nel percorso seguente:
`admin_tools\Workpoint\lib\`

Modifica di `workpoint-client.properties`

Modificare il file `workpoint-client.properties` in base al tipo di server di applicazioni selezionato durante l'installazione di CA Identity Manager.

Configurazione del file `workpoint-client.properties`

1. Aprire `admin_tools\Workpoint\conf\workpoint-client.properties` in un editor di testo.
2. Individuare la sezione WebLogic del file.
3. Rimuovere i commenti da tutti i valori di proprietà in tale sezione.
4. Salvare il file.
Nota: la proprietà `java.naming.provider.url` deve fare riferimento al nome di dominio completo e al numero di porta WebLogic del sistema in cui è installato il server CA Identity Manager.

Configurazione degli strumenti di amministrazione WorkPoint in WebSphere

Per configurare gli strumenti di amministrazione WorkPoint in WebSphere, modificare i file `init.bat/sh` e `workpoint-client.properties`.

Modifica di init.bat/init.sh

Per modificare init.bat/init.sh

1. In un editor di testo modificare uno dei file seguenti:
 - **Windows:**
`admin_tools\Workpoint\bin\init.bat`
 - **UNIX:**
`admin_tools/Workpoint/bin/init.sh`
2. Rimuovere i commenti dalla sezione IBM WebSphere.
Nota: non commentare la voce WP_CLASSPATH nella sezione COMMON WP_CLASSPATH.
3. Nota: verificare che tutte le sezioni per gli altri server di applicazioni contengano commenti.
4. Se necessario, sostituire i valori per JAVA_HOME e WAS_HOME con i percorsi appropriati per l'ambiente in uso.

Modifica di workpoint-client.properties

Modificare il file workpoint-client.properties in base al tipo di server di applicazioni selezionato durante l'installazione di CA Identity Manager.

Configurazione del file workpoint-client.properties

1. Aprire `admin_tools\Workpoint\conf\workpoint-client.properties` in un editor di testo.
`admin_tools` è la directory in cui sono installati gli strumenti amministrativi. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:
 - **Windows:** `C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools`
 - **UNIX:** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`
2. Individuare la sezione intitolata IBM WEBSPPHERE SETTINGS.
3. Rimuovere i commenti da tutti i valori di proprietà in tale sezione.
Ad esempio:

```
java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory
java.naming.provider.url=iiop://localhost:porta_bootstrap
```

Nota: il numero della porta di bootstrap deve corrispondere al numero di porta specificato nella console di amministrazione WebSphere. Per individuare il numero di porta corretto, passare a Server, Endpoint, Indirizzo server bootstrap.

4. Aggiornare la porta BOOTSTRAP_ADDRESS per il profilo WebSphere come segue:
 - a. Nella console di amministrazione di WebSphere passare a Application Servers (Server applicazioni), nome_server, Communications (Comunicazioni).
 - b. Espandere Ports (Porte).
 - c. Modificare il file workpoint-client.properties in iam_im.ear/config.
 - d. Modificare la porta predefinita 2809 nella sezione WebSphere impostando la porta del profilo per BOOTSTRAP_ADDRESS.
5. Salvare il file.

Avvio di WorkPoint Designer

Per avviare WorkPoint Designer, eseguire il seguente file:

- **Windows:** `admin_tools\WorkPoint\bin\Designer.bat`
- **UNIX:** `admin_tools/WorkPoint/bin/Designer.sh`

dove *admin_tools* corrisponde alla directory di installazione degli strumenti di amministrazione di CA Identity Manager. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- **Windows:** `C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools`
- **UNIX:** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`

Nota: prima di poter eseguire WorkPoint Designer, è necessario configurare i componenti del flusso di lavoro installati. Per istruzioni, vedere la sezione "Configurazione degli strumenti di amministrazione di WorkPoint" relativa al proprio server di applicazioni.

Ulteriori informazioni:

[Configurazione degli strumenti di amministrazione WorkPoint in JBoss](#) (a pagina 288)
[Configurazione degli strumenti di amministrazione WorkPoint in WebLogic](#) (a pagina 290)
[Configurazione degli strumenti di amministrazione WorkPoint in WebSphere](#) (a pagina 290)

Processi WorkPoint

In CA Identity Manager è disponibile una serie di processi del flusso di lavoro predefiniti in WorkPoint Designer. È possibile utilizzare i processi predefiniti con i relativi mapping di eventi predefiniti, mappare i processi del flusso di lavoro ad altri eventi, modificare i processi del flusso di lavoro mediante l'aggiunta o la rimozione di attività, nonché creare nuovi processi del flusso di lavoro.

Mapping globale processi/eventi

Il mapping globale di un processo del flusso di lavoro ad un evento può essere o meno basato su criterio.

Per ulteriori informazioni su come mappare un evento ad un processo del flusso di lavoro utilizzando il flusso di lavoro basato su criterio, vedere Mapping globale di eventi a processi del flusso di lavoro basato su criterio.

Nella seguente tabella sono elencati i mapping globali predefiniti tra processi del flusso di lavoro ed eventi. Tali mapping sono specificati nella console di gestione.

Importante: si tratta di mapping globali. Il processo del flusso di lavoro mappato viene eseguito non appena l'evento corrispondente viene generato da qualsiasi attività nell'ambiente.

Processo del flusso di lavoro	Evento mappato
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Nota: per impostazione predefinita, i processi del flusso di lavoro contrassegnati da un asterisco (*) non sono mappati ad alcun evento.

Ulteriori informazioni:

[Mapping di un processo ad un evento a livello globale](#) (a pagina 295)

[Mapping di un processo ad un evento in un'attività specifica](#) (a pagina 296)

Mapping dei processi agli eventi

I processi del flusso di lavoro vengono creati e modificati in WorkPoint Designer. La creazione di un processo del flusso di lavoro per CA Identity Manager in genere è finalizzata a un'attività specifica di CA Identity Manager. L'esecuzione di tale attività viene controllata dal processo del flusso di lavoro.

Oltre a creare il processo del flusso di lavoro, è necessario effettuare le operazioni seguenti:

- Identificare l'evento generato dall'attività di Identity Manager, come descritto in Eventi ed attività di amministrazione. È possibile creare un processo del flusso di lavoro per qualsiasi attività di CA Identity Manager che genera un evento.
 - Mappare il processo del flusso di lavoro ad un evento procedendo in uno dei seguenti modi:
 - Assegnare un processo del flusso di lavoro ad un evento a livello globale.
In seguito a questo mapping globale, il processo del flusso di lavoro viene eseguito quando l'evento viene generato nell'ambiente corrente, indipendentemente dall'attività che lo genera.
 - Assegnare un processo del flusso di lavoro ad un evento generato da un'attività specifica.
In seguito a questo mapping specifico dell'attività, il processo del flusso di lavoro viene eseguito solo quando l'attività specificata genera l'evento.
- Nota:** in caso di mapping di un evento ad un processo del flusso di lavoro sia a livello globale che a livello di attività specifica, il processo del flusso di lavoro associato all'attività specifica ha la priorità assoluta.
- Specificare un resolver partecipanti per l'attività del flusso di lavoro inclusa nel processo del flusso di lavoro.
 - Associare un'attività del flusso di lavoro ad un'attività di approvazione.

Ulteriori informazioni:

[Mapping di un processo ad un evento a livello globale](#) (a pagina 295)

[Mapping di un processo ad un evento in un'attività specifica](#) (a pagina 296)

[Attività del flusso di lavoro](#) (a pagina 298)

[Resolver partecipanti: metodo WorkPoint](#) (a pagina 300)

Mapping di un processo ad un evento a livello globale

Un processo del flusso di lavoro viene mappato ad un evento globalmente in modo tale che tale processo venga eseguito quando l'evento viene generato da qualsiasi attività nell'ambiente.

Per eseguire il mapping di un processo ad un evento a livello globale

1. Aprire la console di gestione immettendo il seguente URL in un browser:

`http://hostname/iam/immanage`

nomehost

Consente di definire il nome di dominio completo del server in cui è installato CA Identity Manager. Ad esempio, server.azienda.com:porta.

2. Fare clic su Ambienti, quindi selezionare il nome dell'ambiente CA Identity Manager appropriato.
3. Fare clic su Impostazioni avanzate, quindi su Flusso di lavoro.
4. Per eseguire il mapping di un evento ad un processo del flusso di lavoro, attenersi alla seguente procedura:
 - a. Selezionare un evento nella casella di riepilogo Eventi.
 - b. Selezionare un processo del flusso di lavoro nella casella di riepilogo Approva processo.
 - c. Fare clic su Aggiungi.
5. Dopo aver eseguito il mapping degli eventi ai processi del flusso di lavoro, fare clic su Salva.
6. Riavviare l'ambiente CA Identity Manager per rendere effettive le modifiche.

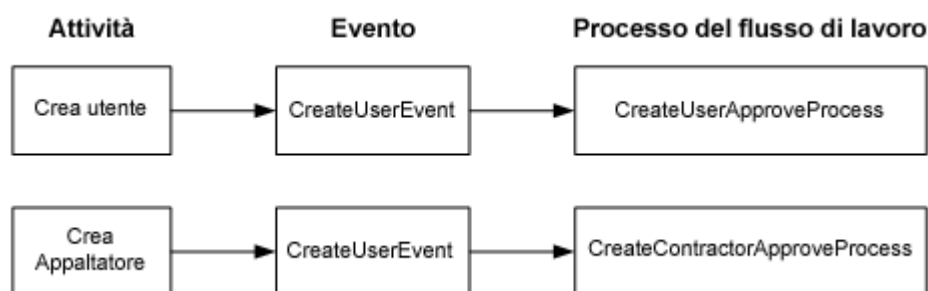
Ulteriori informazioni:

[Mapping globale processi/eventi](#) (a pagina 293)

Mapping di un processo ad un evento in un'attività specifica

È possibile assegnare un processo del flusso di lavoro ad un evento generato da un'attività specifica. In questo caso, il processo del flusso di lavoro viene eseguito solo quando l'evento mappato viene generato dall'attività specificata.

Il mapping a livello di attività fornisce un controllo variabile sui processi del flusso di lavoro che possono essere eseguiti per lo stesso evento. Ad esempio, nel seguente diagramma vengono illustrate due diverse attività che generano lo stesso evento, ma attivano due processi del flusso di lavoro diversi.



In questo diagramma ogni attività utilizza un processo del flusso di lavoro distinto.

Crea utente

Consente di specificare l'attività di amministrazione predefinita che attiva l'evento CreateUserEvent, mappato al processo predefinito CreateUserApproveProcess del flusso di lavoro.

Crea appaltatore

Consente di specificare un'attività personalizzata basata sull'attività crea utente. In questo caso, l'evento CreateUserEvent viene mappato al processo personalizzato CreateContractorApproveProcess del flusso di lavoro creato per approvare gli account dei nuovi appaltatori.

Per eseguire il mapping di un processo del flusso di lavoro ad un evento in un'attività esistente

1. Nella Console utente, selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
2. Cercare un'attività di amministrazione.
3. Selezionare un'attività, ad esempio Modifica utente o Crea utente, quindi fare clic su Seleziona.
4. Nella scheda Eventi selezionare un processo del flusso di lavoro per l'evento incluso nell'attività.

Nota: per visualizzare i nomi degli eventi ed il menu a discesa Processo del flusso di lavoro in questa scheda, è necessario che il flusso di lavoro sia attivato.

5. Utilizzando il menu a discesa Processo del flusso di lavoro assegnare un processo al nome di un evento, quindi fare clic su OK.
6. Fare clic su Invia.
7. Aprire la console di gestione, quindi riavviare l'ambiente CA Identity Manager per rendere effettive le modifiche.

Per eseguire il mapping di un processo del flusso di lavoro ad un evento in una nuova attività

1. Nella Console utente selezionare Ruoli e attività, Attività di amministrazione, Crea attività di amministrazione.
Nota: accertarsi di selezionare un'attività di approvazione del flusso di lavoro esistente, ad esempio Approva Crea gruppo o Approva Crea utente, come modello della nuova attività di approvazione del flusso di lavoro.
2. Nella scheda Profilo immettere le informazioni nei campi appropriati.
3. Nella scheda Eventi selezionare un processo del flusso di lavoro per l'evento incluso nell'attività.
Nota: per visualizzare i nomi degli eventi ed il menu a discesa Processo del flusso di lavoro in questa scheda, è necessario che il flusso di lavoro sia attivato.
4. Utilizzando il menu a discesa Processo del flusso di lavoro assegnare un processo al nome di un evento, quindi fare clic su OK.
5. Fare clic su Invia.
6. Aprire la console di gestione, quindi riavviare l'ambiente CA Identity Manager per rendere effettive le modifiche.

Nota: nell'elenco Processo del flusso di lavoro sono inclusi i processi da utilizzare sia con il metodo basato su modelli che con il metodo WorkPoint:

- Quando si seleziona un processo del metodo basato su modelli (SingleStepApproval oppure TwoStageApprovalProcess), la pagina verrà ingrandita in modo da consentire la configurazione dei resolver partecipanti.
- Se invece si seleziona un metodo WorkPoint, la pagina non verrà ingrandita. I resolver partecipanti vengono configurati in WorkPoint Designer.

Ulteriori informazioni:

[Mapping globale processi/eventi](#) (a pagina 293)

Attività del flusso di lavoro

In CA Identity Manager è disponibile una serie di attività del flusso di lavoro predefinite in WorkPoint Designer. Queste attività vengono assegnate a processi predefiniti del flusso di lavoro.

I processi predefiniti del flusso di lavoro sono processi che si articolano in un unico passaggio, ovvero ogni processo contiene un'unica attività predefinita.

Ogni attività predefinita corrisponde ad un'attività di approvazione del flusso di lavoro avente lo stesso nome precedentemente definito in CA Identity Manager. È possibile utilizzare le attività predefinite in altri processi del flusso di lavoro, nonché creare nuove attività.

È possibile utilizzare i processi predefiniti del flusso di lavoro senza apportarvi nessuna modifica oppure aggiungervi nuove attività. Per informazioni sull'aggiunta di un'attività ad un processo del flusso di lavoro, vedere la documentazione di WorkPoint.

Processi ed attività

Nella seguente tabella sono elencati le attività predefinite del flusso di lavoro ed il processo predefinito del flusso di lavoro a cui ogni attività è assegnata per impostazione predefinita.

Nota: le attività predefinite del flusso di lavoro e le attività di approvazione corrispondenti hanno lo stesso nome.

Processo del flusso di lavoro	Attività del flusso di lavoro
CertifyRoleApprovalProcess**	Approva Certifica ruolo
ConsultationProcess*	
CreateGroupApproveProcess	Approva Crea gruppo
CreateOrganizationApproveProcess	Approva Crea organizzazione
CreateUserApproveProcess	Approva Crea utente
DeleteGroupApproveProcess	Approva Elimina gruppo
DeleteOrganizationApproveProcess	Approva Elimina organizzazione
DeleteUserApproveProcess	Approva Elimina utente
ModifyAccessRoleMembershipApproveProcess	Approva Modifica appartenenza al ruolo di accesso
ModifyAdminRoleMembershipApproveProcess	Approva Modifica appartenenza al ruolo di amministrazione
ModifyGroupMembershipApproveProcess	Approva Modifica appartenenza al gruppo

Processo del flusso di lavoro	Attività del flusso di lavoro
ModifyIdentityPolicySetApproveProcess	Approva Modifica set di criteri di identità
ModifyOrganizationApproveProcess	Approva Modifica organizzazione
ModifyUserApproveProcess	Approva Modifica utente
SelfRegistrationApproveProcess	Approva Registrazione automatica
SingleStepApproval*	
TwoStageApprovalProcess*	

Nota: i processi del flusso di lavoro contrassegnati da un (*) sono destinati all'utilizzo con il metodo basato su modelli. Vengono configurati nella console utente e pertanto non sono associati ad alcuna attività predefinita. Il processo CertifyRoleApprovalProcess (**) è un processo di esempio per illustrare un resolver partecipanti personalizzato.

Associazione di un'attività del flusso di lavoro ad un'attività di approvazione

Per associare un'attività del flusso di lavoro ad un'attività di approvazione del flusso di lavoro, definire una coppia nome/valore in WorkPoint Designer.

Nota: se non si definisce una coppia nome/valore per un'attività del flusso di lavoro, per impostazione predefinita in CA Identity Manager viene utilizzata un'attività con un nome corrispondente all'attività di approvazione.

Per associare un'attività del flusso di lavoro ad un'attività di approvazione

1. Avviare WorkPoint Designer.
2. Fare clic su File, Apri, Processo.
3. Selezionare un processo del flusso di lavoro, quindi fare clic su Apri.
4. Fare clic con il pulsante destro del mouse sul nodo dell'attività nel processo, quindi scegliere Proprietà.
5. Scegliere Testo dal menu a discesa Tipo.
6. Immettere i seguenti valori nella scheda Dati utente:
 - **Nome:** TASK_TAG.
 - **Valore:** nome del tag dell'attività di approvazione.
7. Fare clic su Aggiungi.
8. Fare clic su OK per salvare le modifiche.

Creazione di attività di approvazione per gli endpoint

È possibile creare attività di approvazione per le schermate di gestione account. Per le attività di approvazione delle modifiche agli account, la schermata di approvazione deve essere specifica di un tipo di endpoint, in modo che il responsabile dell'approvazione possa visualizzare i valori modificati. Per creare un'attività di approvazione per attività di creazione o modifica, seguire questa procedura:

Per creare un'attività di approvazione per un endpoint

1. Nella console utente fare clic su Ruoli e attività, Attività di amministrazione, Crea attività di amministrazione.
2. Selezionare "Crea una copia di un'attività amministrativa", utilizzato per la gestione degli account nell'endpoint.

Il nome dovrebbe iniziare con Crea e specificare il nome del tipo di endpoint, ad esempio Crea account Active Directory.

3. Apportare le seguenti modifiche nella scheda Profilo.
4. Modificare il nome della nuova attività.
 - Modificare il tag dell'attività.
 - Modificare l'azione in Approva evento.
5. Apportare le seguenti modifiche nella scheda Schede:
 - a. Rimuovere tutte le schede Relazione.
 - b. Copiare e modificare le schermate di approvazione nelle schede secondo necessità.

Nota: è possibile incorrere in problemi quando si utilizzano le schermate dell'account in un'attività di approvazione ed è possibile che, affinché funzionino in un'attività di approvazione, sia necessario eseguire le modifiche alla schermata dell'account predefinito.

6. Fare clic su Inoltra.

Resolver partecipanti: metodo WorkPoint

Per specificare i partecipanti utilizzando il metodo WorkPoint, definire le seguenti proprietà delle attività in WorkPoint Designer:

- Nome dello script predefinito di CA Identity Manager che consente la comunicazione tra CA Identity Manager e il server del flusso di lavoro. Lo script genera una richiesta a CA Identity Manager relativa ai partecipanti dell'attività, quindi fornisce tale elenco al server del flusso di lavoro.
- Riferimenti a uno o più resolver partecipanti.

Tipi di resolver partecipanti

Anziché immettere un elenco specifico di partecipanti nelle proprietà dell'attività del flusso di lavoro, ai partecipanti viene fatto riferimento mediante un nome arbitrario mappato ad un *resolver partecipanti*.

Per il modello di processo predefinito sono disponibili quattro tipi di resolver partecipanti:

Resolver partecipanti ruoli

Consente di specificare che i partecipanti sono membri di un ruolo specifico.

Resolver partecipanti gruppi

Consente di specificare che i partecipanti sono membri di un gruppo specifico.

Resolver partecipanti personalizzato

Consente di specificare che i partecipanti vengono determinati da un resolver partecipanti personalizzato.

Resolver partecipanti filtri

Consente di specificare che i partecipanti vengono selezionati tramite un filtro di ricerca.

Resolver partecipanti ruoli

Mediante i resolver partecipanti di tipo ruolo, tutti i membri del ruolo vengono recuperati e restituiti come partecipanti.

Se non viene specificato alcun tipo di resolver nel parametro UserData della finestra di dialogo Attività, per impostazione predefinita verrà utilizzato il resolver di tipo ruolo.

Se non si specifica alcun resolver partecipanti nella scheda Dati utente della finestra di dialogo Proprietà attività di WorkPoint, per impostazione predefinita vengono individuati tutti i ruoli disponibili contenenti l'attività di approvazione specificata, quindi tali membri vengono restituiti come partecipanti.

Configurazione dei resolver partecipanti di tipo ruolo

1. Avviare WorkPoint Designer.
2. Fare clic su File, Apri, Processo.
3. Selezionare un processo del flusso di lavoro, quindi fare clic su Apri.
4. Fare clic con il pulsante destro del mouse sul nodo dell'attività nel processo, quindi scegliere Proprietà.
5. Scegliere Testo dal menu a discesa Tipo.

6. Immettere i seguenti valori nella scheda Dati utente:
 - **Nome:** APPROVER_ROLE_NAME
 - **Valore:** nome di un ruolo di ICA Identity Manager, ad esempio Gestore protezione
7. Fare clic su Aggiungi.

Nota: non è necessario che questo ruolo contenga attività di approvazione.
8. Scegliere Testo dal menu a discesa Tipo.
9. Nella scheda Dati utente immettere la seguente coppia nome/valore (facoltativo):

Valore: APPROVERS_REQUIRED

Valore: YES
10. Fare clic su Aggiungi.

Nota: l'impostazione di approvazione predefinita è APPROVERS_REQUIRED=NO. In questo caso, un'attività viene approvata automaticamente se non vengono individuati partecipanti.

Se l'impostazione è APPROVERS_REQUIRED=YES e non vengono rilevati partecipanti, l'attività non viene completata correttamente.
11. Fare clic su OK per salvare le modifiche.

Resolver partecipanti gruppi

Mediante i resolver partecipanti di tipo gruppo, tutti i membri del gruppo vengono recuperati e restituiti come partecipanti.

Configurazione dei resolver partecipanti di tipo gruppo

1. Avviare WorkPoint Designer.
2. Fare clic su File, Apri, Processo.
3. Selezionare un processo del flusso di lavoro, quindi fare clic su Apri.
4. Fare clic con il pulsante destro del mouse sul nodo dell'attività nel processo, quindi scegliere Proprietà.
5. Scegliere Testo dal menu a discesa Tipo.
6. Immettere i seguenti valori nella scheda Dati utente:
 - **Nome:** APPROVER_GROUP_UNIQUENAME
 - **Valore:** nome di un gruppo di CA Identity Manager
7. Fare clic su Aggiungi.
8. Scegliere Testo dal menu a discesa Tipo.

9. Nella scheda Dati utente immettere la seguente coppia nome/valore (facoltativo):

- **Nome:** APPROVERS_REQUIRED

- **Valore:** YES

10. Fare clic su Aggiungi.

Nota: l'impostazione di approvazione predefinita è APPROVERS_REQUIRED=NO. In questo caso, un'attività viene approvata automaticamente se non vengono individuati partecipanti.

Se l'impostazione è APPROVERS_REQUIRED=YES e non vengono rilevati partecipanti, l'attività non viene completata correttamente.

11. Fare clic su OK per salvare le modifiche.

Resolver partecipanti personalizzati

Il resolver partecipanti personalizzato è un oggetto Java che determina i partecipanti dell'attività del flusso di lavoro e restituisce un elenco a CA Identity Manager. Tale elenco viene quindi passato al motore del flusso di lavoro. In genere, viene sviluppato un resolver partecipanti personalizzato solo se i criteri partecipanti standard non sono in grado di fornire l'elenco di partecipanti richiesti da un'attività.

Nota: creare un resolver partecipanti personalizzato utilizzando l'API relativa ai resolver partecipanti. Per ulteriori informazioni, vedere la *Programming Guide for Java*.

Per configurare un resolver partecipanti personalizzato

1. Aprire la console di gestione immettendo il seguente URL in un browser:

`http://hostname/iam/immanage`

nomehost

Consente di definire il nome di dominio completo del server in cui è installato CA Identity Manager. Ad esempio, server.azienda.com:porta.

2. Fare clic su Ambienti, quindi selezionare il nome dell'ambiente CA Identity Manager appropriato.
3. Fare clic su Impostazioni avanzate, Resolver partecipanti flusso di lavoro.

4. Nella schermata Resolver partecipanti flusso di lavoro fare clic su Nuovo, quindi immettere:

Nome

Consente di specificare il nome del resolver partecipanti personalizzato, ad esempio APPROVER_CUSTOMRESOLVER_NAME

Descrizione

Consente di specificare una descrizione del resolver partecipanti personalizzato.

Classe

Consente di specificare il nome della classe Java, ad esempio com.netegrity.samples.GroupFinder

5. Fare clic su Salva.
6. Avviare WorkPoint Designer.
7. Fare clic su File, Apri, Processo.
8. Selezionare un processo del flusso di lavoro, quindi fare clic su Apri.
9. Fare clic con il pulsante destro del mouse sul nodo dell'attività nel processo, quindi scegliere Proprietà.
10. Scegliere Testo dal menu a discesa Tipo.
11. Immettere i seguenti valori nella scheda Dati utente:

Nome

Consente di specificare il nome del resolver partecipanti personalizzato. Questo nome deve corrispondere al nome specificato nella schermata Resolver partecipanti di tipo personalizzato nella console di gestione di CA Identity Manager, ad esempio:

APPROVER_CUSTOMRESOLVER_NAME

Valore

Consente di specificare un nome univoco per il resolver personalizzato, ad esempio GroupFinder.

12. Fare clic su Aggiungi.

Nota: l'impostazione di approvazione predefinita è APPROVERS_REQUIRED=NO. In questo caso, un'attività viene approvata automaticamente se non vengono individuati partecipanti.

Se l'impostazione è APPROVERS_REQUIRED=YES e non vengono rilevati partecipanti, l'attività non viene completata correttamente.

13. Fare clic su OK per salvare le modifiche.

Resolver partecipanti filtri

Un resolver partecipanti filtri consente a CA Identity Manager di individuare gli utenti o i gruppi corrispondenti ai criteri di filtro. Dopo aver specificato un filtro di ricerca in WorkPoint Designer, in CA Identity Manager verranno restituiti i revisori corrispondenti per l'attività del flusso di lavoro appropriata.

Creare un resolver partecipanti filtri nella scheda Dati utente della finestra di dialogo Proprietà attività di WorkPoint.

Sintassi dei resolver partecipanti filtri

Per creare un filtro di ricerca, è necessario utilizzare una combinazione dei seguenti tre attributi obbligatori:

- Attributo Revisore, ad esempio title
- Operatore dell'attributo Revisore, ad esempio equals
- Valore dell'attributo Revisore, ad esempio manager

Gli attributi obbligatori del filtro di ricerca vengono combinati nel seguente ordine:

attributo operatore valore

Ad esempio:

title equals manager o department contains payroll

Attributi obbligatori per i resolver partecipanti filtri

Di seguito sono riportati gli attributi *obbligatori* del filtro resolver partecipanti:

Nota: per ogni filtro, n rappresenta un numero intero positivo indicante il numero di filtro di ricerca. Il valore predefinito è 1.

APPROVER_FILTER_n_ATTRIBUTE

Consente di specificare l'attributo Revisore. Ad esempio, Titolo, Dipartimento, ID utente. Le stringhe relative al nome dell'attributo Revisore devono corrispondere alle stringhe dei nomi degli attributi utente di CA Identity Manager.

APPROVER_FILTER_n_OP

Consente di specificare l'operatore associato all'attributo Revisore. Ad esempio, equals, not_equals o contains. Le parole chiave relative agli operatori non fanno distinzione tra maiuscole e minuscole.

Di seguito sono indicate le voci valide per questo filtro:

- EQUALS
- STARTSWITH

- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

Consente di specificare il valore associato all'attributo Revisore. Ad esempio, manager (responsabile), payroll (paghe), engineering (tecnico).

Attributi facoltativi per i resolver partecipanti filtri

Di seguito sono riportati gli attributi *facoltativi* del filtro resolver partecipanti.

APPROVER_OBJECTTYPE

USER o GROUP (nessuna distinzione tra maiuscole e minuscole)

Il valore predefinito è USER.

APPROVER_ORG_UNIQUENAME

Nome univoco dell'organizzazione di un revisore. Le stringhe relative al nome dell'organizzazione devono corrispondere alle stringhe dei nomi delle organizzazioni di Identity Manager.

L'impostazione predefinita è l'utente root.

APPROVER_ORG_AND_LOWER

Organizzazione o organizzazioni secondarie del revisore:

- 0 indica la ricerca all'interno dell'organizzazione del revisore.
- 1 indica la ricerca in tutte le organizzazioni secondarie dell'organizzazione del revisore.

Il valore predefinito è 1.

APPROVER_FILTER_NO

Numero di filtri di ricerca in uso. In caso di utilizzo di due filtri, questo numero sarà 2.

Il valore predefinito è 1.

Nota: questo filtro è necessario se il numero di filtri è maggiore di uno.

APPROVER_FILTER_n_CONJ_TYPE

È possibile combinare i filtri di ricerca utilizzando l'operatore OR o AND.

Nota: i filtri separati dall'operatore OR hanno la precedenza su quelli separati dall'operatore AND.

Ad esempio, è possibile specificare l'operatore AND per ricerche del tipo "title equals manager" AND "department equals development."

Nota: n rappresenta un numero intero positivo maggiore di 1 indicante il numero di filtri di ricerca.

Aggiunta di un filtro per i resolver partecipanti

Per aggiungere filtri relativi ai resolver partecipanti

1. Avviare WorkPoint Designer.
2. Fare clic su File, Apri, Processo.
3. Selezionare un processo del flusso di lavoro, quindi fare clic su Apri.
4. Fare clic con il pulsante destro del mouse sul nodo dell'attività nel processo, quindi scegliere Proprietà.
5. Scegliere Testo dal menu a discesa Tipo.
6. Immettere i seguenti valori nella scheda Dati utente:
 - **Nome:** APPROVER_FILTER_1_ATTRIBUTE
 - **Valore:** identificativo univoco del ruolo, ad esempio "title".
7. Fare clic su Aggiungi.
8. Ripetere i passaggi 6 e 7 per ogni attributo incluso nel filtro di ricerca.

Nota: l'impostazione di approvazione predefinita è APPROVERS_REQUIRED=NO. In questo caso, un'attività viene approvata automaticamente se non vengono individuati partecipanti.

Se l'impostazione è APPROVERS_REQUIRED=YES e non vengono rilevati partecipanti, l'attività non viene completata correttamente.

9. Fare clic su OK per salvare le modifiche.

Esempio: resolver partecipanti filtri

L'archivio utenti illustrato nella seguente tabella contiene quattro utenti (Maria, Sara, Mario e Davide) associati agli attributi ID utente (User ID), Titolo (Job Title) e Reparto (Department).

User	ID	Titolo	Dipartimento
Maria	admin1	sysadmin	administration

User	ID	Titolo	Dipartimento
Sara	test1	sysadmin	development
John	admin2	manager	development
Davide	admin3	sysadmin	accounting

I tre filtri definiti nella seguente tabella vengono applicati all'archivio utenti precedente.

Nome	Valore
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	equals
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	department
APPROVER_FILTER_2_OP	equals
APPROVER_FILTER_2_VALUE	administration
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	equals
APPROVER_FILTER_3_VALUE	sysadmin

I filtri vengono applicati nella sequenza specificata di seguito:

1. Vengono valutati il secondo e il terzo filtro collegato dall'operatore OR.
"department equals administration" OR "title equals sysadmin"
Mario viene escluso, ma vengono restituiti Maria, Sara e Davide.
2. Vengono valutati il primo e il secondo filtro collegati dall'operatore AND, dove * è un carattere jolly.
"uid equals admin*" AND "department equals administration"
Sara viene esclusa, ma vengono restituiti Maria e Davide.

Gli utenti finali restituiti dall'archivio utenti sono Maria e Davide.

Ordine di priorità dei resolver partecipanti

Se non viene specificato alcun resolver partecipanti, per impostazione predefinita Identity Manager individua tutti i ruoli disponibili contenenti l'attività di approvazione e restituisce i membri di tali ruoli come partecipanti.

Se invece vengono specificati più resolver partecipanti, Identity Manager li valuta in base al seguente ordine di priorità:

1. Personalizzata
2. Ruolo
3. Filtro
4. Gruppo

Identity Manager identifica ed applica il primo resolver rilevato in base a questo ordine di priorità, quindi ignora tutti i rimanenti resolver successivi.

È possibile disporre solo di un resolver alla volta. Accertarsi inoltre che il resolver sia configurato nel modo appropriato per consentire ad Identity Manager di identificare correttamente i partecipanti.

Impostazione dello script delle risorse del flusso di lavoro

Identity Manager viene fornito con uno script, denominato Revisori IM, che consente l'interscambio di informazioni tra Identity Manager ed il server del flusso di lavoro.

Quando per un'attività del flusso di lavoro è necessario specificare un elenco di partecipanti, lo script passa ad Identity Manager il nome dell'attività, l'identificativo del partecipante specificato nella scheda Dati utente nella finestra di dialogo Proprietà attività di WorkPoint e qualsiasi altra informazione immessa nella scheda Dati utente. Identity Manager cerca i partecipanti e li passa sotto forma di elenco allo script. Lo script provvede quindi a fornire tale elenco al server del flusso di lavoro.

Se si dispone di una nuova definizione del processo del flusso di lavoro e l'attività del processo del flusso di lavoro è un'attività di approvazione del flusso di lavoro di Identity Manager, lo script Revisori IM deve essere specificato nella scheda Risorse della finestra di dialogo Proprietà attività di WorkPoint.

Per specificare lo script Revisori IM in WorkPoint Designer

1. Nella scheda Risorse fare clic su Seleziona.
2. Nella finestra di dialogo Seleziona risorse selezionare Regola nell'elenco a discesa. In questo modo vengono elencate le regole (script) che è possibile associare all'attività.

3. Selezionare il nome dello script (Revisori IM), quindi fare clic su Aggiungi.
4. Fare clic su OK, quindi su Applica nella finestra di dialogo Proprietà attività.

Nota: non modificare lo script Revisori IM.

Impostazione dei partecipanti per le attività Certifica utente

Le attività Certifica utente generano l'evento CertifyRoleEvent. Questo evento può essere sottoposto all'approvazione del flusso di lavoro mediante il processo predefinito CertifyRoleApproveProcess.

In Identity Manager è inoltre disponibile il resolver partecipanti predefinito CertifyRoleParticipantResolver, che viene visualizzato nell'ambiente corrente per impostazione predefinita. I partecipanti delle attività incluse in un processo CertifyRoleApprovalProcess vengono specificati mediante il resolver CertifyRoleParticipantResolver.

Per fornire le informazioni di configurazione dei partecipanti

1. Aprire la console di gestione immettendo il seguente URL in un browser:

`http://hostname/iam/immanage`

nomehost

Consente di definire il nome di dominio completo del server in cui è installato CA Identity Manager. Ad esempio, server.azienda.com:porta.

2. Fare clic su Ambienti, quindi selezionare il nome dell'ambiente CA Identity Manager appropriato.
3. Fare clic su Impostazioni avanzate, quindi su Varie.
4. Definire le coppie nome/valore che specificano i revisori per ogni ruolo da certificare:
 - Nel campo Proprietà utilizzare il formato: *tipo ruolo.nome ruolo*
tipo ruolo deve essere uno dei seguenti ruoli: admin, access, provisioning.
nome ruolo corrisponde al nome di qualsiasi ruolo esistente.
Il nome e il tipo di ruolo devono essere separati da un punto (.).
 - Nel campo Valore specificare gli ID dei revisori separandoli con un punto e virgola (;).

Nell'esempio seguente la certificazione degli utenti può essere approvata per i seguenti ruoli e dai seguenti partecipanti:

- jsmith01 e ajones19 possono approvare la certificazione per il ruolo Gestore utente
- plewis12 è l'unico revisore del ruolo Gestore sistema
- rtrevor8 e pkitt3 possono approvare la certificazione di Ruolo di accesso personale

Proprietà	Valore
admin.Gestore utente	jsmith01;ajones19
admin.Gestore sistema	plewis12
access.Ruolo di accesso personale	rtrevor8;pkitt3

Nota: qualsiasi ruolo non specificato non disporrà di revisori per un evento CertifyRoleEvent.

Processi in WorkPoint Designer

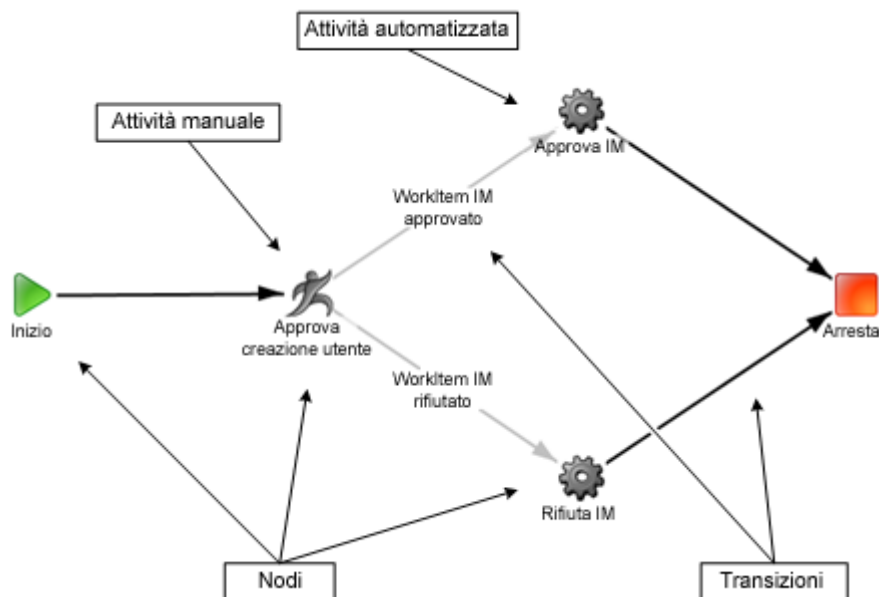
In WorkPoint Designer è possibile personalizzare i processi e le attività predefiniti del flusso di lavoro disponibili in Identity Manager, nonché crearne di nuovi.

In questo argomento vengono fornite informazioni sul flusso di lavoro di WorkPoint che interessano Identity Manager. Per ulteriori informazioni, vedere la documentazione di WorkPoint Designer.

Nota: durante la creazione di un processo del flusso di lavoro, creare una copia di un processo di Identity Manager esistente, quindi modificare il nuovo processo in base alle specifiche esigenze. Un processo del flusso di lavoro creato in questo modo include gli elementi e i nodi predefiniti specifici di Identity Manager, ad esempio gli script di transizione e le attività automatizzate.

Diagramma del processo di WorkPoint

Nel seguente diagramma è illustrato un tipico processo del flusso di lavoro basato su un numero minimo di componenti di un processo che controlla un'attività di Identity Manager. Nel diagramma si fa riferimento al processo predefinito CreateUserApproveProcess, che controlla l'esecuzione di un'attività Crea utente.



Componenti del processo di WorkPoint

Il processo del flusso di lavoro contiene i nodi e le transizioni seguenti:

Inizio

Ogni processo del flusso di lavoro inizia con questo nodo.

Fine

Ogni processo del flusso di lavoro termina con questo nodo.

Attività manuale

Un'attività manuale richiede l'approvazione o il rifiuto di un'attività di Identity Manager da parte di un partecipante e deve avere lo stesso nome dell'attività di approvazione del flusso di lavoro di Identity Manager.

Un processo del flusso di lavoro che controlla un'attività di Identity Manager deve includere almeno un'attività manuale che richieda l'approvazione per tale attività.

Attività automatizzata

Ad un'attività automatizzata viene assegnato uno dei seguenti due script:

- Notifica approvazione IM: informa Identity Manager di eseguire l'attività di Identity Manager sottoponendola al controllo del flusso di lavoro.
- Notifica rifiuto IM: informa Identity Manager di annullare l'esecuzione dell'attività di Identity Manager.

In genere, lo script Notifica approvazione IM viene attivato se vengono approvate tutte le attività manuali, mentre lo script Notifica rifiuto IM viene attivato se viene rifiutata una qualsiasi attività manuale.

Transizione non condizionale

Una transizione non condizionale è un percorso da un nodo ad un altro all'interno del processo del flusso di lavoro. Questo tipo di transizione non è associato ad uno script basato su una condizione.

Transizione condizionale

Una transizione condizionale è un percorso alternativo da un nodo ad un altro all'interno del processo del flusso di lavoro. Questo tipo di transizione è associato ad uno script basato su una condizione.

Uno script basato su una condizione determina se la transizione ha luogo mediante l'analisi del risultato dell'attività associata. Se lo script restituisce True, la transizione viene eseguita ed il processo passa al successivo nodo indicato.

È possibile che due o più script di questo tipo restituiscano True. In questo modo è possibile che un'attività venga eseguita in parallelo, dal momento che ogni script è associato ad una transizione diversa.

Nota: è possibile utilizzare script personalizzati nelle transizioni condizionali. Per ulteriori informazioni, vedere la *Guida alla programmazione per Java*.

Proprietà delle attività manuali

Nella seguente tabella sono elencate le impostazioni delle proprietà specifiche di Identity Manager. Queste impostazioni vengono definite nelle specifiche schede disponibili nella finestra di dialogo Proprietà attività di WorkPoint.

Scheda Proprietà	Descrizione della proprietà
Risorse	Revisori IM: specificato nell'elenco di inclusione. Questo script consente l'interscambio di informazioni tra Identity Manager ed il server del flusso di lavoro.
Agenti	Completamento automatico per nessun partecipante: specificato nell'elenco asincrono ed associato allo stato disponibile. Questo script consente di determinare se un'attività deve essere considerata approvata se non esistono partecipanti dell'attività.

Scheda Proprietà	Descrizione della proprietà
Dati utente	Definire le coppie nome/valore utilizzate da Identity Manager per recuperare i partecipanti dell'attività. Facoltativamente, è inoltre possibile definire i dati da passare ad un resolver partecipanti personalizzato.

Proprietà delle transizioni condizionali

Gli script predefiniti riportati di seguito sono disponibili nella scheda Condizione della finestra di dialogo Proprietà transizione:

Elemento di lavoro IM approvato

Restituisce True se l'attività associata viene approvata. Il processo del flusso di lavoro passa al successivo nodo indicato dalla transizione.

Elemento di lavoro IM rifiutato

Restituisce True se l'attività associata viene rifiutata. Il processo del flusso di lavoro passa al successivo nodo indicato dalla transizione.

Processi ed istanze di processi

Un *processo del flusso di lavoro* definisce le fasi che devono essere completate prima che Identity Manager sia in grado di completare un'attività specifica. Un *processo* è un'istanza runtime di un processo del flusso di lavoro.

Ad esempio, il processo predefinito CreateUserApproveProcess del flusso di lavoro definisce le fasi che devono essere completate per l'approvazione di un nuovo utente. Quando un nuovo utente viene creato in Identity Manager e l'attività viene inoltrata per l'approvazione, in WorkPoint Designer viene creata un'istanza del processo CreateUserApproveProcess.

È possibile aprire, visualizzare e modificare i processi in WorkPoint Designer utilizzando un'interfaccia molto simile a quella utilizzata per modificare i processi del flusso di lavoro.

È possibile che esistano contemporaneamente più processi basati sullo stesso processo.

Filtri dei processi

In WorkPoint Designer è disponibile la funzionalità di applicazione di filtri, che consente di cercare processi in base a vari criteri. Ad esempio, è possibile cercare processi che:

- Sono basati su uno o più processi del flusso di lavoro selezionati
- Dispongono di un riferimento definito dall'utente o un ID processo univoco

- Sono associati ad uno stato specifico, ad esempio Attivo, Completato o Sospeso
- Sono stati creati o avviati all'interno di un intervallo di date specificato

Nota: per istruzioni ed informazioni di riferimento sull'applicazione di filtri ai processi, vedere la documentazione di WorkPoint Designer.

Stato e proprietà dei processi

Quando viene aperto un processo, viene visualizzato il diagramma del flusso di lavoro associato a tale processo. I nodi e le transizioni delle attività del flusso di lavoro vengono visualizzati in colori specifici ad indicare se sono stati eseguiti o meno.

È possibile visualizzare ed in alcuni casi modificare:

- Le proprietà di un processo, comprese le informazioni relative alla cronologia di partecipanti e processi
- Lo stato di un processo aperto, ad esempio se è stato completato o meno
- Proprietà di nodi e transizioni specifiche all'interno di un processo

Proprietà di attività ed elementi di lavoro

È possibile visualizzare ed in alcuni casi modificare le proprietà delle attività dei processi, comprese le seguenti informazioni:

- Informazioni sullo stato delle attività
- Informazioni sull'approvazione delle attività
- Informazioni sulle attività di approvazione, denominate *elemento di lavoro* in WorkPoint Designer, ad esempio:
 - Se nessun partecipante ha riservato l'elemento di lavoro (operazione che rimuove l'elemento dall'elenco di lavoro degli altri revisori), lo stato sarà impostato su Disponibile e non verrà visualizzato alcun ID utente dei partecipanti.
 - Se un partecipante ha riservato ma non completato l'elemento di lavoro, lo stato sarà impostato su Aperto e verranno visualizzati l'ID utente del partecipante e l'ora di esecuzione della riserva.
 - Se l'elemento di lavoro è stato completato, lo stato sarà impostato su Completato. Verranno visualizzati l'ID utente del partecipante che ha approvato o rifiutato l'attività controllata dal flusso di lavoro e l'ora di completamento.

Le specifiche proprietà degli elementi di lavoro includono:

- Nome e stato corrente dell'elemento di lavoro
- Informazioni sulla cronologia dello stato, compresi gli ID utente dei partecipanti responsabili degli stati assegnati
- Informazioni sui partecipanti autorizzati degli elementi di lavoro

Nota: per ulteriori informazioni sulle proprietà relative a processi, attività ed elementi di lavoro, vedere la documentazione di WorkPoint Designer.

Esecuzione delle attività del flusso di lavoro

In un processo del flusso di lavoro, un'attività manuale viene eseguita da una persona designata come partecipante dell'attività, in grado di approvare o rifiutare un evento associato ad un'attività di approvazione. I partecipanti eseguono questa attività in Identity Manager.

Le operazioni riportate di seguito vengono attivate quando viene eseguita un'attività associata ad un'attività di approvazione di Identity Manager:

1. Identity Manager invia una notifica ai partecipanti.
2. Un partecipante approva o rifiuta l'attività.
3. Il server del flusso di lavoro completa l'attività.

Ricerca e notifica dei partecipanti

Quando viene avviata un'attività del flusso di lavoro associata ad un'attività di approvazione di Identity Manager, il server del flusso di lavoro passa le informazioni relative ai partecipanti dell'attività ad Identity Manager. Queste informazioni vengono definite nelle proprietà dell'attività. Identity Manager utilizza queste informazioni per recuperare i partecipanti delle attività ed avviarli in merito ad un'attività di approvazione in sospeso.

Dopo aver identificati i partecipanti, Identity Manager aggiunge un nuovo elemento di lavoro (attività di approvazione) all'elenco di lavoro di ogni partecipante. Facoltativamente, Identity Manager invia inoltre una notifica per posta elettronica ad ogni partecipante, grazie alla quale vengono informati del nuovo elemento di lavoro.

Nota: se la proprietà APPROVERS_REQUIRED dell'attività è impostata su False e non vengono individuati partecipanti, l'attività viene considerata approvata per impostazione predefinita.

Nota: un cerchio nella colonna Stato indica che l'attività di approvazione è disponibile per essere assegnata a qualsiasi partecipante. Un segno di spunta indica che il proprietario dell'elemento di lavoro ha accettato l'attività di approvazione, ma non l'ha ancora completata.

Accettazione ed esecuzione dell'attività di approvazione

Dopo aver individuato i partecipanti, l'attività può essere completata solo quando uno dei partecipanti accetta l'attività di approvazione ed accetta o rifiuta l'attività controllata dal flusso di lavoro.

Un partecipante accetta un'attività di approvazione facendo clic sul nome dell'elemento di lavoro nella console delle attività del flusso di lavoro, quindi facendo clic su Riserva elemento. Non appena un elemento viene riservato, tale elemento viene rimosso dall'elenco di lavoro degli altri revisori.

Quando un partecipante accetta un'attività di approvazione, accetta di approvare o rifiutare l'attività controllata dal flusso di lavoro. Poiché non è possibile che più partecipanti accettino la stessa attività di approvazione, tale attività viene rimossa dagli elenchi di lavori degli altri partecipanti.

Dopo che un partecipante accetta un'attività di approvazione, viene visualizzato lo schermo relativo all'approvazione, dove il partecipante può eseguire una delle seguenti azioni:

- Approvare o rifiutare subito l'attività controllata dal flusso di lavoro.
- Rilasciare l'attività di approvazione per renderla disponibile agli altri partecipanti.
- Chiudere la finestra di dialogo e completare l'attività in una fase successiva. Per riaprire la finestra di dialogo Approva Crea utente precedentemente riportata, il partecipante deve fare clic sul nome dell'attività di approvazione disponibile nel proprio elenco di lavoro.

Inoltre, il partecipante può aggiornare uno o più campi modificabili, se presenti, nello schermo di approvazione. È possibile rendere modificabili i campi disponibili in questo schermo durante la creazione dell'attività.

Dopo l'approvazione o il rifiuto dell'attività controllata dal flusso di lavoro da parte del partecipante, l'attività risulta completata e il processo del flusso di lavoro può continuare lungo il percorso definito dal risultato dell'attività, come descritto nella sezione successiva.

Completamento dell'attività da parte del server del flusso di lavoro

Un'attività manuale visualizzata nella finestra Designer è associata a due o più transizioni condizionali.

Ogni transizione condizionale è associata ad uno script. Quando un partecipante completa l'attività, gli script analizzano il risultato dell'attività stessa. Il risultato di queste analisi determina la direzione del flusso del processo.

Nella seguente figura è illustrata l'attività Approva Crea utente visualizzata nel Designer assieme all'attività di approvazione corrispondente avente lo stesso nome in Identity Manager.

Quando il partecipante dell'attività (o revisore) fa clic sul pulsante Approva o Rifiuta in Identity Manager:

1. L'attività Approva Crea utente nell'istanza del processo viene terminata. Gli script associati alle transizioni condizionali analizzano l'esito dell'attività.
2. L'istanza del processo continua in base a quale transizione condizionale restituisce True:
 - Se l'attività viene approvata, lo script Elemento di lavoro IM approvato restituisce True. La transizione Elemento di lavoro IM approvato passa al nodo successivo. Questa attività automatizzata, Approvazione IM, notifica ad Identity Manager di eseguire l'attività Crea utente.
 - Se l'attività viene rifiutata, lo script Elemento di lavoro IM rifiutato restituisce True. La transizione Elemento di lavoro IM rifiutato passa al nodo successivo del flusso di lavoro. Questa attività automatizzata, Rifiuto IM, notifica ad Identity Manager di annullare l'attività Crea utente.

Visualizzazione di processi Workpoint

È possibile visualizzare nella console utente lo stato dei processi Workpoint dai seguenti elementi:

- Attività di approvazione
- Visualizza attività inoltrate.

Nei nuovi ambienti, tutte le attività di approvazione includono per impostazione predefinita la scheda Visualizza processo. Solo gli eventi creati in questa versione supportano la visualizzazione in Visualizza attività inoltrate delle immagini dei processi per tutte le definizioni di processo richiamate per quel determinato evento o attività. Gli eventi creati con le versioni precedenti non supportano la funzione di visualizzazione processi del flusso di lavoro.

Aggiunta della scheda Visualizza processo alle schede di approvazione esistenti

Per le attività di approvazione è necessario aggiungere la nuova scheda Visualizza processo a tutte le attività esistenti, al fine di visualizzare l'immagine del processo relativo all'elemento di lavoro.

Nota: nei nuovi ambienti questa scheda è presente per tutte le attività di approvazione.

Aggiunta della scheda Visualizza processo a un'attività esistente

1. Dalla categoria Admin Tasks and Role (Attività di amministrazione e ruolo), eseguire ModifyAdminTask selezionando Attività di amministrazione, Modifica attività di amministrazione.
2. Fare clic su Cerca e selezionare un'attività di approvazione, ad esempio Approva Crea utente, quindi scegliere Seleziona.

Viene visualizzata la finestra di dialogo Modifica attività di amministrazione: Approva Crea utente.

3. Fare clic sulla scheda Schede e selezionare Visualizza processo (JobView) dal menu a discesa, quindi fare clic su Inoltra.

La scheda Visualizza processo viene aggiunta all'attività di approvazione.

Ripetere la procedura per tutte le attività di approvazione esistenti.

Flusso di lavoro basato su criterio

Il flusso di lavoro basato su criterio consente di assoggettare un evento o un'attività di amministrazione al controllo del flusso di lavoro in base alla valutazione di una regola. In tal modo, anziché far sì che sia sempre un evento o un'attività di amministrazione ad avviare il processo del flusso di lavoro, è il processo del flusso di lavoro ad essere eseguito e a generare un elemento di lavoro se la regola associata all'evento o attività di amministrazione è vera.

La condizione che determina se avviare un processo di lavoro è una *regola di approvazione*. Se avviato, il processo del flusso di lavoro assoggetta l'evento o l'attività di amministrazione al controllo del flusso di lavoro aggiungendo un elemento all'elenco dei lavori di un revisore.

Un *criterio di approvazione* comprende la regola di approvazione, il tipo di valutazione della regola, l'ordine del criterio, la descrizione del criterio e il processo del flusso di lavoro.

Ad esempio, quando si crea un nuovo gruppo, è possibile definire un criterio di approvazione per assoggettare CreateGroupEvent al controllo del flusso di lavoro e creare un elemento di lavoro solo se il nuovo gruppo fa parte di un'organizzazione di livello superiore designata. Se il nuovo gruppo non fa parte di una tale organizzazione, il processo del flusso di lavoro non viene eseguito e non viene creato alcun elemento di lavoro.

Se un evento presenta regole multiple, sarà necessaria l'approvazione di tutti i flussi di lavoro associati all'evento affinché l'evento stesso venga approvato. Analogamente, per un'attività di amministrazione è possibile definire un criterio di approvazione per assoggettare CreateGroupEvent al controllo del flusso di lavoro e creare un elemento di lavoro solo se il nome del nuovo gruppo inizia con Vendite. Se il nome del nuovo gruppo non inizia con Vendite, il processo del flusso di lavoro non viene eseguito e non viene creato alcun elemento di lavoro.

È possibile creare una regola con criteri da valutare sempre o soltanto quando un determinato attributo o oggetto gestito varia, ad esempio se il valore dello stipendio di un dipendente cambia.

Nota: Nelle versioni precedenti del flusso di lavoro basato sul criterio, le eventuali modifiche apportate agli attributi da un responsabile dell'approvazione venivano inviate per una nuova approvazione. Con l'approvazione e il rifiuto a livello di attributo, le modifiche effettuate in qualsiasi fase vengono approvate solo una volta. L'elemento di lavoro non viene mai inoltrato per una nuova approvazione, anche se l'attributo contenuto nella regola viene modificato. Approvata una modifica, il responsabile dell'approvazione visualizzerà di nuovo l'elemento di lavoro solo quando verrà inoltrata una nuova modifica o l'attività sarà inoltrata nuovamente.

Ulteriori informazioni:

[Flusso di lavoro a livello di evento](#) (a pagina 272)

[Flusso di lavoro a livello di attività](#) (a pagina 269)

[Ordine criterio](#) (a pagina 324)

[Valutazione regola](#) (a pagina 322)

Oggetti delle regole

L'amministratore di CA Identity Manager può creare criteri di approvazione per un evento o un'attività di amministrazione basati sui seguenti oggetti. Di seguito sono elencati gli oggetti per un evento, se si riferiscono a un determinato evento e se sono presenti durante l'esecuzione dell'evento stesso:

- **Iniziatore attività:** amministratore CA Identity Manager che esegue l'attività.
- **Oggetto primario dell'evento:** oggetto primario associato all'evento.
- **Oggetto secondario per l'evento:** oggetto secondario associato all'evento relativo all'oggetto primario.

Di seguito sono elencati gli oggetti per un'attività di amministrazione:

- **Oggetto primario dell'attività:** oggetto primario associato all'attività
- **Iniziatore attività** - amministratore di Identity Manager che esegue l'attività.
- **Violazione criteri di identità:** per le violazioni dei criteri di identità, le regole sono basate sul nome del criterio di identità che ha provocato la violazione, ad esempio Nome criterio UGUALE A CriterioTitolo. Il messaggio di violazione viene visualizzato nella scheda dei dettagli sull'attività della schermata di approvazione, che corrisponde ai dettagli sull'attività di Visualizza attività inviate. Il messaggio di violazione SOD viene visualizzato sotto una nuova intestazione di sezione, denominata Violazione criteri di identità. Un responsabile dell'approvazione può visualizzare questi messaggi e decidere se approvare o rifiutare l'attività.

Valutazione regola

Le regole dei criteri per un evento possono essere valutate nei due modi seguenti:

- **Sempre**

Un criterio con tipo di valutazione Always viene richiamato se il criterio si rivela vero, indipendentemente dall'applicazione o meno di modifiche a qualsiasi attributo contenuto nel criterio. Nella schermata di approvazione di un elemento di lavoro generato per effetto di un criterio con valutazione di tipo Always, un responsabile dell'approvazione può modificare qualsiasi attributo modificabile.

Nota: se il responsabile dell'approvazione fa clic sul pulsante Rifiuta, l'evento viene rifiutato come in precedenza.

- **Solo se varia un attributo specificato nella condizione di approvazione**

Un criterio con tipo di valutazione OnChange viene richiamato solo se il criterio si rivela vero e se qualsiasi attributo contenuto nel criterio è stato modificato. Nella schermata di approvazione di un elemento di lavoro generato per effetto di un criterio con valutazione di tipo Onchange, il responsabile dell'approvazione può modificare solo i valori degli attributi contenuti nel criterio, se tali attributi dispongono di autorizzazioni di lettura e scrittura. Tutti gli altri attributi presenti nella schermata di approvazione dispongono di autorizzazioni di sola scrittura.

Nota: se il responsabile dell'approvazione fa clic sul pulsante Rifiuta, vengono rifiutate solo le modifiche apportate agli attributi contenuti nel criterio di approvazione e viene valutato il criterio di approvazione successivo.

Questa opzione si applica solo all'oggetto primario dell'evento o dell'attività.

Si considerino ad esempio i criteri seguenti, tutti relativi a ModifyUserEvent nell'attività di amministrazione Modifica utente:

Criterio	Regola	Valutazione
Criterio1	User where (User ID = Smith01)	Sempre
Criterio2	User where (Title = Manager)	Quando varia l'attributo Title
Criterio3	User where (Salary >= 80000)	Quando varia l'attributo Salary

Policy1 viene valutato tutte le volte che l'amministratore richiama l'attività Modifica utente per l'utente Smith01, a prescindere da quale sia l'attributo che varia.

Policy2 viene valutato quando l'amministratore richiama l'attività Modifica utente per modificare l'attributo Title di un oggetto utente qualsiasi. Policy2 è vero se Title cambia in Manager.

Policy3 viene valutato quando l'amministratore richiama l'attività Modifica utente per modificare l'attributo Salary di un oggetto utente qualsiasi. Policy3 è vero se Salary passa a 80 000 o più.

Nell'esempio, se un amministratore utilizza l'attività Modifica utente per modificare l'attributo Title in Manager per l'utente Smith01, allora verranno valutati come veri sia il criterio Policy1 sia il criterio Policy2, avviando i rispettivi processi di flusso di lavoro. In questo caso si applica l'ordine di priorità standard.

La valutazione condizionale delle regole consente al revisore di un elemento di lavoro di modificare un attributo che influisce su un altro elemento di lavoro relativo allo stesso evento mentre l'evento è ancora in sospeso. Ciò è possibile solo per i criteri di approvazione con tipo di valutazione Always. Sempre facendo riferimento all'esempio precedente, se un amministratore modifica un attributo relativo all'utente Smith01, allora Policy1 è vero e genera un elemento di lavoro. Mentre approva l'elemento di lavoro generato da Policy1, il revisore potrà modificare l'attributo Salary di Smith01 direttamente sulla schermata di approvazione. In questo caso, il nuovo valore di Salary per l'utente Smith01 determina se il criterio Policy3 genererà un elemento di lavoro per la stessa istanza di ModifyUserEvent. Se il revisore modifica lo stipendio in 90 000, allora Policy3 genererà un nuovo elemento di lavoro che dovrà essere approvato prima dell'approvazione dell'evento in sé. Si applica l'ordine di priorità standard.

Ulteriori informazioni:

[Ordine criterio](#) (a pagina 324)

[Oggetti delle regole](#) (a pagina 321)

Esempio di valutazione regola

Si considerino i criteri seguenti, tutti relativi a ModifyUserEvent nell'attività di amministrazione Modifica utente:

Criterio	Regola	Valutazione
Criterio1	User where (User ID = Smith01)	Sempre
Criterio2	User where (Title = Manager)	Quando varia l'attributo Title
Criterio3	User where (Salary >= 80000)	Quando varia l'attributo Salary

Policy1 viene valutato tutte le volte che l'amministratore richiama l'attività Modifica utente per l'utente Smith01, a prescindere da quale sia l'attributo che varia.

Policy2 viene valutato quando l'amministratore richiama l'attività Modifica utente per modificare l'attributo Title di un oggetto utente qualsiasi. Policy2 è vero se Title cambia in Manager.

Policy3 viene valutato quando l'amministratore richiama l'attività Modifica utente per modificare l'attributo Salary di un oggetto utente qualsiasi. Policy3 è vero se Salary passa a 80 000 o più.

Nell'esempio, se un amministratore utilizza l'attività Modifica utente per modificare l'attributo Title in Manager per l'utente Smith01, allora verranno valutati come veri sia il criterio Policy1 sia il criterio Policy2, avviando i rispettivi processi di flusso di lavoro. In questo caso si applica l'ordine di priorità standard.

La valutazione condizionale delle regole consente al revisore di un elemento di lavoro di modificare un attributo che influisce su un altro elemento di lavoro relativo allo stesso evento mentre l'evento è ancora in sospeso. Ciò è possibile solo per i criteri di approvazione con tipo di valutazione Always. Sempre facendo riferimento all'esempio precedente, se un amministratore modifica un attributo relativo all'utente Smith01, allora Policy1 è vero e genera un elemento di lavoro. Mentre approva l'elemento di lavoro generato da Policy1, il revisore potrà modificare l'attributo Salary di Smith01 direttamente sulla schermata di approvazione. In questo caso, il nuovo valore di Salary per l'utente Smith01 determina se il criterio Policy3 genererà un elemento di lavoro per la stessa istanza di ModifyUserEvent. Se il revisore modifica lo stipendio in 90 000, allora Policy3 genererà un nuovo elemento di lavoro che dovrà essere approvato prima dell'approvazione dell'evento in sé. Si applica l'ordine di priorità standard.

Ordine criterio

Tutti i criteri di approvazione contengono un campo Ordine criterio in cui un valore intero positivo specifica la priorità, dal più basso al più alto. La priorità di ciascun criterio determina quanto segue:

- L'ordine di valutazione delle regole di approvazione
- Per le regole vere, l'ordine di avvio dei processi di flusso di lavoro

Viene data priorità al criterio con il valore intero più basso e la relativa regola viene valutata prima dei criteri con valore intero più alto. Per tutti i criteri per cui esiste un evento o un'attività di amministrazione vera, il criterio con la priorità più alta avvia per primo il relativo processo di flusso di lavoro.

Esempio di ordinamento dei criteri

Questo semplice esempio dimostra il funzionamento dell'ordinamento dei criteri. In questo esempio, si presuppone che le regole dei criteri vengano sempre valutate.

Se un evento presenta più criteri che vengono sempre valutati, affinché l'evento stesso venga approvato tutti i criteri devono essere approvati. Se tuttavia viene rifiutato un criterio associato all'evento il cui tipo di valutazione criterio è ALWAYS, l'evento viene rifiutato.

Nota: se un criterio associato all'evento ha un tipo di valutazione Onchange, vengono rifiutate solo le modifiche associate agli attributi contenuti nel criterio. L'evento non viene rifiutato e viene valutato il criterio successivo.

In questo esempio, il tipo di valutazione criterio di Criterio1, Criterio2 e Criterio3 corrisponde ad ALWAYS. Criterio1 viene valutato falso, quindi il processo del flusso di lavoro denominato Processo1 non viene eseguito e nessun elemento di lavoro viene generato per l'Utente1. Il controllo dell'evento passa immediatamente a Criterio2. Criterio2 e Criterio3 risultano entrambi veri. Vista la sua priorità di livello superiore, il Processo2 del flusso di lavoro viene eseguito per primo e genera un elemento di lavoro per l'Utente2.

Se l'Utente2 approva l'elemento di lavoro, viene eseguito il Processo3 del flusso di lavoro, che genera un elemento di lavoro per l'Utente3, che deve approvarlo affinché l'evento stesso venga approvato. Le azioni sono indicate nella seguente tabella.

Priorità	Criterio	Risultato	Flusso di lavoro	Responsabile dell'approvazione	Azione
1	Criterio1	False	Processo1	Utente1	—
2	Criterio2	True	Processo2	Utente2	Approvato
3	Criterio3	True	Processo3	Utente3	Approvato

Se tuttavia l'Utente2 rifiuta l'elemento di lavoro, l'evento stesso viene rifiutato e non viene generato alcun elemento di lavoro per l'Utente3, come illustrato nella tabella seguente:

Priorità	Criterio	Risultato	Flusso di lavoro	Responsabile dell'approvazione	Azione
1	Criterio1	False	Processo1	Utente1	—
2	Criterio2	True	Processo2	Utente2	Rifiutato

Priorità	Criterio	Risultato	Flusso di lavoro	Responsabile dell'approvazione	Azione
3	Criterio3	True	Processo3	Utente3	—

Nell'esempio che segue, il tipo di valutazione criterio di Criterio1, Criterio2 e Criterio3 è ONCHANGE. Se l'Utente2 rifiuta l'elemento di lavoro, vengono rifiutate solo le modifiche associate agli attributi contenuti in Criterio2. Viene quindi valutato il Criterio3, il Processo3 del flusso di lavoro viene eseguito e genera un elemento di lavoro per l'Utente3. Se l'Utente3 rifiuta l'elemento di lavoro, l'evento viene rifiutato in quanto tutte le modifiche apportate all'evento sono state rifiutate. Se l'Utente3 approva l'elemento di lavoro, l'evento viene approvato e le modifiche associate agli attributi contenuti nel Criterio3 vengono mantenute.

Priorità	Criterio	Risultato	Flusso di lavoro	Responsabile dell'approvazione	Azione
1	Criterio1	False	Processo1	Utente1	—
2	Criterio2	True	Processo2	Utente2	Rifiutato
3	Criterio3	True	Processo3	Utente3	Approvato

Descrizione criterio

Un attributo di descrizione della stringa non obbligatorio e non ricercabile è stato aggiunto all'oggetto gestito Criterio di approvazione e verrà visualizzato negli elementi di lavoro risultanti.

Numero massimo di caratteri supportati: 255 caratteri

Per la descrizione è possibile inserire le informazioni relative a raggruppamento/chave nel seguente formato:

\$ (bundle=<nome completo dei raggruppamenti di risorse> : key=<chiave>)

Criteri di approvazione e attributi multivalore

In precedenza, se si impostava una regola per un attributo multivalore, non era possibile specificare che la regola andava eseguita solo sui valori aggiunti o rimossi di recente all'attributo. Questo risultato può essere ora raggiunto tramite l'esame del tipo di valutazione della regola basata su un attributo multivalore. Impostando il tipo di valutazione della regola su Onchange è possibile applicare la regola solo ai valori aggiunti o rimossi di recente dell'attributo multivalore e non a tutti i suoi valori. Se la regola deve essere basata su tutti i valori dell'attributo multivalore, indipendentemente da quando questi sono stati aggiunti o rimossi, il tipo di regola da utilizzare è Always.

Le modifiche apportate agli attributi multivalore sono evidenziate nella schermata di profilo e sono provviste di un'icona di annullamento. Se una regola viene valutata come vera perché è stato rimosso o aggiunto un nuovo valore a un attributo multivalore, il responsabile dell'approvazione di questa modifica visualizza TUTTI i valori contenuti nell'attributo multivalore. Facendo clic sull'icona di annullamento verrà ripristinato il valore originale dell'attributo. Se il responsabile dell'approvazione desidera visualizzare i valori rimossi, facendo clic sull'icona di annullamento verrà visualizzato il set di valori originale. Facendo clic sull'icona di ripetizione verrà visualizzato il nuovo set di valori, consentendo al responsabile dell'approvazione di distinguere i valori aggiunti da quelli rimossi. Facendo clic sul pulsante Approva verranno approvate tutte le modifiche all'attributo multivalore. Facendo clic sul pulsante Rifiuta verranno rifiutate tutte le modifiche all'attributo multivalore. Tutte le regole successive di pertinenza di questo attributo multivalore non verranno valutate, a meno che non sia presente un nuovo delta di valori per l'attributo multivalore.

Nota: per le regole basate su attributi multivalore, i valori contenuti nell'attributo multivalore sono i valori effettivi e non quelli visualizzati. Ad esempio, il valore visualizzato per lo stato MA è Massachusetts. Quando si crea un criterio di approvazione basato sull'attributo relativo allo stato, la regola deve avere l'aspetto stato=MA.

Si considerino i criteri seguenti, tutti relativi a ModifyUserEvent nell'attività di amministrazione Modifica utente:

Criterio	Regola	Valutazione
Criterio1	Utente dove (Stato = MA)	OnChange
Criterio2	Utente dove (Stato = DC)	Sempre

Il Criterio1 viene valutato ogni volta che un amministratore richiama l'attività ModifyUser per modificare l'attributo relativo allo stato e viene valutata come vera se il valore MA viene aggiunto o rimosso dall'attributo.

Il Criterio2 viene valutato ogni volta che l'amministratore richiama l'attività ModifyUser per un utente il cui stato contiene il valore DC.

Attributi evidenziati come modificati nelle schermate di approvazione del flusso di lavoro

In una schermata di approvazione, è possibile che gli attributi aggiuntivi siano evidenziati come modificati anche se non sono stati modificati dall'amministratore nell'attività originale. Ciò si verifica perché la schermata può contenere script che modificano i valori di alcuni attributi contenuti nella schermata stessa come parte di inizializzazione o convalida di schermata per la modifica di un altro attributo.

Esempi di criteri

I seguenti esempi di Use Case aziendali mostrano com'è possibile applicare i criteri di approvazione del flusso di lavoro per un evento:

Esempio 1

Use Case: un amministratore modifica l'account del database relazionale di un dipendente.

Attività di amministrazione – ModifyMSSQLAccount

Evento – ModifyMSSQLAccountEvent

Regola di approvazione – Utente dove (Titolo = RDBAcctManager)

Processo del flusso di lavoro – ModAcctApproval (personalizzato)

Oggetto – Iniziatore attività

Valutazione – Valutare sempre la regola

Esempio 2

Use Case – Un amministratore modifica lo stipendio di un dipendente in seguito a un avanzamento di carriera.

Attività di amministrazione – Modifica utente

Evento – ModifyUserEvent

Regola di approvazione – Utente dove (Salary >= 100000)

Processo del flusso di lavoro – SalaryChangeApproval (personalizzato)

Oggetto – Oggetto primario dell'evento (utente)

Valutazione – Valutare solo quando cambia l'attributo Salary

Esempio 3

Use Case – Un amministratore aggiunge un utente al gruppo Appaltatori quando il suo titolo diviene Contractor. Questo esempio può essere suddiviso sui due seguenti criteri di approvazione:

Criterio 1:

Attività di amministrazione – Modifica utente

Evento – ModifyUserEvent

Regola di approvazione – Utente dove (Title = Contractor)

Processo del flusso di lavoro – SingleStepApproval (predefinito)

Oggetto – Oggetto primario dell'evento (utente)

Valutazione – Valutare solo quando cambia l'attributo Title

Criterio 2:

Attività di amministrazione – Modifica gruppo o Modifica membri del gruppo

Evento – AddToGroup

Regola di approvazione – Utente dove (Nome gruppo = Contractors)

Processo del flusso di lavoro – SingleStepApproval (predefinito)

Oggetto – Oggetto secondario dell'evento (gruppo)

Valutazione – Valutare sempre la regola

I seguenti esempi di Use Case aziendali mostrano com'è possibile applicare i criteri di approvazione del flusso di lavoro per un'attività:

Esempio 1

Use Case: un amministratore modifica l'account Active Directory di un dipendente.

Attività di amministrazione – ModifyActiveDirectoryAccount

Oggetto – Iniziatore attività

Regola di approvazione – Utente dove (Titolo = ActiveDirectoryManager)

Processo del flusso di lavoro – SingleStepApproval

Valutazione – Valutare sempre la regola

Esempio 2

Use Case – Un amministratore modifica un utente il cui codice dipendente è HighSecurity.

Attività di amministrazione – Modifica utente

Oggetto – Oggetto primario dell'attività

Regola di approvazione – Utente dove (employeenumber = HighSecurity)

Processo del flusso di lavoro – SingleStepApproval

Valutazione – Valutare sempre la regola

Esempio 3

Use Case – Un amministratore modifica un utente per assegnargli i ruoli di amministrazione CheckApprover e CheckSigner.

Attività di amministrazione – Modifica utente

Oggetto – Violazione criteri di identità

Regola di approvazione – IdentityPolicy dove (Nome = CheckRoles)

Processo del flusso di lavoro – SingleStepApproval

Valutazione – Valutare sempre la regola

Configurazione di un flusso di lavoro basato su criterio per gli eventi

La procedura di configurazione di un flusso di lavoro basato su criterio è simile a quella necessaria per configurare un flusso di lavoro del livello evento, ma richiede anche la definizione dei criteri di approvazione che stabiliscono se il flusso di lavoro viene eseguito.

Per configurare un flusso di lavoro basato su criterio

1. Nella console utente selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione o Crea attività di amministrazione.
Verrà visualizzata la schermata Selezionare attività di amministrazione.
2. Cercare l'attività per la quale impostare il controllo da parte del flusso di lavoro, quindi fare clic su Seleziona.
Verrà visualizzata la schermata Modifica attività di amministrazione o Crea attività di amministrazione.
3. Nella scheda Profilo, verificare che l'opzione Attiva flusso di lavoro sia selezionata.
4. Nella scheda Eventi selezionare un evento da mappare ad un modello di processo.
Verrà visualizzato la schermata del mapping del flusso di lavoro.
5. Selezionare il pulsante di opzione Basato su criterio e quindi fare clic su Aggiungi.
Verrà visualizzata la schermata Criterio di approvazione.
6. [Configurare un criterio di approvazione.](#) (a pagina 334)
7. Configurare i resolver partecipanti in modo conforme al processo di flusso di lavoro selezionato.
Le richieste dei partecipanti verranno aggiunte al processo.
8. Fare clic su OK.
La configurazione del flusso di lavoro a livello di evento viene salvata.
9. Fare clic su Inoltra.
La modifica all'attività viene elaborata in CA Identity Manager.

Nota: nell'elenco Processo del flusso di lavoro sono inclusi i processi da utilizzare sia con il metodo basato su modelli che con il metodo WorkPoint:

- Quando si seleziona un processo del metodo basato su modelli (SingleStepApproval oppure TwoStageApprovalProcess), la pagina verrà ingrandita in modo da consentire la configurazione dei resolver partecipanti.
- Se invece si seleziona un metodo WorkPoint, la pagina non verrà ingrandita. I resolver partecipanti vengono configurati in WorkPoint Designer.

Ulteriori informazioni:

[Resolver partecipanti: metodo WorkPoint](#) (a pagina 300)

[Modalità di configurazione di un criterio di approvazione](#) (a pagina 334)

Configurazione di un flusso di lavoro basato su criterio per le attività

La procedura di configurazione di un flusso di lavoro basato su criterio per le attività è simile a quella necessaria per configurare un flusso di lavoro del livello attività, ma richiede anche la definizione dei criteri di approvazione che stabiliscono se il flusso di lavoro viene eseguito.

Per configurare un flusso di lavoro basato su criterio

1. Nella console utente selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione o Crea attività di amministrazione.
Verrà visualizzata la schermata Selezionare attività di amministrazione.
2. Cercare l'attività per la quale impostare il controllo da parte del flusso di lavoro, quindi fare clic su Seleziona.
Verrà visualizzata la schermata Modifica attività di amministrazione o Crea attività di amministrazione.
3. Nella scheda Profilo, verificare che l'opzione Attiva flusso di lavoro sia selezionata.
4. Nella scheda Profilo, fare clic sull'icona a forma di matita accanto al campo Processo del flusso di lavoro.
Verrà visualizzato la schermata del mapping del flusso di lavoro.
5. Selezionare il pulsante di opzione Basato su criterio e quindi fare clic su Aggiungi.
Verrà visualizzata la schermata Criterio di approvazione.
6. [Configurare un criterio di approvazione.](#) (a pagina 334)
7. Configurare i resolver partecipanti in modo conforme al processo di flusso di lavoro selezionato.
Le richieste dei partecipanti verranno aggiunte al processo.
8. Fare clic su OK.
La configurazione del flusso di lavoro a livello di attività viene salvata.
9. Fare clic su Inoltra.
La modifica all'attività viene elaborata in CA Identity Manager.

Nota: l'elenco Processo del flusso di lavoro contiene i processi da utilizzare con il metodo del modello per il flusso di lavoro basato sul criterio a livello di attività:

- Quando si seleziona un processo del metodo basato su modelli (SingleStepApproval oppure TwoStageApprovalProcess), la pagina verrà ingrandita in modo da consentire la configurazione dei resolver partecipanti.

Ulteriori informazioni

[Modalità di configurazione di un criterio di approvazione](#) (a pagina 334)

Modalità di configurazione di un criterio di approvazione

La configurazione di un criterio di approvazione per un evento o un'attività implica i seguenti passaggi.

1. Selezionare un oggetto da sottoporre a test.
2. Definire una regola di approvazione per l'oggetto.
3. Per gli oggetti primari, stabilire se si tratta di una valutazione condizionale.
4. Immettere l'ordine di valutazione del criterio.
5. Configurare un processo del flusso di lavoro da eseguire se la regola di approvazione è vera.

Per configurare un criterio di approvazione

1. Nella schermata Criterio di approvazione, selezionare un oggetto per la regola da sottoporre a test nell'elenco a discesa.

La schermata viene aggiornato in base alla selezione effettuata.

2. Nell'elenco a discesa accanto al nome dell'oggetto, selezionare un modello di espressione di condizione.

La schermata viene aggiornato in base alla selezione effettuata.

3. Creare e modificare l'espressione di condizione come necessario.
4. Selezionare il pulsante di opzione Valutazione regola per indicare se la regola deve essere sempre valutata oppure solo nel caso in cui un attributo nella condizione di approvazione cambia.
5. Immettere un valore intero positivo per specificare l'ordine di valutazione del criterio (se vi sono più criteri per l'evento).
6. Selezionare e configurare il processo del flusso di lavoro che viene eseguito se la regola viene valutata come vera (true).
7. Fare clic su OK per salvare il criterio di approvazione.

Ulteriori informazioni:

[Procedura di configurazione del flusso di lavoro a livello di evento](#) (a pagina 274)

[Configurazione di un flusso di lavoro basato su criterio per gli eventi](#) (a pagina 331)

[Configurazione di un flusso di lavoro basato su criterio per le attività](#) (a pagina 333)

Stato del flusso di lavoro di basato su criterio

Gli amministratori di CA Identity Manager possono visualizzare lo stato delle attività contenenti criteri di approvazione del flusso di lavoro mediante i seguenti strumenti di sistema standard:

- Scheda Visualizza attività inviate
- Scheda Cronologia utente
- Rapporti e registri

Le informazioni sulle attività inoltrate e sulla cronologia delle attività includono:

- Informazioni su attività ed eventi
- Informazioni sulle regole di flusso di lavoro e di approvazione
- Risultati della valutazione delle regole di approvazione

Vedere la documentazione relativa alla scheda Sistema per le descrizioni della cronologia delle attività inoltrate.

Ulteriori informazioni:

[Descrizione dello stato degli eventi](#) (a pagina 583)

[Stato delle attività in CA Identity Manager](#) (a pagina 576)

Mapping globale di eventi a processi del flusso di lavoro basato su criterio

Un evento può essere mappato a un processo del flusso di lavoro dalla console di gestione, oppure essere associato a criteri di approvazione del flusso di lavoro basato su criterio all'interno di una specifica attività. La nuova attività Configurare il flusso di lavoro basato sul criterio globale per Eventi consente agli amministratori di impostare a livello di ambiente il mapping del flusso di lavoro basato sul criterio per gli eventi. A differenza dell'impostazione del flusso di lavoro basato su criterio per un evento in un'attività di amministrazione, i mapping del flusso di lavoro basati su criteri configurati vengono applicati a tutte le attività che generano l'evento.

Nota: l'attività Configurare il flusso di lavoro basato sul criterio globale per Eventi funziona solo quando è attivato il flusso di lavoro. L'esecuzione di questa attività quando il flusso di lavoro è disattivato genera un errore.

Questa attività è stata aggiunta alla scheda Sistema. Quando viene inviata un'attività, viene recuperato il processo del flusso di lavoro di ogni evento dell'attività, come descritto di seguito:

Qualsiasi flusso di lavoro configurato per l'evento per l'attività amministrativa in questione ha la precedenza. Un evento può essere configurato sia per il flusso di lavoro basato su criterio che per il flusso di lavoro non basato su criterio. Se per l'evento per l'attività amministrativa in questione è configurato il flusso di lavoro basato su criterio, viene richiamato il flusso di lavoro associato al criterio. Se non viene soddisfatta alcuna regola, per l'evento non viene richiamato alcun flusso di lavoro. Analogamente, se per l'evento per l'attività amministrativa in questione è configurato il flusso di lavoro non basato su criterio, viene richiamato il processo del flusso di lavoro associato al criterio. Se per l'evento non è stato configurato un flusso di lavoro per l'attività amministrativa in questione, ha la precedenza la configurazione del flusso di lavoro globale per tale evento.

Schermata attività Configurare il flusso di lavoro basato sul criterio globale per Eventi

L'attività Configurare il flusso di lavoro basato sul criterio globale per Eventi consente agli amministratori di configurare il flusso di lavoro basato o non basato su criterio per tutti gli eventi dell'ambiente corrente. Facendo clic sull'attività viene visualizzato il mapping predefinito degli eventi alle definizioni dei processi del flusso di lavoro. È possibile modificare tutti i mapping degli eventi e aggiungere nuovi mapping per gli eventi non configurati.

Configurare il flusso di lavoro basato sul criterio globale per Eventi

Processi di flusso associati a eventi in questo ambiente.

Nome evento	Processo del flusso di lavoro
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
CertifyRoleEvent	CertifyRoleApproveProcess
CreateGroupEvent	CreateGroupApproveProcess
CreateOrganizationEvent	CreateOrganizationApproveProcess
CreateUserEvent	CreateUserApproveProcess
DeleteGroupEvent	DeleteGroupApproveProcess
DeleteOrganizationEvent	DeleteOrganizationApproveProcess
DeleteUserEvent	DeleteUserApproveProcess
ModifyOrganizationEvent	ModifyOrganizationApproveProcess
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
SelfRegisterUserEvent	SelfRegistrationApproveProcess

Aggiungi nuovi mapping

Evento: AccountChangePasswordEvent

Aggiungi

Di seguito sono descritti i campi presenti in questa schermata:

Processi di flusso associati a eventi in questo ambiente.

Consente di specificare i processi del flusso di lavoro associati ai criteri di approvazione.

Aggiungi nuovi mapping

Consente di specificare un criterio di approvazione da mappare a un processo del flusso di lavoro.

Pulsante Aggiungi

Consente di aggiungere il nuovo mapping.

Aggiungendo o modificando un mapping viene visualizzata la schermata di mapping del flusso di lavoro, in cui è possibile selezionare i mapping dei processi e i criteri di approvazione. Il comportamento è analogo a quello della configurazione del flusso di lavoro del livello evento. Facendo clic sul pulsante Aggiungi nella pagina Workflow Mappings (Mapping del flusso di lavoro) viene visualizzata un'altra pagina in cui è possibile configurare un criterio di approvazione.

Ulteriori informazioni

[Configurazione di un flusso di lavoro basato su criterio per gli eventi](#) (a pagina 331)

[Modalità di configurazione di un criterio di approvazione](#) (a pagina 334)

Richieste in linea

CA Identity Manager consente di creare attività di richiesta in linea per scopi generali. L'implementazione delle richieste in linea predefinite prevede una serie di attività correlate finalizzate sia alle richieste di modifica automatica che alle richieste di modifica di utenti con diritti di amministratore. Tuttavia, la funzionalità delle richieste in linea può essere facilmente implementata per altre attività di richiesta di CA Identity Manager.

Una richiesta di modifica dell'utente attiva un processo del flusso di lavoro che genera un elemento di lavoro. I partecipanti del flusso di lavoro possono approvare ed implementare l'elemento di lavoro oppure rifiutarlo. L'utente che avvia l'attività immette una descrizione della richiesta nell'Editor cronologia, ovvero un'area di testo utilizzata da CA Identity Manager per gestire la cronologia di una richiesta. L'Editor cronologia può essere configurato per consentire ai partecipanti di inserire commenti relativi alle azioni eseguite sull'elemento di lavoro. Questi commenti diventano parte della cronologia globale dell'elemento di lavoro.

È inoltre possibile eseguire nuove azioni oltre alle o al posto delle azioni di approvazione e rifiuto standard. Ad esempio, un partecipante aziendale può descrivere o commentare una richiesta, mentre un partecipante dell'area tecnica può implementare tale richiesta. Queste nuove attività possono essere rappresentate da nuovi pulsanti di azione, ad esempio "Descrivi" o "Implementa", che è possibile aggiungere ai pulsanti standard "Approva" e "Rifiuta" disponibili nell'attività di approvazione.

Attività associate alle richieste in linea

Sono disponibili cinque attività che compongono l'implementazione predefinita delle richieste in linea. Tali attività consentono di illustrare l'utilizzo di pulsanti personalizzati relativi a richieste, cronologia ed attività del flusso di lavoro.

Nota: per impostazione predefinita, le attività di amministrazione (Modifica account personale e Crea richiesta in linea) vengono configurate per il flusso di lavoro a livello di evento mediante il modello Processo consulenza.

Modifica account personale

Attività di amministrazione di modifica automatica che crea una richiesta di modifica dell'account utente. Dispone di una scheda Richiesta con un Editor cronologia per la descrizione della richiesta e di una scheda Profilo contenente dettagli utente di sola lettura.

Crea richiesta in linea

Attività di amministrazione di modifica dell'utente che crea una richiesta di modifica dell'account per un particolare utente. Dispone di una scheda Richiesta contenente un Editor cronologia per la descrizione della richiesta e di una scheda Profilo soggetto contenente dettagli utente di sola lettura.

Approva Richiesta in linea

Attività di approvazione che consente al partecipante aziendale di approvare o rifiutare l'attività oppure richiedere ulteriori chiarimenti relativi all'attività. Questa attività dispone di una scheda Richiesta contenente una Visualizzazione cronologia ed un Editor cronologia per query o commenti, una scheda Profilo soggetto di sola lettura ed una scheda Assegnatari.

Precisa richiesta in linea

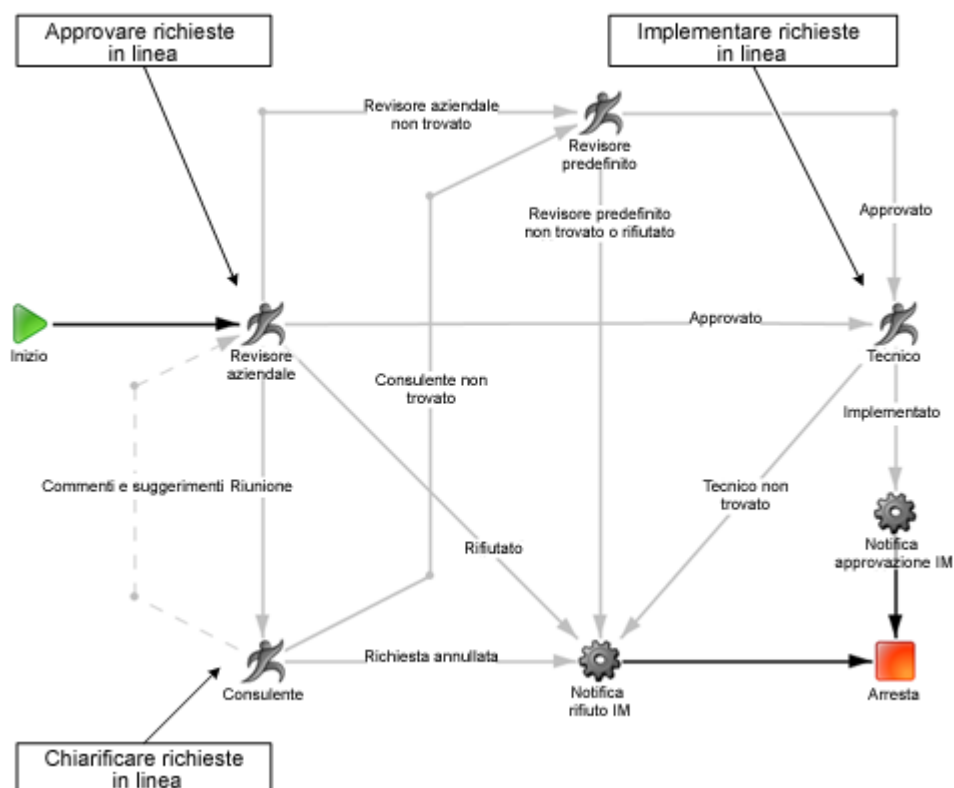
Attività di approvazione che consente al partecipante interessato di rispondere ad una richiesta di chiarimenti, nonché di reinviare un'attività al partecipante aziendale per l'approvazione. Dispone di una scheda Richiesta contenente una Visualizzazione cronologia ed un Editor cronologia per commenti, nonché di una scheda Profilo soggetto di sola lettura.

Implementa richiesta in linea

Attività di approvazione che consente al partecipante tecnico di implementare l'attività ed aggiungere un commento alla cronologia dell'attività. Dispone di una scheda Implementa richiesta contenente una Visualizzazione cronologia ed un Editor cronologia per commenti, una scheda Profilo soggetto di sola lettura ed una scheda Assegnatari.

Processo della richiesta in linea

Le attività di richiesta in linea sono controllate da un modello di processo del flusso di lavoro denominato Processo consulenza, disponibile in WorkPoint Designer.



In tale processo sono incluse quattro attività manuali che corrispondono alle attività di approvazione nell'implementazione della richiesta in linea:

- Un'attività per il revisore aziendale, che rifiuta l'elemento di lavoro, approva l'elemento di lavoro e lo passa al tecnico oppure richiede ulteriori chiarimenti al consulente.
- Un'attività per il consulente, che dettaglia l'elemento di lavoro e lo reinvia al revisore aziendale.
- Un'attività per il revisore predefinito, che esegue l'attività se risulta impossibile contattare il revisore aziendale o il consulente.
- Un'attività per il tecnico, che implementa la richiesta e completa l'elemento di lavoro.

Cronologia delle richieste in linea

La funzionalità di cronologia delle richieste in linea consente ai partecipanti di creare un record contenente le azioni eseguite sugli elementi di lavoro. Poiché la responsabilità relativa all'elemento di lavoro passa da un partecipante all'altro, il nuovo partecipante sarà in grado di analizzare la cronologia dell'elemento di lavoro prima di decidere.

Per implementare la cronologia della richiesta in linea, vengono utilizzati due controlli:

- La Visualizzazione cronologia è in modalità di sola lettura e contiene i dettagli delle precedenti voci di cronologia in ordine cronologico.
- L'Editor cronologia è un'area di testo in cui è possibile creare nuove voci di cronologia. È inoltre disponibile un pulsante aggiuntivo che consente di aggiungere altre voci senza inoltrare l'elemento di lavoro.

Per impostazione predefinita, l'Editor cronologia e la Visualizzazione cronologia sono visualizzati nelle schede Richiesta per tutte le attività associate all'implementazione delle richieste in linea. Nella seguente figura sono illustrati i controlli della cronologia nell'attività Precisa richiesta in linea.

Precisa richiesta

Profilo soggetto

Un utente autorizzato ad approvare la richiesta ha richiesto ulteriori informazioni prima di procedere. I commenti di tale utente dovrebbero comparire nella cronologia della richiesta. Fornire le informazioni aggiuntive e fare clic su Restituisci per rinviare la richiesta al revisore. In alternativa, fare clic su Annulla per ritirare tale richiesta in modo permanente.

Richiesta e cronologia:

Origine	Descrizione	▲ Ora
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Promuovere "SalesDir" a "SalesVP"	2007-09-28 14:56:31.127
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Perché non "SalesVeep"?	2007-09-28 15:03:16.093
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	D'accordo, "SalesVeep"	2007-09-28 15:14:16.093

Informazioni aggiuntive

Aggiungi storia evento

Storia Editor

Storia di visualizzazione

Ritorna

Annullare la richiesta

Riserva elemento

Chiudi

Utilizzo delle richieste in linea

Nei seguenti passaggi viene illustrato il processo del flusso di lavoro relativo alle richieste in linea. Per ogni passaggio, viene indicata tra parentesi l'attività IM generata. In corrispondenza di ogni passaggio del processo, il partecipante può aggiungere un commento nell'Editor cronologia. Tale commento risulterà visibile nella Visualizzazione cronologia stessa al successivo partecipante del processo del flusso di lavoro.

1. L'iniziatore dell'attività richiede una modifica ad un utente IM (Crea richiesta in linea).
2. Il revisore aziendale riceve un elemento di lavoro e procede in uno dei seguenti modi:
 - Approva l'elemento di lavoro (Approva Richiesta in linea).
 - Rifiuta l'elemento di lavoro e termina il processo del flusso di lavoro. Non verrà generata alcuna nuova attività.
 - Richiede un chiarimento al consulente (Precisa richiesta in linea).
3. Il consulente riceve un elemento di lavoro e procede in uno dei seguenti modi:
 - Aggiunge un chiarimento e passa l'elemento di lavoro al revisore aziendale. Non verrà generata alcuna nuova attività.
 - Annulla l'elemento di lavoro e termina il processo del flusso di lavoro. Non verrà generata alcuna nuova attività.
4. Il tecnico riceve un elemento di lavoro ed implementa la richiesta (Implementa richiesta in linea).

Comandi operazione del flusso di lavoro

Le attività di approvazione in CA Identity Manager presentano i pulsanti di azione Approva e Rifiuta mostrati sulle schermate dell'elemento di lavoro corrispondente. I pulsanti di azione del flusso di lavoro consentono agli amministratori di estendere la funzionalità delle attività e dei flussi di lavoro di CA Identity Manager grazie all'aggiunta di pulsanti di azione per le attività di approvazione e la rimozione o la modifica dei pulsanti esistenti. I pulsanti Approva e Rifiuta standard vengono implementati come i pulsanti di azione del flusso di lavoro personalizzati.

Ad esempio, un processo del flusso di lavoro potrebbe richiedere un'azione che consenta ai partecipanti di livello intermedio di delegare determinati casi ai partecipanti di supervisione per l'approvazione o il rifiuto finale. I partecipanti di livello intermedio possono aggiungere un commento o un consiglio con l'editor cronologia e inviare l'elemento di lavoro al partecipante di supervisione perché lo riveda ai fini dell'approvazione o del rifiuto.

L'aggiunta o la rimozione dei pulsanti di azione del flusso di lavoro richiede modifiche appropriate al processo del flusso di lavoro di WorkPoint che fornisce la logica aziendale per la gestione di queste nuove azioni.

Ulteriori informazioni:

[Configurazione dei pulsanti in CA Identity Manager](#) (a pagina 343)

[Pulsanti del flusso di lavoro nelle attività di approvazione](#) (a pagina 343)

[Configurazione dei comandi in WorkPoint Designer](#) (a pagina 346)

Pulsanti del flusso di lavoro nelle attività di approvazione

I comandi operazione del flusso di lavoro corrispondono ai nodi delle transizioni che partono dai nodi delle attività manuali nel diagramma di un processo di WorkPoint. Ad esempio, nel processo di consulenza il nodo dell'attività relativa al tecnico è associata ad un'unica transizione denominata Implementato. Ciò corrisponde al pulsante "Implementato" disponibile nell'attività di approvazione della richiesta in linea, come illustrato nella seguente figura.

Implementa richiesta	Profilo soggetto	Assegnatari												
La richiesta descritta per le modifiche all'utente di cui è stato fornito il profilo è stata approvata e dovrebbe essere attuata. Avviare le attività utilizzando i comandi forniti per implementare la richiesta. In seguito, fare clic su Implementato per chiudere la richiesta. Richiesta e cronologia: <table border="1"> <thead> <tr> <th>Origine</th> <th>Descrizione</th> <th>▲ Ora</th> </tr> </thead> <tbody> <tr> <td>Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente</td> <td>Promuovere "SalesDir" a "SalesVP"</td> <td>2007-09-28 14:56:31.127</td> </tr> <tr> <td>Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente</td> <td>Abbiamo bisogno di un rappresentante Aussie, in modo che la donna non si spostano a Sydney.</td> <td>2007-09-28 15:03:16.093</td> </tr> <tr> <td>Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente</td> <td>Deve coprire anche la Nuova Zelanda?</td> <td>2007-09-28 15:14:16.093</td> </tr> </tbody> </table> Commenti La SalesRepAsia account utente è stato attuato, come richiesto. Aggiungi Utilizzare queste attività per implementare la richiesta:			Origine	Descrizione	▲ Ora	Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Promuovere "SalesDir" a "SalesVP"	2007-09-28 14:56:31.127	Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Abbiamo bisogno di un rappresentante Aussie, in modo che la donna non si spostano a Sydney.	2007-09-28 15:03:16.093	Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Deve coprire anche la Nuova Zelanda?	2007-09-28 15:14:16.093
Origine	Descrizione	▲ Ora												
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Promuovere "SalesDir" a "SalesVP"	2007-09-28 14:56:31.127												
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Abbiamo bisogno di un rappresentante Aussie, in modo che la donna non si spostano a Sydney.	2007-09-28 15:03:16.093												
Commento utente da SuperAdmin (SuperAdmin), in qualità di Richiedente	Deve coprire anche la Nuova Zelanda?	2007-09-28 15:14:16.093												

Flusso di lavoro pulsante di azione → Implementato Riserva elemento Chiudi

Nota: i pulsanti "Riserva elemento" e "Chiudi" sono gestiti dalla logica di programmazione di CA Identity Manager e non sono controllati dal flusso di lavoro.

Ulteriori informazioni:

[Comandi operazione del flusso di lavoro](#) (a pagina 342)

[Configurazione dei pulsanti in CA Identity Manager](#) (a pagina 343)

Configurazione dei pulsanti in CA Identity Manager

Per configurare un comando operazione del flusso di lavoro, fare clic sul pulsante denominato Comandi operazione del flusso di lavoro disponibile nella scheda Profilo di un'attività di approvazione.

In questa scheda Profilo è disponibile una tabella con una riga per ogni comando operazione del flusso di lavoro. Ogni riga include le seguenti quattro proprietà, che corrispondono alle colonne della tabella:

Visualizza nome

Nome visualizzato sul pulsante nella schermata di approvazione. Il nome è un valore localizzato in modo condizionale, che può essere una stringa oppure una chiave di stringa localizzata in un file di risorse.

Azione

Valore passato al processo del flusso di lavoro quando l'opzione viene selezionata. Questo valore è un attributo del nodo della transizione corrispondente nel diagramma del processo di WorkPoint. Il valore è una stringa non localizzata. Le impostazioni predefinite sono Approvato e Rifiutato.

Descrizione comando

Breve descrizione dell'azione del pulsante visualizzata quando l'utente posiziona il cursore del mouse sul pulsante. La descrizione comando è un valore localizzato in modo condizionale, che può essere una stringa oppure una chiave di stringa localizzata in un file di risorse.

Descrizione estesa

Descrizione estesa dell'azione del pulsante. Consente di aggiungere un messaggio che descrive l'azione nella schermata "Visualizza attività inoltrate". Se la descrizione è vuota, il messaggio riportato nella schermata "Visualizza attività inoltrate" corrisponde al nome del pulsante. Il nome è un valore localizzato in modo condizionale, che può essere una stringa oppure una chiave di stringa localizzata in un file di risorse.

Ulteriori informazioni:

[Configurazione dei comandi in WorkPoint Designer](#) (a pagina 346)

Aggiunta di comandi operazione del flusso di lavoro

Per aggiungere un nuovo comando a un processo del flusso di lavoro esistente, eseguire i passaggi ad alto livello riportati di seguito:

1. Aggiungere il comando del flusso di lavoro in Identity Manager.

Per istruzioni, vedere [Aggiunta di un comando operazione del flusso di lavoro](#) (a pagina 345).

2. Se necessario, aggiungere tasti di localizzazione.

Per istruzioni, consultare la *Guida alla configurazione*.

3. Aggiungere tutti i nodi richiesti in WorkPoint Designer.
Per istruzioni, consultare la Guida in linea di WorkPoint Designer.
4. Definire uno script nel nodo transizione di WorkPoint Designer.
Per istruzioni, vedere [Configurazione dei comandi in WorkPoint Designer](#) (a pagina 346).

Ulteriori informazioni:

[Configurazione dei comandi in WorkPoint Designer](#) (a pagina 346)
[Aggiunta di un comando operazione del flusso di lavoro](#) (a pagina 345)

Aggiunta di un comando operazione del flusso di lavoro

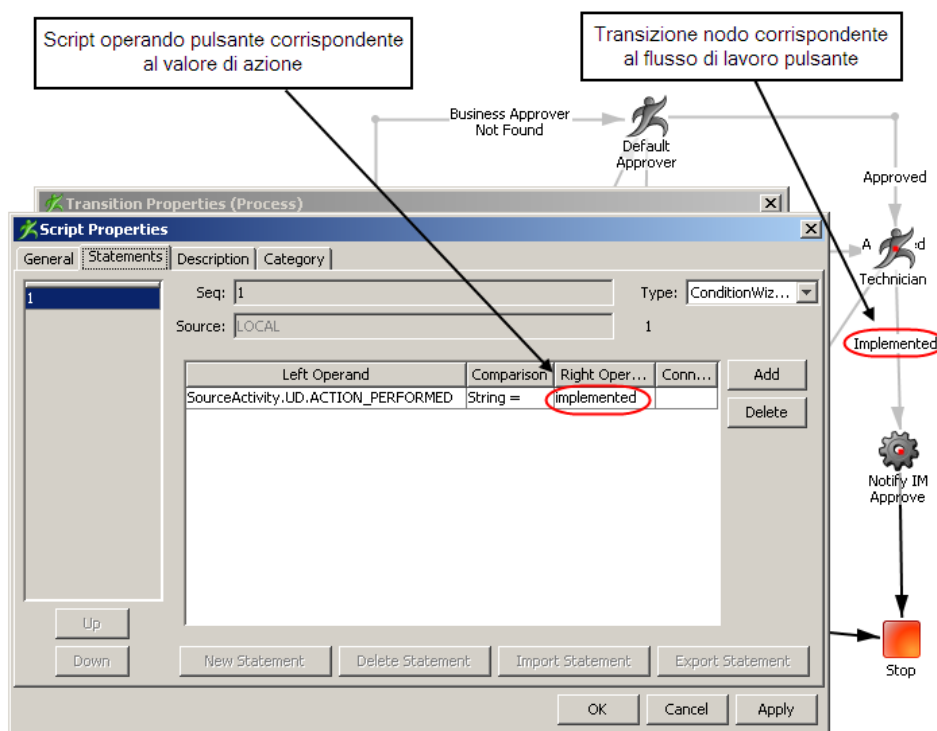
CA Identity Manager consente di aggiungere pulsanti di azione del flusso di lavoro alle attività di approvazione.

Come aggiungere un comando operazione del flusso di lavoro a un'attività di amministrazione

1. Nella Console utente, selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
Verrà visualizzato la schermata Selezionare attività di amministrazione.
2. Cercare l'attività di approvazione e fare clic su Seleziona.
Verrà visualizzato la schermata Modifica attività di amministrazione.
3. Nella scheda Profilo, fare clic sul pulsante Comandi operazione del flusso di lavoro.
Verrà visualizzata la scheda Profilo comando operazione del flusso di lavoro.
4. Fare clic su "Aggiungi pulsante" per aggiungere un nuovo comando all'attività di approvazione.
5. Immettere le informazioni sulle proprietà del comando.
6. Fare clic su OK.
Le informazioni sul nuovo pulsante vengono salvate in CA Identity Manager.
7. Fare clic su Inoltra.
La modifica all'attività viene elaborata in CA Identity Manager.

Configurazione dei comandi in WorkPoint Designer

In WorkPoint Designer, i pulsanti azione del flusso di lavoro vengono configurati tramite le proprietà degli script dei nodi di transizione, come illustrato nella figura seguente:



Per impostazione predefinita, per i comandi operazione del flusso di lavoro vengono utilizzate le proprietà di script riportate di seguito per l'esecuzione di un confronto tra stringhe:

- Operando di sinistra--ACTION_PEFORMED, definito nelle proprietà Dati utente del nodo attività manuale precedente.
- Operando di destra--Valore di azione del pulsante, definito nella scheda del profilo del comando nella Console utente.

Nota: per informazioni sugli script e le proprietà di nodi attività e nodi transizione, consultare la Guida in linea di WorkPoint Designer.

Ulteriori informazioni:

[Configurazione dei pulsanti in CA Identity Manager](#) (a pagina 343)

Elenchi ed elementi di lavoro

Un *elenco di lavoro* è un elenco di elementi di lavoro (o attività di approvazione) visualizzato nella console utente del partecipante autorizzato all'approvazione dell'attività. Gli elementi di lavoro corrispondono ad attività manuali in un processo del flusso di lavoro. Gli elementi di lavoro sono rappresentati come righe nell'elenco di lavoro.

È possibile aggiungere elementi ad un elenco di lavoro in uno dei modi descritti di seguito:

- Determinazione di un elenco di revisori da parte di un Resolver partecipante.
- Ricezione di elementi di lavoro delegati da un altro utente.
- Riassegnazione ad un altro utente.

È possibile rimuovere elementi da un elenco di lavoro in uno dei modi descritti di seguito:

- Completamento (approvazione o rifiuto) dell'elemento di lavoro.
- Riassegnazione ad un altro utente.
- Riserva dell'elemento. In questo modo, l'elemento viene rimosso dall'elenco dei lavori di tutti gli altri partecipanti.

Nota: quando si accetta o rifiuta un elemento di lavoro, la modifica non è immediata. Ad esempio, se si rifiuta un elemento di lavoro, tale elemento continuerà ad apparire nell'elenco lavori finché il processo del flusso di lavoro non avrà registrato l'informazione e fatto avanzare il processo al nodo successivo.

Le schede Informazioni visualizzate per un elemento di lavoro dipendono dal fatto che tale elemento sia stato generato dal flusso di lavoro con controllo a livello di attività o di evento:

- **Profilo:** fornisce informazioni sul profilo relative all'oggetto su cui agisce l'evento (solo a livello di evento).
- **Dettagli sull'attività:** fornisce informazioni dettagliate relative a tutti gli eventi in un'attività (solo a livello di attività).
- **Responsabili dell'approvazione:** fornisce un elenco di tutti i singoli responsabili dell'approvazione e deleganti dell'attività o dell'evento (a livello di attività e di evento).

Visualizzazione di un elenco lavori

L'elenco lavori viene visualizzato automaticamente quando si accede alla console utente se l'utente è stato assegnato come partecipante per l'approvazione di attività o elementi di lavoro iniziati da altri utenti.

Come visualizzare manualmente l'elenco lavori personale

1. Nella Console utente, selezionare Principale, Visualizza elenco lavori personali.
Verrà visualizzato l'elenco dei lavori personali.
2. Fare clic sul nome di un elemento di lavoro per visualizzarlo.
Verrà visualizzato l'elemento di lavoro selezionato.

Gli amministratori possono gestire gli elementi di lavoro per gli utenti che rientrano nel loro ambito.

Nota: la gestione degli elementi di lavoro di un utente consente agli amministratori di riservarli. La visualizzazione dell'elenco lavori di un utente non consente di apportare alcun tipo di modifica agli elementi.

Come visualizzare l'elenco lavori di un altro utente

1. Nella Console utente, selezionare Utenti, Gestisci elementi di lavoro, Visualizza elenco di lavoro utente.
Verrà visualizzato una schermata Seleziona utente.
2. Cercare l'utente di cui si desidera visualizzare l'elenco lavori e fare clic su Seleziona.
Verrà visualizzato la schermata dell'elenco lavori dell'utente.

Come gestire elementi di lavoro per un altro utente

1. Nella Console utente, selezionare Utenti, Gestisci elementi di lavoro, Gestisci elementi di lavoro dell'utente.
Verrà visualizzato una schermata Seleziona utente.
2. Cercare l'utente di cui si desidera gestire gli elementi di lavoro e fare clic su Seleziona.
Verrà visualizzato la schermata dell'elenco lavori dell'utente.
3. Fare clic sul nome di un elemento di lavoro per visualizzarlo.
Verrà visualizzato l'elemento di lavoro selezionato.

Attivazione della schermata di ricerca Elenco di lavoro

È possibile abilitare le schermate di ricerca pre-configurate per trovare elementi di lavoro.

1. Nella console di gestione, accedere a Pagina principale, Ambienti <ambiente>, Ruoli.
2. Fare clic su Importa. Importare il file worklistsearch.xml da questa posizione:
<Percorso_installazione>\CA\IdentityManager\IAM Suite\Identity Manager\tools\worklistsearch
3. Fare clic su Fine.
4. Accedere all'ambiente CA Identity Manager.
5. Nella Console utente, selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
6. Effettuare la ricerca e selezionare l'attività Visualizza elenco lavori personali.
7. Selezionare la scheda Ricerca. Fare clic su Sfoglia.
Viene visualizzato un elenco di definizioni di schermata.
8. Fare clic su Nuovo.
Viene visualizzato un elenco dei nuovi tipi di schermata.
9. Selezionare Schermata di ricerca Elenco di lavoro e fare clic su OK.
10. Immettere i dettagli per configurare la schermata di ricerca Elenco di lavoro e fare clic su OK.
La nuova schermata di ricerca viene aggiunta all'elenco delle definizioni di schermata.

Riserva di elementi di lavoro

È possibile riservare un elemento di lavoro per "estrarlo" e rimuoverlo dall'elenco lavori degli altri partecipanti. Riservando un elemento di lavoro questo viene mantenuto per l'utente che lo ha riservato.

Se l'utente in questione rilascia l'elemento di lavoro, questo torna disponibile nell'elenco lavori degli altri partecipanti. Se l'utente approva o rifiuta l'elemento di lavoro, questo viene completato e non sarà più disponibile per gli altri partecipanti.

Ulteriori informazioni:

[Delega ed elementi di lavoro riservati](#) (a pagina 350)

[Riassegnazione ed elementi di lavoro riservati](#) (a pagina 350)

Riassegnazione ed elementi di lavoro riservati

Se un utente dispone di un elemento di lavoro riservato durante la sua riassegnazione, l'elemento viene mantenuto riservato all'utente. Tuttavia, se in seguito l'utente rilascia l'elemento di lavoro, non sarà più in grado di accedervi.

Un amministratore può riassegnare, riservare o rilasciare l'elemento di lavoro di un altro utente, ma non può approvarlo o rifiutarlo. Solo un partecipante a cui è stato assegnato l'elemento di lavoro può approvarlo o rifiutarlo.

Ulteriori informazioni:

[Riassegnazione degli elementi di lavoro](#) (a pagina 356)

Delega ed elementi di lavoro riservati

Mentre è attiva una delega, delegato o delegante possono riservare un elemento di lavoro. Un elemento di lavoro riservato da un utente non può comparire nell'elenco lavori di un altro.

Ad esempio, se un delegato ha un elemento di lavoro riservato mentre la delega viene ritirata, l'elemento viene mantenuto riservato al delegato. Tuttavia, se in seguito il delegato rilascia l'elemento di lavoro, non sarà più in grado di accedervi.

Se un utente delegato viene eliminato mentre ha un elemento di lavoro riservato, continuerà a mantenere l'elemento di lavoro. Se, successivamente, il delegato approva l'elemento di lavoro, il controllo non potrà più determinare da chi sia stato delegato.

Se un delegato ha un elemento di lavoro riservato mentre la delega viene ritirata, mantiene l'accesso all'elemento fino a che questo non viene completato o rilasciato.

Ulteriori informazioni:

[Delega di elementi di lavoro](#) (a pagina 351)

[Riserva di elementi di lavoro](#) (a pagina 349)

Riserva o rilascio di un elemento di lavoro

Riservando un elemento di lavoro lo si "estrae" e lo si rimuove dall'elenco lavori degli altri partecipanti.

Rilasciando un elemento di lavoro riservato lo si rende disponibile nell'elenco lavori di altri partecipanti.

Nota: l'unico modo per liberare un elemento di lavoro riservato consiste nel rilasciarlo esplicitamente.

Come riservare o rilasciare un elemento di lavoro

1. Nella Console utente, selezionare Principale, Visualizza elenco lavori personali.
Verrà visualizzato l'elenco dei lavori personali.
2. Selezionare l'elemento di lavoro da riservare o rilasciare.
Verrà visualizzata la schermata dell'elemento di lavoro espanso.
3. Fare clic su Riserva elemento o su Rilascia elemento.
L'azione viene confermata da CA Identity Manager.

Delega di elementi di lavoro

La *delega* degli elementi di lavoro consente a un utente (il delegante) di specificare che un altro utente (il delegato) è autorizzato ad approvare le attività nell'elenco lavori del delegante. Un delegante può assegnare elementi di lavoro a un altro revisore nei periodi in cui non è presente in ufficio. Il delegante mantiene l'accesso completo ai propri elementi di lavoro durante il periodo di delega.

Gli elementi di lavoro delegati non vengono modificati in alcun modo. La registrazione indica se un elemento di lavoro è stato delegato.

Grazie alla delega, il delegato può “impersonare” il delegante e visualizzare gli elementi nel suo elenco lavori. Durante la visualizzazione di un elenco lavori, i delegati vedono i propri elementi di lavoro e quelli del delegante.

La delega non è transitiva. Un delegato può visualizzare solo gli elementi a lui assegnati direttamente dal delegante. Ad esempio, se l'utente A delega elementi di lavoro all'utente B e questi delega elementi di lavoro all'utente C, quest'ultimo può visualizzare solo gli elementi di lavoro appartenenti all'utente B, non quelli eventualmente delegati all'utente B dall'utente A.

Ulteriori informazioni:

[Delega ed elementi di lavoro riservati](#) (a pagina 350)

Attributo noto della delega

Per la delega viene utilizzato l'attributo noto seguente:

%DELEGATORS%

In questo attributo noto vengono memorizzati i nomi degli utenti che hanno eseguito la delega all'utente con l'attributo, oltre alla data e ora di creazione della delega.

Attivazione della delega

Per poter delegare elementi di lavoro a un altro utente è necessario aver attivato la delega dell'approvazione del flusso di lavoro. Per impostazione predefinita, la delega è disattivata.

Come attivare la delega dell'approvazione del flusso di lavoro

1. Aprire la console di gestione immettendo il seguente URL in un browser:

`http://hostname/iam/immanage`

nomehost

Consente di definire il nome di dominio completo del server in cui è installato CA Identity Manager. Ad esempio, `server.azienda.com:porta`.

2. Fare clic su Ambienti, quindi selezionare il nome dell'ambiente CA Identity Manager appropriato.
3. Fare clic su Impostazioni avanzate, quindi su Delega approvazione flusso di lavoro.
4. Selezionare la casella di controllo Attivato e fare clic su Salva.

Ulteriori informazioni:

[Delega dei propri elementi](#) (a pagina 352)

[Delega per altri utenti](#) (a pagina 355)

Delega dei propri elementi

È possibile delegare elementi di lavoro a un altro utente nei periodi in cui non si è presenti in ufficio. Il delegante mantiene l'accesso completo ai propri elementi di lavoro durante il periodo di delega.

Come delegare i propri elementi di lavoro

1. Nella console utente selezionare Principale, Assistente fuori sede.
Verrà visualizzato la schermata Assistente fuori sede.
2. Fare clic su Aggiungi utente.
Verrà visualizzato una schermata Seleziona utente.
3. Ricercare e selezionare uno o più utenti da far agire come delegati.
Gli utenti vengono aggiunti all'elenco dei delegati.
4. Fare clic su Inoltra.
L'attività viene inoltrata e la delega salvata.

Nota: gli utenti già delegati non vengono visualizzati nei risultati della ricerca quando si aggiunge un delegato.

Ulteriori informazioni:

[Attivazione della delega](#) (a pagina 352)

Delega degli elementi di lavoro basata sul tempo

Nelle versioni precedenti è possibile specificare una data di inizio per le deleghe, ma non una data di fine. Le nuove deleghe hanno la data di delega impostata su true e l'ora di inizio predefinita impostata sull'ora corrente.

Al momento della modifica è possibile cambiare l'ora e le date di inizio e fine. L'ora di fine predefinita corrisponde a una settimana dopo la data di inizio.

Per modificare le ore di inizio e fine, attenersi alla seguente procedura:

1. Nella scheda Principale della console utente, selezionare Assistente fuori sede.
2. Fare clic sull'icona a forma di matita accanto all'ID utente di cui si desidera modificare le informazioni di delega.

Verrà visualizzata la schermata Modifica informazioni delega.

3. Fare clic sul calendario accanto a Data di inizio per modificare la data di inizio della delega.

Nota: se la data di inizio delega è anteriore alla data corrente verrà visualizzato un messaggio di errore.

4. Se si desidera selezionare una data di fine, selezionare la casella di controllo Ha una data di fine.

Il campo Data di fine diventerà disponibile.

5. Fare clic sul calendario accanto a Data di fine per impostare la data di fine della delega.
6. Dopo aver impostato le date, fare clic su OK.

In alternativa, è possibile compiere le stesse operazioni dalla scheda Delega elementi di lavoro durante la creazione o la modifica di un utente.

Attivazione della delega degli elementi di lavoro basata sul tempo

Per attivare la delega degli elementi di lavoro basata sul tempo in un ambiente esistente al momento dell'aggiornamento, attenersi alla seguente procedura:

Dalla console di gestione

1. Passare alla pagina Environments (Ambienti).
2. Passare all'ambiente selezionato, Advanced Settings (Impostazioni avanzate), Work Item Delegation (Delega elementi di lavoro).
3. Deselezionare la casella di controllo Enabled (Attivato).
4. Salvare le modifiche e riavviare l'ambiente.
5. Passare ad Advanced Settings (Impostazioni avanzate), Work Item Delegation (Delega elementi di lavoro).
6. Selezionare la casella di controllo Enabled (Attivato).
7. Salvare le modifiche e riavviare l'ambiente.

Nota: questa procedura è solo per gli ambienti esistenti. La delega degli elementi di lavoro basata sul tempo è attivata per i nuovi ambienti.

Schermata Assistente fuori sede

Utilizzare la schermata Assistente fuori sede seguente per aggiungere e rimuovere delegati per i propri elementi.

Nella schermata Assistente fuori sede viene visualizzato un elenco dei delegati attuali. Oltre alle colonne che identificano il delegato, l'elenco ne comprende altre tre:

Data di inizio

Indica la data di creazione della delega.

Data di fine

Indica la data di fine della delega.

Ha delegati

Indica se il delegato ha a sua volta delegato elementi di lavoro a un altro utente.

Se si fa clic sull'icona a forma di matita accanto all'ID utente selezionato viene visualizzata la schermata Modifica informazioni delega, in cui è possibile modificare la data di inizio e specificare la data di fine della regola.

Delega per altri utenti

Gli amministratori possono delegare elementi di lavoro di un altro utente (il delegante) ad altri. Ad esempio, un utente potrebbe trovarsi inaspettatamente fuori ufficio, oppure un amministratore potrebbe aver bisogno di assegnare un carico di lavoro di grandi dimensioni a più utenti.

Gli amministratori possono delegare gli elementi di lavoro solo per gli utenti che rientrano nel loro ambito. Analogamente, possono aggiungere o rimuovere dall'elenco dei delegati solo gli utenti da loro gestiti.

Come delegare elementi di lavoro per un altro utente

1. Nella console utente selezionare Utenti, Gestisci elementi di lavoro, Delega elementi di lavoro.
Verrà visualizzato una schermata Seleziona utente.
2. Cercare l'utente di cui si desidera delegare gli elementi di lavoro (il delegante) e fare clic su Seleziona.
Verrà visualizzato una schermata Delega elementi di lavoro.
3. Fare clic su Aggiungi utente.
Verrà visualizzato una schermata Seleziona utente.
4. Cercare e selezionare uno o più utenti da far agire come delegati.
Gli utenti vengono aggiunti all'elenco dei delegati.
5. Fare clic su Inoltra.
L'attività viene inoltrata e la delega salvata.

Nota: gli utenti già delegati non vengono visualizzati nei risultati della ricerca quando si aggiunge un delegato.

Ulteriori informazioni:

[Attivazione della delega](#) (a pagina 352)

Rimozione di una delega

Se un utente accede a CA Identity Manager con deleghe attive, viene visualizzato l'avviso seguente:

Sono presenti deleghe attive. Verificare che siano ancora richieste.

Come rimuovere una propria delega

1. Nella console utente selezionare Principale, Assistente fuori sede.
Verrà visualizzato la schermata Assistente fuori sede.
2. Fare clic sul segno meno (-) corrispondente ai delegati da rimuovere.
I delegati vengono eliminati dall'elenco.
3. Fare clic su Inoltra.
L'attività viene inoltrata e la delega eliminata.

Come rimuovere una delega per un altro utente

1. Nella console utente selezionare Utenti, Gestisci elementi di lavoro, Delega elementi di lavoro.
Verrà visualizzato una schermata di ricerca utente.
2. Ricercare e selezionare l'utente di cui si desidera rimuovere le deleghe.
Verrà visualizzato l'elenco dei delegati.
3. Fare clic sul segno meno (-) corrispondente ai delegati da rimuovere.
I delegati vengono eliminati dall'elenco.
4. Fare clic su Inoltra.
L'attività viene inoltrata e la delega eliminata.

Nota: per rimuovere una delega, l'utente deve rientrare nel proprio ambito.

Riassegnazione degli elementi di lavoro

La riassegnazione consente a utenti e amministratori di modificare gli assegnatari di un elemento di lavoro dopo la sua creazione. Un amministratore può:

- Visualizzare l'elenco di lavoro di un altro utente
- Aggiungere e rimuovere assegnatari dell'elemento di lavoro
- Modificare lo stato di riserva degli elementi di lavoro

Ad esempio, un amministratore può riassegnare un elemento di lavoro o rilasciare un elemento di lavoro riservato da un utente che non lo sta utilizzando.

Se un utente, al momento della riassegnazione, dispone di un elemento di lavoro riservato, tale elemento rimane all'utente che lo aveva riservato. Tuttavia, se poi l'utente rilascia quell'elemento di lavoro, non vi ha più accesso.

Se un delegato al momento del ritiro della delega dispone di un elemento di lavoro riservato, mantiene l'accesso finché l'elemento di lavoro non viene completato o rilasciato.

Ulteriori informazioni:

[Riassegnazione ed elementi di lavoro riservati](#) (a pagina 350)

Scheda Responsabili dell'approvazione

La riassegnazione viene eseguita nella scheda relativa ai responsabili dell'approvazione degli elementi di lavoro, contenente un elenco degli attuali responsabili dell'approvazione (o assegnatari) degli elementi di lavoro. Quando si esegue la riassegnazione, si assegna l'elemento di lavoro aperto a tutti i responsabili dell'approvazione in elenco. Pertanto, per riassegnare un elemento di lavoro a un nuovo assegnatario, è necessario rimuovere anche l'assegnatario attuale.

Modalità di riassegnazione degli elementi di lavoro

La riassegnazione di un elemento di lavoro da un utente a un altro è un processo in due fasi:

- Selezione di un nuovo responsabile dell'approvazione.
- Rimozione del responsabile dell'approvazione attuale.

Nota: È necessario disporre dell'ambito degli utenti a cui si desidera effettuare la riassegnazione.

Per riassegnare il proprio elemento di lavoro

1. Selezionare Pagina principale, Visualizza elenco lavori personali.
Verrà visualizzato l'elenco dei lavori personali.
2. Selezionare un elemento di lavoro per espanderlo.
3. Selezionare la scheda Responsabili dell'approvazione.
Viene visualizzato l'elenco di tutti i responsabili dell'approvazione attuali, compreso l'utente di cui si sta gestendo l'elenco di lavoro.
4. Fare clic su Aggiungi assegnatari.
Verrà visualizzato una schermata Seleziona utente.

5. Cercare e selezionare uno o più utenti ai quali si desidera effettuare la riassegnazione.

Nota: Per le modalità di approvazione ALL (TUTTI) e SUBSET (SOTTOINSIEME), è possibile riassegnare soltanto un elemento di lavoro a *un* utente.

6. Fare clic sul pulsante di segno meno (-) per rimuovere il proprio utente dall'elenco di assegnatari.
7. Fare clic su Esegui riassegnazione.

L'elemento di lavoro viene visualizzato negli elenchi di lavoro degli utenti riassegnati.

Nota: Un amministratore può riassegnare, riservare o rilasciare un elemento di lavoro di un altro utente, ma non può approvare o rifiutare un elemento di lavoro di un altro utente. Solamente il titolare dell'elemento di lavoro può eseguire tali azioni.

Per riassegnare un elemento di lavoro di un altro utente

1. Selezionare Utenti, Gestisci elementi di lavoro, Gestisci elementi di lavoro dell'utente.

Verrà visualizzato una schermata Seleziona utente.

2. Cercare l'utente di cui si desidera riassegnare gli elementi di lavoro e fare clic su Seleziona.

Viene visualizzata la schermata Gestisci elementi di lavoro dell'utente.

3. Selezionare un elemento di lavoro per espanderlo.

4. Selezionare la scheda Responsabili dell'approvazione.

Viene visualizzato l'elenco di tutti i responsabili dell'approvazione attuali, compreso l'utente di cui si sta gestendo l'elenco di lavoro.

5. Fare clic su Aggiungi assegnatari.

Verrà visualizzato una schermata Seleziona utente.

6. Cercare e selezionare uno o più utenti ai quali si desidera effettuare la riassegnazione.
7. Fare clic sul pulsante di segno meno (-) per rimuovere l'assegnatario attuale.
8. Fare clic su Esegui riassegnazione.

L'elemento di lavoro viene visualizzato negli elenchi di lavoro degli utenti riassegnati.

Operazioni in blocco su elementi di lavoro

In questa versione di CA Identity Manager è possibile eseguire le seguenti operazioni in blocco sugli elementi di lavoro:

- Approva
- Rifiuta
- Riserva
- Rilascia

Nella console utente, la scheda di configurazione Elenco di lavoro è stata migliorata per includere la nuova casella di controllo Supporta operazioni in blocco del flusso di lavoro. Se si abilita questa casella di controllo, gli utenti possono eseguire operazioni in blocco quali l'approvazione, il rifiuto, il rilascio e la riserva degli elementi di lavoro di cui sono titolari oppure degli elementi di lavoro dei deleganti. Gli amministratori possono eseguire queste operazioni in blocco per gli elementi di lavoro solo mediante le attività Gestisci elementi di lavoro dell'utente.

Nota: non è possibile abilitare le operazioni in blocco per le attività di tipo Visualizza, quale l'attività Visualizza elenco di lavoro personale.

Configurazione della scheda Elenco di lavoro per le operazioni in blocco

Per configurare la scheda Elenco di lavoro per il supporto delle operazioni in blocco a livello di elementi di lavoro, attenersi alla procedura riportata di seguito.

Nella scheda Ruoli e attività della console utente

1. Selezionare una delle seguenti opzioni:
 - Ruoli e attività.
 - Attività, Ruoli e attività.
2. Selezionare Attività di amministrazione, Gestisci attività di amministrazione.
3. Fare clic su Cerca.
4. Selezionare Gestisci elementi di lavoro dell'utente.
5. Nella scheda Schede, fare clic sull'icona a forma di matita accanto ad Elenco di lavoro.

Verrà visualizzata la schermata di configurazione dell'elenco di lavori.
6. Selezionare Supporta operazioni di flusso di lavoro in blocco.
7. Salvare le modifiche e inoltrare l'attività.

Le operazioni in blocco per gli elementi di lavoro sono ora disponibili.

Capitolo 12: Notifiche di posta elettronica

Questa sezione contiene i seguenti argomenti:

[Notifiche di posta elettronica in CA Identity Manager](#) (a pagina 362)

[Selezione di un metodo di notifica di posta elettronica](#) (a pagina 363)

[Configurazione delle impostazioni SMTP](#) (a pagina 364)

[Configurazione di un indirizzo di posta elettronica di amministrazione univoco per ciascun ambiente](#) (a pagina 367)

[Creazione di criteri della notifica di posta elettronica](#) (a pagina 368)

[Utilizzo dei modelli di messaggio di posta elettronica](#) (a pagina 378)

Notifiche di posta elettronica in CA Identity Manager

Le notifiche di posta elettronica informano gli utenti di CA Identity Manager delle attività e degli eventi che si verificano nel sistema. Ad esempio, CA Identity Manager può inviare un messaggio di posta elettronica ai responsabili dell'approvazione quando un evento o un'attività richiede l'approvazione.

In CA Identity Manager sono disponibili i due metodi seguenti per configurare le notifiche di posta elettronica:

■ Criteri di notifica di posta elettronica

I criteri della notifica di posta elettronica consentono agli amministratori di creare, visualizzare, modificare ed eliminare le notifiche di posta elettronica utilizzando attività nella console utente. Per la creazione delle notifiche di posta elettronica non è necessaria la scrittura di codice.

Gli amministratori possono definire il contenuto di un messaggio di posta elettronica, i destinatari e il momento dell'invio. Il messaggio di posta elettronica, definito nell'editor HTML, può contenere informazioni dinamiche, quali la data attuale o informazioni sull'evento, che vengono popolate da CA Identity Manager al momento dell'invio del messaggio. Ad esempio, è possibile configurare una notifica di posta elettronica da inviare a un responsabile dell'approvazione ogni volta che viene creato un nuovo utente. Il messaggio di posta elettronica può contenere i dati di accesso dell'utente, la data di assunzione e il manager.

Nota: i criteri di notifica di posta elettronica sono [criteri di Policy Xpress](#) (a pagina 495) che vengono creati e gestiti da un set separato di attività.

■ Modelli di messaggio di posta elettronica

Con questo metodo, le notifiche di posta elettronica vengono generate da modelli e-mail. In CA Identity Manager sono disponibili modelli di messaggio di posta elettronica personalizzati che possono essere utilizzati così come sono, oppure personalizzati dagli amministratori di sistema. Gli amministratori utilizzano un'API modello e-mail per specificare il contenuto dinamico, ad esempio l'elenco dei destinatari e le informazioni sull'evento che attiva l'invio del messaggio.

In CA Identity Manager è possibile generare notifiche di posta elettronica quando si verifica quanto segue:

- Un evento o un'attività che richiede l'approvazione o il rifiuto da parte di un responsabile dell'approvazione flusso di lavoro risulta in sospeso.

Nota: se si dispone di un processo di approvazione Workpoint che prevede più attività di approvazione, la notifica di posta elettronica configurata nella console utente invia una notifica per ogni attività. Se si utilizzano i modelli e-mail per la stessa notifica, ai responsabili dell'approvazione viene inviato un solo messaggio di posta elettronica (quando l'evento raggiunge lo stato in sospeso).

- Un responsabile dell'approvazione approva un evento o un'attività.
- Un responsabile dell'approvazione rifiuta un evento o un'attività.

- Un evento o un'attività viene avviato, non riesce o viene completato
- Un utente viene creato o modificato

Per utilizzare le notifiche dei messaggi di posta elettronica di CA Identity Manager, configurare le [impostazioni SMTP](#) (a pagina 364). Se si utilizza il metodo del modello e-mail, è inoltre possibile attivare le notifiche di posta elettronica in CA Identity Manager.

Selezione di un metodo di notifica di posta elettronica

La tabella seguente riassume le differenze fra i criteri di notifica di posta elettronica e i modelli di messaggio di posta elettronica:

Attività	Attività di gestione della posta elettronica	Modelli di messaggio di posta elettronica
Configurazione delle notifiche di posta elettronica	Gli amministratori utilizzano le attività di amministrazione della Console utente per creare, modificare, visualizzare ed eliminare le notifiche di posta elettronica.	Gli amministratori modificano i modelli predefiniti negli strumenti di amministrazione di CA Identity Manager.
Configurazione del periodo di invio dei messaggi di posta elettronica	CA Identity Manager può generare notifiche di posta elettronica quando si verificano certe attività o eventi. Le attività di gestione dei messaggi di posta elettronica e i modelli di messaggio di posta elettronica supportano gli stessi eventi e attività, tuttavia le attività di gestione della posta elettronica forniscono in alcuni casi più granularità. Le notifiche di posta elettronica sono supportate per le attività e gli eventi seguenti: ■ Un evento o un'attività che richiede l'approvazione o il rifiuto da parte di un responsabile dell'approvazione flusso di lavoro risulta in sospeso. ■ Nota: se si dispone di un processo di approvazione Workpoint che prevede più attività di approvazione, la notifica di posta elettronica configurata nelle attività di gestione della posta elettronica invia una notifica per ogni attività. Se si utilizzano i modelli e-mail per la stessa notifica, ai responsabili dell'approvazione viene inviato un solo messaggio di posta elettronica (quando l'evento raggiunge lo stato in sospeso). ■ Un responsabile dell'approvazione approva un evento o un'attività. ■ Un responsabile dell'approvazione rifiuta un evento o un'attività. ■ Un evento o un'attività viene avviato, non riesce o viene completato ■ Un utente viene creato o modificato	

Attività	Attività di gestione della posta elettronica	Modelli di messaggio di posta elettronica
Aggiunta di contenuto dinamico ai messaggi di posta elettronica	Gli amministratori aggiungono contenuto dinamico al corpo di un messaggio di posta elettronica selezionando un'opzione da un elenco di opzioni nella scheda Contenuto delle attività di creazione o modifica dei messaggi di posta elettronica. CA Identity Manager popola automaticamente il contenuto dinamico in base alle informazioni sull'attività o evento che attiva la notifica.	Gli amministratori utilizzano l'API del modello di messaggio di posta elettronica per personalizzare i modelli di messaggio di posta elettronica predefiniti, utilizzati per generare le notifiche di posta elettronica.
Supporto per le notifiche di posta elettronica esistenti	Le notifiche di posta elettronica configurate mediante le attività di gestione della posta elettronica si basano su criteri di Policy Xpress. Se si eseguisse l'aggiornamento da CA Identity Manager Option Pack 1 a CA Identity Manager 12.6.5, le notifiche di posta elettronica configurate in Policy Xpress continueranno a funzionare. Tuttavia, tali notifiche vengono gestite mediante le attività di gestione della posta elettronica, invece di Policy Xpress.	Le notifiche di posta elettronica create utilizzando il metodo dei modelli di messaggio di posta elettronica in versioni precedenti di CA Identity Manager continueranno a funzionare in CA Identity Manager 12.6.5.

Configurazione delle impostazioni SMTP

Prima di abilitare le notifiche di posta elettronica, configurare le impostazioni SMTP. Consultare le sezioni seguenti per configurare le impostazioni SMTP per il server applicazioni.

Configurazione delle impostazioni SMTP su JBoss

1. In un editor di testo, aprire il descrittore di distribuzione del servizio di posta elettronica nel modo seguente:

Nodo singolo: *jboss_home\server\default\deploy\mail-service.xml*

Cluster: *jboss_home\server\all\deploy\mail-service.xml*

2. Modificare la proprietà mail.smtp.host con il nome del server SMTP nel modo seguente:

```
<-- Change to the SMTP gateway server -->
```

```
<property name="mail.smtp.host" value="your_smtp_server" />
```

Ad esempio:

```
<property name="mail.smtp.host" value="smtp.mailserver.company.com" />
```

3. Salvare il file mail-service.xml.
4. In un editor di testo, aprire il file di proprietà della posta elettronica seguente:

Nodo singolo:

jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

Cluster: *jboss_home\server\all\farm\iam_im.ear\config\com\netegrity\config\email.properties*

5. Per impostare l'indirizzo di risposta del messaggio di posta elettronica utilizzato dal messaggio di posta elettronica generato dal flusso di lavoro, individuare la proprietà admin.email.address e impostare il valore con l'indirizzo di posta elettronica appropriato. Ad esempio:

```
admin.email.address=admin@company.com
```

6. Se si utilizza il metodo del modello di messaggio di posta elettronica, abilitare le notifiche di posta elettronica nella console di gestione.

Non è necessario abilitare le notifiche di posta elettronica nella console di gestione se si stanno utilizzando criteri di notifica di posta elettronica.

Configurazione delle impostazioni SMTP su WebLogic

Si configurano le impostazioni della posta elettronica nella console di amministrazione server WebLogic e nel file `email.properties`.

Per configurare le impostazioni di posta elettronica per WebLogic

1. Nella console di amministrazione server WebLogic, creare una sessione di messaggio di posta con le proprietà seguenti:
 - proprietà **mail.smtp.host**: impostare questo valore sul server SMTP. Ad esempio, `mail.smtp.host=mymailserver.company.com`
 - proprietà **mail.transport.protocol**: impostare questo valore su SMTP. Ad esempio, `mail.transport.protocol=smtp`
 - **JNDI Name**: `nete/Mail`
 - **Destinazione**: il nome del server WebLogic
2. In un editor di testo, aprire il file di proprietà della posta elettronica di CA Identity Manager seguente:
`weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties`
3. Impostare l'indirizzo di risposta al messaggio di posta elettronica utilizzato dai messaggi di posta elettronica generati dal flusso di lavoro individuando la proprietà `admin.email.address` e impostando il valore sull'indirizzo e-mail appropriato. Ad esempio:
`admin.email.address=admin@company.com`
4. Abilitare la notifica di posta elettronica nella console di gestione.
Nota: non è necessario abilitare le notifiche di posta elettronica nella console di gestione se si stanno utilizzando criteri di notifica di posta elettronica.

Configurazione delle impostazioni SMTP su WebSphere

L'utilità `imsSetup` eseguita dopo avere installato i componenti di CA Identity Manager configura un nuovo oggetto di sessione di posta elettronica chiamato `mailMail`.

Perché la funzionalità di notifica di posta elettronica funzioni correttamente, specificare il server al quale WebSphere si connette quando invia un messaggio di posta elettronica nel campo `Mail Transport Host` per la sessione `mailMail`.

La sessione mailMail si trova in Risorse, Mail Providers (Provider di posta elettronica), Mail Sessions (Sessioni di posta elettronica), mailMail nella console di amministrazione di WebSphere.

Nota: per visualizzare l'oggetto mailMail, modificare l'opzione Scope to Server (Ambito a Server) nella schermata Mail Session (Sessione di posta elettronica). Se non si modifica l'ambito a Server, l'oggetto mailMail non viene visualizzato.

Per ulteriori informazioni sulla configurazione del provider di posta di WebSphere, consultare la documentazione di WebSphere.

Se si sta utilizzando il metodo dei modelli di messaggio di posta elettronica, abilitare la notifica di posta elettronica nella console di gestione dopo avere configurato le impostazioni SMTP.

Nota: non è necessario abilitare le notifiche di posta elettronica nella console di gestione se si stanno utilizzando criteri di notifica di posta elettronica.

Configurazione di un indirizzo di posta elettronica di amministrazione univoco per ciascun ambiente

È possibile configurare un unico indirizzo di posta elettronica di amministrazione per ciascun ambiente CA Identity Manager.

Procedere come descritto di seguito::

1. Nella Console di gestione, fare clic su Ambienti.
Viene visualizzato l'elenco degli ambienti di CA Identity Manager.
2. Selezionare un ambiente CA Identity Manager.
3. Accedere a Impostazioni avanzate, Posta elettronica.
4. Nel campo Indirizzo di posta elettronica amministratore, specificare un indirizzo per l'ambiente.
5. Fare clic su Salva.
6. Fare clic su Restart environment (Riavvia ambiente).

È ora possibile suddividere i messaggi provenienti dai diversi ambienti CA Identity Manager durante la ricezione di notifiche di posta elettronica da diversi indirizzi per ciascun ambiente CA Identity Manager.

Creazione di criteri della notifica di posta elettronica

È possibile utilizzare la console utente per creare criteri della notifica di posta elettronica che determinano l'invio di messaggi di posta elettronica quando vengono eseguite specifiche azioni. Ad esempio, è possibile creare un criterio per l'invio di un messaggio di notifica ai responsabili dell'approvazione ogni volta che viene creato un nuovo utente.

Procedere come descritto di seguito:

1. Selezionare Sistema, Messaggio di posta elettronica, Crea messaggio di posta elettronica.
2. Selezionare una delle seguenti opzioni:
 - Crea un nuovo oggetto di tipo Posta elettronica gestita
 - Crea una copia di un oggetto di tipo Posta elettronica gestita

Consente di utilizzare un criterio della notifica di posta elettronica esistente come modello per la creazione di un criterio.
3. Inserire le informazioni di base sul criterio della notifica di posta elettronica nella scheda Profilo.
4. Specificare quando sarà inviato il messaggio di posta elettronica da CA Identity Manager nella scheda Invia messaggi con stato.

Nella scheda Invia messaggi con stato sono disponibili varie opzioni per specificare le azioni che attivano le notifiche di posta elettronica.
5. Specificare i destinatari del messaggio di posta elettronica nella scheda Destinatari.
6. Definire l'oggetto e il contenuto del messaggio di posta elettronica nella scheda Contenuto.

Nel contenuto del messaggio di posta elettronica è possibile specificare contenuto dinamico, ad esempio la data, il nome dell'attività o dell'evento e gli attributi utente.

Ulteriori informazioni:

[Scheda Invia messaggi con stato](#) (a pagina 370)

[Scheda Destinatari](#) (a pagina 372)

[Contenuto](#) (a pagina 374)

[Scheda Profilo delle notifiche di posta elettronica](#) (a pagina 369)

Scheda Profilo delle notifiche di posta elettronica

La scheda Profilo nelle attività di gestione della posta elettronica consente di specificare informazioni di base su un criterio della notifica di posta elettronica. Questa scheda contiene i campi seguenti:

Nome messaggio di posta elettronica

Consente di identificare il criterio della notifica di posta elettronica nella console utente.

Nota: quando il messaggio di posta elettronica viene inviato, il nome del messaggio non viene visualizzato. Il nome viene utilizzato solo per gestire il criterio della notifica di posta elettronica nella console utente.

Categoria

Consente di raggruppare i criteri della notifica di posta elettronica per semplificare la gestione.

Specificare una categoria esistente selezionandola dall'elenco a discesa, oppure selezionare il secondo pulsante di opzione e inserire il nome di una nuova categoria.

Descrizione

Consente di descrivere il criterio della notifica di posta elettronica agli amministratori.

Quando il messaggio di posta elettronica viene inviato, la descrizione non viene visualizzata.

Attivato

Consente di specificare che quando saranno soddisfatte le condizioni definite nella scheda Invia messaggi con stato, CA Identity Manager invierà il messaggio di posta elettronica.

Dati personalizzati

Consente di creare un elemento dati personalizzato in Policy Xpress, utilizzabile per configurare destinatari o contenuti personalizzati.

È inoltre possibile utilizzare gli elementi dati personalizzati come parametri per altri elementi dati.

Nota: per ulteriori informazioni sugli elementi dati, fare riferimento alla sezione [Dati](#) (a pagina 502).

Facendo clic su Dati personalizzati verrà visualizzata una schermata in cui è possibile aggiungere nuovi elementi dati.

Regole di ingresso

Consente di definire regole in base alle quali in CA Identity Manager vengono inviate notifiche di posta elettronica, nei casi in cui le regole predefinite nella scheda Invia messaggi con stato non sono sufficientemente granulari.

Ad esempio, nella scheda Invia messaggi con stato è disponibile una regola predefinita che prevede l'invio del messaggio di posta elettronica in caso di modifica di qualsiasi attributo di un profilo utente. Se si desidera che CA Identity Manager invii un messaggio di posta elettronica solo quando viene modificato il dipartimento di un utente, è possibile creare una regola di ingresso personalizzata. (In questo caso, si crea un elemento dati personalizzato che identifica quando il dipartimento viene modificato, quindi si crea una regola di ingresso che utilizza l'elemento dati personalizzato creato.)

Nota: per ulteriori informazioni, fare riferimento alla sezione [Regole di ingresso](#) (a pagina 505).

Scheda Invia messaggi con stato

In CA Identity Manager sono disponibili diverse opzioni predefinite per stabilire quando deve essere inviato il messaggio di posta elettronica. Per alcune di queste opzioni sono necessarie informazioni aggiuntive, ad esempio il nome di un'attività o di un evento. Ad esempio, per inviare un messaggio di posta elettronica all'avvio di un'attività è necessario selezionare l'attività che attiva l'invio del messaggio.

Per Invia messaggi con stato è possibile selezionare una o più delle seguenti opzioni:

Utente creato

Consente di inviare un messaggio di posta elettronica dopo la creazione di un utente. Il messaggio viene inviato al completamento dell'evento CreateUserEvent.

Utente modificato

Consente di inviare un messaggio di posta elettronica dopo la modifica di un utente. Il messaggio viene inviato al completamento dell'evento ModifyUserEvent.

Flusso di lavoro in sospeso

Consente di inviare un messaggio di posta elettronica quando un processo del flusso di lavoro assegna un responsabile dell'approvazione. Se si seleziona questa opzione è necessario specificare i processi del flusso di lavoro applicabili. Il messaggio di posta elettronica definito con questo criterio invia un messaggio di posta elettronica individuale ai responsabili dell'approvazione a ogni fase del processo del flusso di lavoro selezionato.

Indirizzo di posta elettronica - Flusso di lavoro in sospeso

Consente di inviare un messaggio di posta elettronica quando un processo del flusso di lavoro raggiunge un'attività specificata. Se si seleziona questa opzione è necessario specificare i processi del flusso di lavoro applicabili. Il messaggio di posta elettronica definito con questo criterio invia una notifica di posta elettronica per ciascuna fase di approvazione.

Inizio evento

Consente di inviare un messaggio di posta elettronica quando un evento raggiunge lo stato Prima. Quando si seleziona questa opzione, specificare l'evento.

Nota: se l'opzione Inizio evento viene specificata e il messaggio di posta elettronica non viene inviato, l'evento associato alla notifica non verrà eseguito.

Evento terminato

Consente di inviare un messaggio di posta elettronica quando un evento raggiunge lo stato Dopo. Quando si seleziona questa opzione, specificare l'evento.

Evento approvato

Consente di inviare un messaggio di posta elettronica quando un evento raggiunge lo stato Approvato. Quando si seleziona questa opzione, specificare l'evento.

Evento rifiutato

Consente di inviare un messaggio di posta elettronica quando un evento raggiunge lo stato Rifiutato. Quando si seleziona questa opzione, specificare l'evento.

Evento non riuscito

Consente di inviare un messaggio di posta elettronica quando un evento non riesce. Quando si seleziona questa opzione, specificare l'evento.

Attività inviata

Consente di inviare un messaggio di posta elettronica quando inizia l'elaborazione dell'attività. Quando si seleziona questa opzione, specificare l'attività.

Attività completata

Consente di inviare un messaggio di posta elettronica quando l'attività viene completata. Quando si seleziona questa opzione, specificare l'attività.

Attività non riuscita

Consente di inviare un messaggio di posta elettronica se l'attività non riesce. Quando si seleziona questa opzione, specificare l'attività.

Scheda Destinatari

Nei campi A, CC o CCN di un messaggio di posta elettronica è possibile configurare più destinatari. L'elenco dei destinatari può essere statico, oppure può dipendere dal tipo di azione che attiva il messaggio di posta elettronica e dagli utenti coinvolti.

Per specificare i destinatari, selezionare l'icona Modifica in corrispondenza del campo A, CC o CCN della scheda Destinatari. Selezionare quindi una delle seguenti opzioni, che consentono di configurare l'elenco dei destinatari:

Responsabili dell'approvazione flusso di lavoro

Consente di inviare il messaggio di posta elettronica a tutti i responsabili dell'approvazione nel processo del flusso di lavoro. Questa opzione è applicabile solo se il messaggio viene inviato per un evento del flusso di lavoro in sospeso.

Manager

Consente di inviare il messaggio di posta elettronica al manager dell'utente sul quale è stata eseguita l'attività.

Nota: per utilizzare l'opzione destinatario Manager, configurare l'attributo manager per l'ambiente. Per configurare l'attributo manager, nella console di gestione accedere ad Ambienti, *NomeAmbiente*, Impostazioni avanzate, Varie. Impostare managerattribute sul nome dell'attributo fisico che memorizza il nome univoco del manager di un utente.

Per i database relazionali, specificare l'attributo nel formato seguente:

tablename.attribute

Membri del gruppo

Consente di inviare il messaggio di posta elettronica a tutti i membri di un gruppo. Selezionando questa opzione verrà visualizzato un elenco a discesa contenente i nomi dei gruppi disponibili.

Membri del ruolo

Consente di inviare il messaggio di posta elettronica a tutti i membri di un ruolo di amministrazione. Selezionando questa opzione verrà visualizzato un elenco a discesa contenente i nomi dei ruoli disponibili.

Indirizzo statico

Consente di inviare il messaggio di posta elettronica a un indirizzo specificato. È possibile specificare l'indirizzo di posta elettronica nell'area di testo aggiuntiva disponibile.

Nota: non specificare più di un indirizzo nell'area di testo.

Utente

Consente di inviare il messaggio di posta elettronica all'utente sul quale è stata eseguita l'attività.

Initiator of request (Iniziatore della richiesta)

Consente di inviare il messaggio di posta elettronica all'utente che ha effettuato la richiesta.

Personalizzato

Consente di selezionare un elemento dati personalizzato per definire i destinatari.

Selezionando questa opzione verrà visualizzato un elenco a discesa contenente gli elementi dati personalizzati disponibili.

Nota: per ulteriori informazioni sugli elementi dati, fare riferimento alla sezione [Dati](#) (a pagina 502).

Contenuto

È possibile definire l'oggetto e il corpo di un messaggio di posta elettronica utilizzando testo semplice, oppure aggiungendovi contenuto dinamico che verrà calcolato al momento dell'invio del messaggio.

La riga dell'oggetto è un campo di testo semplice in cui è possibile scrivere il messaggio. Il testo inserito costituirà l'oggetto del messaggio di posta elettronica.

Il corpo viene visualizzato in un editor HTML. È possibile inserire e formattare qualsiasi testo per comporre il corpo del messaggio di posta elettronica.

Per includere contenuto dinamico, selezionare le opzioni dall'apposito elenco a discesa. L'editor aggiungerà indicatori di contenuto dinamico simili al seguente nel punto in cui si trova il cursore:

{tipo}

tipo rappresenta uno dei tipi di contenuto dinamico supportati.

Ad esempio, quando si seleziona il contenuto dinamico Attributo e si specifica l'attributo FirstName, nella scheda Contenuto dell'editor HTML verrà visualizzato quanto segue:

{Attribute: FirstName}

Nota: per aggiungere contenuto dinamico alla riga dell'oggetto, utilizzare l'elenco a discesa sotto la riga dell'oggetto. Per aggiungere contenuto dinamico nel corpo del messaggio di posta elettronica, utilizzare l'elenco a discesa sotto la casella del contenuto.

Al momento dell'invio, il contenuto dinamico verrà sostituito con il testo appropriato. Il testo conserva la formattazione specificata nell'editor HTML, ad esempio i caratteri in grassetto.

I tipi di contenuto dinamico includono:

Data

Consente di specificare la data corrente nel formato scelto.

Attività

Consente di specificare l'attività per cui viene inviato il messaggio di posta elettronica.

Nome oggetto

Consente di specificare il nome dell'oggetto nell'evento che attiva il messaggio di posta elettronica. Nel caso di un evento utente, questo campo corrisponde al nome di accesso dell'utente.

L'oggetto non deve necessariamente essere un utente. Può trattarsi ad esempio di qualsiasi oggetto gestito, ad esempio un gruppo, un ruolo di amministrazione ecc.

Attributo

Consente di specificare il valore di uno degli attributi utente. Il soggetto dell'attività è l'utente. Per questa opzione è necessario selezionare l'attributo da un elenco a discesa.

Attributo Manager

Consente di specificare il valore di uno degli attributi del manager dell'utente. Il soggetto dell'attività è l'utente. Per questa opzione è necessario selezionare l'attributo da un elenco a discesa.

Nota: per utilizzare l'opzione destinatario Manager, configurare l'attributo manager per l'ambiente. Per configurare l'attributo manager, nella console di gestione accedere ad Ambienti, *NomeAmbiente*, Impostazioni avanzate, Varie. Impostare managerattribute sul nome dell'attributo fisico che memorizza il nome univoco del manager di un utente.

Per i database relazionali, specificare l'attributo nel formato seguente:

tablename.attribute

Personalizzato

Consente di selezionare un elemento dati personalizzato per definire i destinatari.

Selezionando questa opzione verrà visualizzato un elenco a discesa contenente gli elementi dati personalizzati disponibili.

Nota: per ulteriori informazioni sugli elementi dati, fare riferimento alla sezione [Dati](#) (a pagina 502).

Modifica di criteri della notifica di posta elettronica

È possibile modificare i criteri della notifica di posta elettronica esistenti per adattarli alle proprie esigenze aziendali.

Per modificare un criterio della notifica di posta elettronica

1. Selezionare Sistema, Messaggio di posta elettronica, Crea messaggio di posta elettronica.
CA Identity Manager mostrerà una schermata di ricerca.
2. Cercare e selezionare il criterio della notifica di posta elettronica da modificare.
3. Modificare le impostazioni nelle schede Profilo, Invia messaggi con stato, Destinatari e Contenuto secondo le necessità.

Disattivazione di criteri della notifica di posta elettronica

Nella fase di creazione o di modifica di un criterio della notifica di posta elettronica, è possibile attivare o disattivare il criterio stesso utilizzando la casella di controllo Attivato nella scheda Profilo. Quando un criterio della notifica di posta elettronica è disattivato, il messaggio di posta elettronica selezionato non è attivo e non vengono inviati messaggi.

Nota: i criteri della notifica di posta elettronica sono abilitati per impostazione predefinita.

Use Case: invio di un messaggio di posta elettronica di benvenuto

Quando viene assunto un nuovo dipendente, Forward, Inc, desidera inviare all'utente un messaggio di benvenuto nell'azienda. Il messaggio di posta elettronica deve contenere dati importanti per il nuovo dipendente, ad esempio collegamenti alla pagina iniziale del dipendente e informazioni sul manager e il dipartimento.

Per creare il messaggio, l'amministratore delle Risorse umane utilizza l'attività Crea messaggio di posta elettronica nella console utente per configurare le seguenti impostazioni:

- Nella scheda Invia messaggi con stato, selezionare Utente creato.
- Nella scheda Destinatari, completare i seguenti passaggi:
 - Fare clic sull'icona Modifica accanto al campo A.
Selezionare Utente, quindi fare clic sul segno più. Selezionare il manager con lo stesso metodo, quindi fare clic su OK.
 - Fare clic sull'icona Modifica accanto al campo CC.
Selezionare Iniziatore, fare clic sul segno più, quindi fare clic su OK per inviare una copia del messaggio di posta elettronica all'utente che ha creato il dipendente in CA Identity Manager.
- Nella scheda Contenuto, completare i seguenti passaggi:
 - Nel campo Oggetto, immettere il seguente testo: Benvenuto,
Posizionare il cursore alla fine del testo inserito e selezionare Attributo dall'elenco a discesa. Selezionare Nome completo dal secondo elenco a discesa, quindi fare clic sul segno più.
La riga dell'oggetto sarà simile alla seguente:
Benvenuto, {'Attribute: eTFullName'}
Nota: il nome dell'attributo dipende dall'archivio utente e dall'attributo utilizzati.
 - Nella casella Contenuto, aggiungere il testo di benvenuto. Includere collegamenti al portale dei dipendenti e utilizzare le opzioni relative al contenuto dinamico sotto la casella del contenuto per visualizzare il dipartimento dell'utente, il manager e il numero di telefono del manager, come descritto di seguito:

Profilo

Invia messaggi con stato

Destinatari

Contenuto

•Oggetto

Welcome, {'Attribute: cn'}

Attributo Manager

Business Phone (telephoneNumber)

+

format font size

Hello, {'Attribute: givenName'},

Welcome to Forward, Inc. We are so glad that you joined our team!

Here are some helpful links to get you started in your new role:

[Employee home page](#)

[Intranet](#)

You may also need the following information about your department and manager:

Department: {'Attribute: departmentNumber'}

Manager: {'Manager Attribute: cn'}

Manager Phone: {'Manager Attribute: telephoneNumber'}

Utilizzo dei modelli di messaggio di posta elettronica

CA Identity Manager include modelli di messaggio di posta elettronica predefiniti utilizzabili per generare messaggi di posta elettronica. È possibile utilizzare i modelli predefiniti installati o personalizzarli per adattarli alle proprie esigenze.

Per utilizzare modelli di messaggio di posta elettronica

1. Configurare le impostazioni SMTP per abilitare CA Identity Manager per l'invio delle notifiche di posta elettronica.
2. [Abilitare la notifica di posta elettronica nella console di gestione](#) (a pagina 379).
3. [Configurare un evento o attività per l'invio di posta elettronica.](#) (a pagina 379)
4. (Facoltativo) [Personalizzare i modelli predefiniti](#) (a pagina 385), secondo necessità.

Abilitazione delle notifiche di posta elettronica

È possibile abilitare o disabilitare le notifiche di posta elettronica per un ambiente di CA Identity Manager. Se si abilitano le notifiche di posta elettronica, CA Identity Manager invia notifiche di posta elettronica per gli eventi e le attività specificate.

Nota: per utilizzare la funzionalità Password dimenticata, abilitare la notifica di posta elettronica.\

Prima di abilitare le notifiche di posta elettronica in CA Identity Manager, [configurare le impostazioni SMTP](#) (a pagina 364) del server applicazioni.

Per abilitare le notifiche di posta elettronica

1. Nella Console di gestione, fare clic su Environments (Ambienti).
Viene visualizzato l'elenco degli ambienti di CA Identity Manager.
2. Fare clic sull'ambiente di Identity Manager appropriato.
3. Accedere a Impostazioni avanzate, Posta elettronica.
4. Selezionare la casella di controllo Attivato.
5. [Configurare gli eventi e le attività che attivano i messaggi di posta elettronica](#) (a pagina 379).
6. Fare clic su Salva.
7. Riavviare l'istanza del server applicazioni nel quale è installato CA Identity Manager.

Configurare un messaggio di posta elettronica per un evento o attività da inviare

Se le notifiche di posta elettronica sono abilitate, è possibile specificare un elenco di eventi e attività che le attivano. Ad esempio, è possibile inviare un messaggio di posta elettronica nei seguenti casi:

- A un amministratore di sistema, al completamento di un'attività di ripristino della password utente.
- Al manager di un nuovo dipendente, al completamento di un'attività di creazione utente. In aggiunta, quando l'evento AddToGroup generato nell'attività Crea utente viene approvato, è possibile inviare un altro messaggio di posta elettronica a tutti i membri di un gruppo a cui il nuovo utente viene aggiunto.

Per specificare eventi e attività che attivano le notifiche di posta elettronica

1. Nella Console di gestione, fare clic su Environments (Ambienti).
Viene visualizzato l'elenco degli ambienti di CA Identity Manager.
2. Fare clic sull'ambiente di CA Identity Manager appropriato.

3. Accedere a Impostazioni avanzate, Posta elettronica.
Viene visualizzata la schermata Email Properties (Proprietà posta elettronica).
4. Selezionare le seguenti caselle di controllo di abilitazione applicabili:
 - Events E-mail Enabled (Messaggio di posta elettronica eventi abilitato)
Consente di abilitare le notifiche di posta elettronica per gli eventi di CA Identity Manager
 - Tasks Email Enabled (Messaggio di posta elettronica attività abilitato)
Consente di abilitare le notifiche di posta elettronica per le attività di CA Identity Manager
5. Immettere la posizione dei modelli di messaggio di posta elettronica utilizzati da CA Identity Manager per creare i messaggi di posta elettronica.
I modelli di messaggio di posta elettronica si trovano in una sottodirectory nella posizione seguente:
`iam_im.ear\custom\emailTemplates`
Nota: quando si crea un file di modello di messaggio di posta elettronica con un nome file utilizzando una lingua diversa, la sessione del sistema operativo deve operare in una lingua che supporta il set di caratteri.
6. Specificare gli eventi per i quali le notifiche di posta elettronica vengono inviate nel modo seguente:
 - Per aggiungere un evento, selezionare l'evento nella casella di riepilogo Evento e fare clic su Aggiungi.
CA Identity Manager aggiunge l'evento selezionato all'elenco degli eventi per i quali vengono inviate le notifiche di posta elettronica.
Nota: se si seleziona un evento non associato con un processo di flusso di lavoro, CA Identity Manager invia una notifica di posta elettronica quando l'evento viene completato.
 - Per eliminare un evento, selezionare la casella di controllo dell'evento e fare clic su Elimina.

7. Specificare le attività per le quali le notifiche di posta elettronica vengono inviate nel modo seguente:
 - Per aggiungere un'attività, cercare l'attività selezionando una condizione nel primo campo e immettendo un nome di attività nel secondo campo. Fare clic su Cerca.

È possibile immettere un nome di attività parziale usando il carattere jolly (*). Per cercare, ad esempio, un'attività di creazione immettere Crea*.

Selezionare una o più attività fra i risultati della ricerca. Fare clic su Aggiungi.

Nota: le notifiche di posta elettronica a livello di attività non sono disponibili per le attività che hanno Visualizza o Autovisualizzazione come tipo di azione. Per visualizzare il tipo di azione di un'attività, accedere a Modifica attività di amministrazione, Select a Task (Seleziona un'attività), e selezionare il campo azione nel profilo dell'attività.
 - Per eliminare un'attività, selezionare la casella di controllo dell'attività e fare clic su Elimina.

L'eliminazione di un'attività consente di rimuovere l'attività dalla tabella Attività, ma non elimina l'attività.
8. Dopo aver configurato le attività e gli eventi che attivano le notifiche di posta elettronica, fare clic su Salva.
9. Riavviare il server applicazioni nel quale è installato CA Identity Manager.

Contenuto dei messaggi di posta elettronica

Le notifiche di posta elettronica sono costituite da un modello generico e dai dettagli specifici sulle attività che vengono aggiunti al messaggio di posta elettronica attraverso l'API di posta elettronica. Ad esempio, è possibile inserire le informazioni seguenti in un messaggio di posta elettronica per un'attività Crea utente:

- Nome dell'amministratore che sta eseguendo l'attività
- Nome del nuovo utente
- Indirizzo di posta elettronica dell'utente, il nome del dipartimento e altri dati di attributi
- Organizzazione in cui l'utente viene creato
- Stato di approvazione del flusso di lavoro e ora di approvazione
- Nome dell'attività e i nomi degli eventi nell'attività

Modelli di messaggio di posta elettronica

Le notifiche di posta elettronica vengono generate da modelli di messaggio di posta elettronica. Identity Manager fornisce modelli di messaggio di posta elettronica predefiniti che è possibile utilizzare così come sono installati o per creare i propri modelli di messaggio di posta elettronica.

Ciascun modello di messaggio di posta elettronica contiene quanto segue:

- **Informazioni di consegna**--Un elenco di destinatari del messaggio di posta elettronica. Identity Manager genera automaticamente l'elenco dei destinatari, in base agli utenti coinvolti nell'attività. Ad esempio, un messaggio di posta elettronica di approvazione viene inviato a tutti i responsabili dell'approvazione per quell'attività.
- **Oggetto** -- Il testo utilizzato nell'oggetto del messaggio.
- **Contenuto** -- Il testo del messaggio. Il corpo del messaggio contiene generalmente sia testo statico sia variabili, che vengono risolte in base all'attività o evento che attiva il messaggio di posta elettronica.

I modelli di messaggio di posta elettronica predefiniti si trovano nella directory emailTemplates in cui sono installati gli strumenti di amministrazione di Identity Manager. La posizione di installazione predefinita degli strumenti di amministrazione è:

- Per Windows--C:\Programmi\CA\CA Identity Manager\
- Per UNIX--<home_directory>/CA/CA Identity Manager

La directory emailTemplates contiene quattro cartelle. Ciascuna cartella viene associata a uno stato di attività o evento:

Directory	Sommario
Approvato	defaultEvent.tmpl--Informa i destinatari che un evento è stato approvato.

Directory	Sommario
Completato	■ CertificationNonCertifiedActionCompletedNotification.tmpl--Informa il manager che un'azione di non conformità è stata applicata a un dipendente. ■ CertificationNonCertifiedActionPendingNotification.tmpl--Informa il manager che un'azione di non conformità sarà applicata a un dipendente. ■ CertificationRequiredFinalNotification.tmpl--Promemoria finale a un manager per informare che è necessario completare l'attività di certificazione utente per un dipendente. ■ CertificationRequiredNotification.tmpl--Informa il manager che è iniziato il processo di certificazione per un dipendente. Il manager deve completare un'attività di certificazione utente per questo dipendente. ■ CertificationRequiredReminderNotification.tmpl--Ricorda al manager che è necessario completare l'attività di certificazione utente per un dipendente. ■ Certify Employee.tmpl--Informa un amministratore che il processo di certificazione di un dipendente è stato completato. ■ CreateProvisioningUserNotificationEvent.tmpl--Invia una password temporanea a un utente quando l'account di quell'utente viene creato nella directory di provisioning. ■ defaultTask.tmpl--Informa i destinatari che Identity Manager ha completato un'attività. ■ ForgottenPassword.tmpl--Invia una password temporanea agli utenti che hanno utilizzato la funzionalità di password dimenticata. ■ ForgottenUserID.tmpl--Invia un ID utente agli utenti che hanno utilizzato la funzionalità dell'ID utente dimenticato. ■ Self Registration.tmpl--Informa un utente che un'attività di registrazione automatica è stata completata correttamente.
In sospeso	■ defaultEvent.tmpl--Informa i responsabili dell'approvazione che una voce dell'elenco di lavoro richiede attenzione. ■ ModifyUserEvent.tmpl--Stessa azione del modello predefinito, ma include metodi per recuperare gli attributi dell'oggetto gestito dall'utente.
Rifiutato	defaultEvent.tmpl--Informa i destinatari che un evento è stato rifiutato.

Utilizzare i modelli di Identity Manager e la struttura di directory di modello installati nella directory `<im_admin_tools_dir>\Identity Manager\emailTemplates` come base per creare modelli di messaggio di posta elettronica personalizzati.

Directory di modello

Ciascuna directory modello descritta in [Modelli di messaggio di posta elettronica](#) (a pagina 382) viene associata a uno stato di attività o evento particolare. Ad esempio, se si desidera inviare un messaggio di posta elettronica per un evento rifiutato in un processo di flusso di lavoro, Identity Manager cerca il modello da utilizzare in una directory distribuita contenente modelli di rifiuto. Identity Manager genera quindi il messaggio di posta elettronica dal modello di messaggio appropriato della directory.

Modelli di messaggio di posta elettronica in una directory

Ciascuna directory di modello distribuita contiene uno o più modelli di messaggio di posta elettronica. Quando si verifica un'attività o un evento per il quale la posta elettronica è abilitata, Identity Manager cerca nella directory di modelli appropriata un nome modello che sia uguale al nome dell'attività o dell'evento. Se non è possibile trovare un tale modello, Identity Manager utilizza il modello predefinito presente nella directory. I nomi di modello predefiniti sono elencati in [Modelli di messaggio di posta elettronica](#) (a pagina 382). Ad esempio, Identity Manager utilizza il modello defaultEvent.tmpl nella directory In sospeso per informare i responsabili dell'approvazione che è presente una nuova voce nell'elenco di lavoro.

Set di directory di modelli

Un set di directory di modelli contiene una directory per ogni categoria di modelli: Approvato, Completato, In sospeso e Rifiutato. È possibile distribuire più set di directory di modelli e specificare un set da utilizzare per un dato ambiente di Identity Manager.

La funzione di [distribuzione dei modelli di messaggio di posta elettronica](#) (a pagina 405) fornisce informazioni sulla distribuzione dei set di directory di modelli.

Per informazioni sulla configurazione delle directory di modelli di messaggi di posta elettronica per fare in modo che Identity Manager utilizzi il set corretto per un dato ambiente, consultare *Guida alla configurazione di CA Identity Manager*.

Creazione di modelli di messaggio di posta elettronica

Per creare messaggi di posta elettronica personalizzati

1. Aprire il modello che si desidera modificare.

Ad esempio, se si desidera creare un messaggio di posta elettronica per un evento di creazione utente in sospeso, aprire il modello `defaultEvent.tmpl` nella directory `In sospeso`.

2. Salvare il modello nella stessa directory con un nuovo nome. Il nome deve corrispondere al nome dell'evento a cui il messaggio di posta elettronica si applica e avere l'estensione `.tmpl`.

Ad esempio, denominare il messaggio per l'evento di creazione utente in sospeso nel modo seguente:

`CreateUserEvent.tmpl`

Consultare Eventi di Identity Manager per visualizzare un elenco di eventi.

Nota: quando si crea un file di modello di messaggio di posta elettronica con un nome file utilizzando una lingua diversa, la sessione del sistema operativo deve operare in una lingua che supporta il set di caratteri.

3. Modificare il modello di messaggio secondo le esigenze, come viene descritto nella sezione successiva, [Modelli di messaggio di posta elettronica personalizzati](#) (a pagina 385).

Modelli di messaggio di posta elettronica personalizzati

Un modello di messaggio di posta elettronica è un file dinamico che supporta sia HTML sia JavaScript lato server integrato. Un modello consente di inserire valori variabili nel testo statico, permettendo a messaggi specifici di essere generati da un unico modello.

È possibile utilizzare lo stesso modello per un numero indefinito di volte per stampare un testo statico standard (come ad esempio la frase "è stato approvato") insieme a un testo variabile specifico per un dato contesto (come ad esempio il nome dell'evento che viene approvato).

Ad esempio, di seguito viene riportato un modello usato per segnalare l'approvazione di un evento:

```
<!-- Define the E-mail Properties --->
<%
    _to = _util.getNotifiers("ADMIN");
    _cc = "" ;
    _bcc = "";
    _subject = _eventContextInformation.getEventName() + " approved";
%>
<!-- Start of Body --->
<html>
<body text="Navy">

Event: <b> <%= _eventContextInformation.getEventName() %> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:
<b><%= _eventContextInformation.getPrimaryObjectName() %></b><br>
In <%= _eventContextInformation.getSecondaryObjectTypeName() %>:
<b><%= _eventContextInformation.getSecondaryObjectName() %></b><br>
Status: <b>Approved</b>
</body>
</html>
```

Nota: gli oggetti di Identity Manager `_util` e `_eventContextInformation` utilizzati nell'esempio riportato sopra vengono descritti nella sezione API del modello del messaggio di posta elettronica.

Se viene generata un'approvazione per l'evento `CreateUserEvent`, e l'utente John Jones viene creato nel reparto Risorse Umane dell'organizzazione, il corpo della notifica del messaggio di posta elettronica generato dal modello di approvazione può assomigliare al seguente:

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

Le sezioni seguenti descrivono la sintassi e gli oggetti di Identity Manager che rendono i messaggi di posta elettronica dinamici possibili.

Elementi dei modelli

I modelli dei messaggi di posta elettronica di Identity Manager supportano:

- Tag HTML standard.
- JavaScript lato server.
- Uno o più oggetti impliciti che Identity Manager rende disponibili a un'istanza del modello, ovvero, a un messaggio di posta elettronica.
- I tag di Identity Manager che consentono di integrare JavaScript nel modello, chiamano i metodi negli oggetti di Identity Manager impliciti e inseriscono valori variabili nel testo statico del modello.

Estensioni di tag di Identity Manager

I modelli dei messaggi di posta elettronica supportano i tag seguenti:

`<% %>`

Integrazione di JavaScript in un modello di messaggio di posta elettronica.

`<%= %>`

Inserimento di un valore variabile nel testo statico.

I tag vengono descritti nelle sezioni seguenti.

`<% %>`

Questo tag consente di integrare JavaScript per l'esecuzione in-line in un modello di messaggio di posta elettronica.

È possibile utilizzare qualsiasi oggetto JavaScript all'interno del JavaScript integrato. È possibile chiamare anche i metodi degli oggetti impliciti di Identity Manager all'interno del JavaScript integrato.

Ad esempio, il codice seguente modifica il corpo del modello di approvazione riportato nella sezione [Modelli di messaggio di posta elettronica personalizzati](#) (a pagina 385). JavaScript viene utilizzato per determinare se un oggetto secondario è coinvolto nell'evento (ad esempio un oggetto ORGANIZZAZIONE quando viene aggiunto un oggetto primario UTENTE). Se non è presente nessun oggetto secondario, il testo che fa riferimento all'oggetto secondario viene omissso dal messaggio:

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                ObjectName()+" </b><br>");
}
%>
Status: <b>Approved</b>
```

<%= %>

Questo tag consente di inserire un valore variabile in un testo statico. Il valore può essere:

- Una variabile definita in un JavaScript precedentemente eseguito nel modello, ad esempio:

```
<%
var secondaryType =
    _eventContextInformation.getSecondaryObjectTypeName();
...           // More JavaScript processing
%>
...           // More HTML
L'oggetto primario era stato creato in <%=secondaryType%>.
```

- Un valore restituito da un metodo in un oggetto implicito di Identity Manager, ad esempio:

```
Event <%=_eventContextInformation.getEventName()%> is approved.
```

API del modello del messaggio di posta elettronica

Quando un messaggio viene generato da un modello, Identity Manager rende gli oggetti impliciti riportati sotto disponibili per il messaggio. Questi oggetti consentono di inserire informazioni specifiche di istanza in un messaggio chiamando i metodi nella API del modello di messaggio di posta elettronica.

Un modello può chiamare i metodi in uno qualsiasi degli oggetti seguenti:

- `_contentType`. Specifica il `contentType` per il messaggio di posta elettronica.
- `_priority`. Specifica la priorità per il messaggio di posta elettronica.
- `_to`. Aggiunge destinatari al campo A del messaggio.
- `_cc`. Aggiunge destinatari al campo Cc (invia copia conoscenza a) del messaggio.
- `_bcc`. Aggiunge destinatari al campo Ccn (invia copia conoscenza nascosta a) del messaggio.
- `_subject`. Specifica l'oggetto del messaggio di posta elettronica.
- `_encoding`. Specifica la codifica del messaggio di posta elettronica.
- `modello`. Consente di aggiungere una stringa di testo a un messaggio da righe di codice JavaScript.
- `_util`. Un oggetto di utilità.
- `_eventContextInformation`. Contiene informazioni sull'evento generato dall'attività corrente, come il nome dell'evento e lo stato di approvazione.
- `_taskContextInformation`. Contiene una raccolta di informazioni sull'attività attuale, come il nome dell'attività, il nome dell'organizzazione e gli eventi costitutivi.

Questi oggetti sono descritti nelle sezioni seguenti.

`_contentType`.

Specifica il `contentType` per il messaggio di posta elettronica.

Se nessun `contentType` viene specificato mediante la variabile `_contentType`, è valido il `contentType` "text/html" predefinito.

Metodi: nessuno.

Esempio:

```
<% _contentType = "text/html"; %>
```

`_priority.`

Specifica la priorità per il messaggio di posta elettronica. Specificare 0 per nessuna priorità (valore predefinito) e 1 per priorità alta.

Metodi: nessuno.

Esempio:

```
<% _priority = "1"; %>
```

`_to.`

Aggiunge destinatari al campo A del messaggio.

Il valore della variabile `_to` è una stringa JavaScript. Sono consentiti più destinatari ma la stringa deve essere conforme alla sintassi di JavaScript, come mostrato nell'esempio seguente.

Metodi: nessuno.

Esempio:

```
<%  
_to =  
_util.getNotifiers("USER") + ', ' +  
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");  
_cc = "" ;  
_bcc = "" ;  
_subject = "Your new password ";  
%>
```

Nota: quando i messaggi di posta elettronica avvertono i partecipanti che un'attività è in uno stato In sospeso e sotto il controllo del flusso di lavoro, l'oggetto `_to` viene precompilato con gli indirizzi dei partecipanti. Non è possibile utilizzare l'oggetto `_to` in un modello In sospeso.

`_cc.`

Aggiunge destinatari al campo Cc (invia copia conoscenza a) del messaggio.

Il valore della variabile `_to` è una stringa JavaScript. Sono consentiti più destinatari ma la stringa deve essere conforme alla sintassi di JavaScript, come mostrato nell'esempio seguente.

Metodi: nessuno.

Esempio:

```
<%  
_cc =  
_util.getNotifiers("USER") + ',' +  
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");  
%>
```

_bcc.

Aggiunge destinatari al campo Ccn (invia copia conoscenza nascosta a) del messaggio.

Gli indirizzi di posta elettronica specificati in questo campo non vengono visualizzati nel messaggio di posta elettronica.

Il valore della variabile `_to` è una stringa JavaScript. Sono consentiti più destinatari ma la stringa deve essere conforme alla sintassi di JavaScript, come mostrato nell'esempio seguente.

Metodi: nessuno.

Esempio:

```
<%  
_bcc =  
_util.getNotifiers("USER") + ',' +  
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");  
%>
```

_subject.

Specifica l'oggetto del messaggio di posta elettronica.

Metodi: nessuno.

Esempio:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding.

Specifica la codifica del messaggio di posta elettronica.

Se non è specificata nessuna codifica mediante la variabile `_encoding` o `LANG`, i caratteri nel messaggio di posta elettronica potrebbero non essere visualizzati correttamente. Assicurarsi di impostare `_encoding` o `LANG` per le impostazioni locali appropriate.

Metodi: nessuno.

Esempio:

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

Specifica attributi di intestazione di messaggio di posta elettronica aggiuntivi nel modello di messaggio di posta elettronica.

È necessario assegnare un `HashMap()` a questo attributo. I nomi e i valori archiviati in `HashMap` devono essere stringhe.

Esempio: aggiungere attributi di intestazione personalizzati

L'esempio seguente mostra come aggiungere due attributi di intestazione personalizzati, "X-TCCCSWD" e "myheader":

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```


template

Consente di aggiungere una stringa di testo a un messaggio dalle righe del codice JavaScript (ovvero, le righe all'interno dei tag <% %>). La stringa può contenere tag HTML, testo statico, e/o valori di variabile restituiti da metodi negli oggetti impliciti di Identity Manager.

Nota: l'oggetto di modello non è preceduto dal carattere di sottolineatura (_).

Metodo:

- add(String)

L'argomento deve valutare una stringa, inclusa qualsiasi chiamata ai metodi di un oggetto implicito di Identity Manager. Nell'esempio riportato sotto, consultare `_eventContextInformation.getSecondaryObjectName()`.

Esempio:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                   ObjectName()+ " </b><br>");
}
%>
```

_util.

Oggetto di utilità.

Metodo:

- getNotifiers(String [,String])

Restituisce ID di messaggi di posta elettronica in base a una regola di notifica.

Il primo argomento supporta le regole di notifica predefinite seguenti, racchiuse tra virgolette:

- "ADMIN". Invia il messaggio di posta elettronica all'amministratore che ha avviato l'attività.
- "USER". Invia il messaggio di posta elettronica all'utente nel contesto attuale.
- "USER_MANAGER". Invia il messaggio di posta elettronica al manager dell'utente nel contesto attuale.

È possibile anche fare riferimento a una regola di notifica personalizzata che si crea con l'API *Regola di notifica*. Per ulteriori informazioni, consultare la guida *Programming Guide for Java*.

Il secondo argomento è facoltativo. È possibile utilizzarlo per passare una o più coppie nome/valore definite dall'utente in una regola di notifica personalizzata. Separare ciascuna coppia nome/valore con una virgola, nel formato seguente:
"name1=value1,name2=value2..."

Esempi:

```
<%  
_to = _util.getNotifiers("ADMIN");_cc = "";  
%>  
<%  
_to = _util.getNotifiers("MYRULE","type=loan,district=3");  
_cc = "";  
%>
```

Notifica al manager di un utente

È possibile utilizzare la regola di notifica `USER_MANAGER` per inviare un messaggio di posta elettronica a qualsiasi manager di un utente. Identity Manager utilizza questa regola nei modelli di messaggio di posta elettronica che supportano la certificazione diritto utente.

Nota: la regola di notifica `USER_MANAGER` è valida solo per gli eventi o attività che creano o gestiscono un utente singolo.

Poiché una relazione da utente a manager può essere specificata in molti modi all'interno di una directory utente, l'Adattatore notifiche del manager utente predefinito risolve questa relazione in base a un'espressione di attributo specificata nel secondo parametro del metodo `getNotifiers()`.

Esempio:

```
<%  
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
_cc = "";  
%>
```

L'Adattatore notifiche del manager utente supporta due opzioni di ricerca:

- `managerattribute = <Manager AttributeName>`: dove l'oggetto Utente mantiene un attributo che indica il DN o l'ID utente del manager di quell'utente
- `commonattribute = <AttributeName>`: dove l'utente e il manager dell'utente condividono un valore di attributo comune, come ad esempio "dipartimento"

Queste opzioni di ricerca vengono configurate in Miscellaneous Properties (Proprietà varie) di un ambiente nella console di gestione di Identity Manager.

Per configurare la regola di notifica USER_MANAGER:

1. Nella console di gestione di Identity Manager, selezionare Identity Manager Environments (Ambienti di Identity Manager). Selezionare l'ambiente per il quale si sta configurando la notifica di posta elettronica.
2. Selezionare Impostazioni avanzate > Miscellaneous Properties (Proprietà varie).
3. Nella pagina Miscellaneous Properties (Proprietà varie), completare i passaggi di configurazione per l'opzione di ricerca che si desidera utilizzare:
 - Per utilizzare l'opzione di ricerca `managerattribute=<Manager AttributeName>`:
 - a. Nel campo Proprietà, immettere `managerattribute`.
 - b. Nel campo Valore, immettere l'attributo che archivia il DN o l'utente ID del manager.
 - c. Fare clic su Aggiungi.
 - d. Fare clic su Salva.
 - Per utilizzare l'opzione di ricerca `commonattribute=<AttributeName>`:
 - a. Nel campo Proprietà, immettere `commonattribute`.
 - b. Nel campo Valore, immettere l'attributo che l'utente e il manager dell'utente hanno in comune.
 - c. Fare clic su Aggiungi.
 - d. Nel campo Proprietà, immettere `ismanagerfilter`.
 - e. Nel campo Valore, immettere un'espressione di ricerca mediante la sintassi seguente:
`<attribute> <operator> <filter>`
Ad esempio, titolo EQUALS manager
 - f. Fare clic su Aggiungi.
 - g. Fare clic su Salva.

È possibile scrivere anche un adattatore personalizzato e creare le proprie regole di notifica al Manager di un utente. Per ulteriori informazioni, consultare la guida *Programming Guide for Java*.

_eventContextInformation.

Contiene informazioni sull'evento generato dall'attività corrente, come il nome dell'evento e lo stato di approvazione. Queste informazioni vengono chiamate informazioni di *contesto* dell'evento.

L'oggetto `_eventContextInformation` viene creato dalla classe di `ExposedEventContextInformation` nel pacchetto `com.netegrity.imapi`.

Questo oggetto è disponibile per messaggi di posta elettronica basati sui modelli Approvato, In sospeso e Rifiutato. Per informazioni su questi modelli, consultare la sezione [Modelli di messaggio di posta elettronica](#) (a pagina 382).

Metodi: tutti i metodi seguenti restituiscono una stringa.

di autenticazione	Descrizione
<code>getAdminName()</code>	Restituisce il nome della persona che ha inoltrato l'attività che ha generato l'evento. Obsoleto in CA Identity Manager 5.6. Utilizzare uno dei seguenti metodi ereditati: ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>
<code>getApprovalStatus()</code>	Ripristina lo stato di approvazione dell'evento. Uno di questi valori: <code>APPROVAL_STATUS_APPROVED</code> <code>APPROVAL_STATUS_REJECTED</code>
<code>getApprovalTime()</code>	Ripristina la data/ora di approvazione dell'evento.
<code>getEventName()</code>	Restituisce il nome dell'evento. Per un elenco dei nomi di evento, consultare la sezione Eventi di CA Identity Manager.
<code>getOrgName()</code>	Restituisce il nome descrittivo dell'organizzazione in cui l'attività viene eseguita. Obsoleto in CA Identity Manager 5.6. Utilizzare il metodo ereditato <code>getObjectOrganizationFriendlyName()</code> .
<code>getPassword()</code>	Se l'oggetto primario è di tipo USER, restituisce la password dell'utente.

di autenticazione	Descrizione
getPrimaryObjectTypeName()	Restituisce il tipo di oggetto primario. Tipi di oggetto primario restituiti: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getPrimaryObjectName()	Restituisce il nome dell'oggetto primario interessato dall'evento. Un <i>oggetto primario</i> è l'oggetto direttamente interessato dall'evento. Un <i>oggetto secondario</i> è l'oggetto a cui l'oggetto primario è associato, se presente. Ad esempio: ■ Il tipo di oggetto primario per <code>CreateUserEvent</code> è <code>USER</code>. L'oggetto secondario è l'oggetto in cui l'utente viene creato, ovvero <code>ORGANIZATION</code>. ■ Il tipo di oggetto primario per <code>CreateAdminRoleEvent</code> è <code>ADMINROLE</code>. Questo oggetto non è associato ad altri oggetti, pertanto non esiste nessun oggetto secondario. Con un oggetto primario di tipo <code>USER</code>, è possibile che <code>getPrimaryObjectName()</code> restituisca John Jones.
getSecondaryObjectTypeName()	Se un oggetto secondario è stato interessato dall'evento, restituisce il tipo di oggetto. Tipi di oggetto secondari restituiti: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

di autenticazione	Descrizione
getSecondaryObjectName()	Se un oggetto secondario è stato interessato dall'evento, restituisce il nome dell'oggetto. Consultare getPrimaryObjectName() per informazioni sugli oggetti primari e secondari. Con un oggetto secondario di tipo ORGANIZATION, è possibile che il metodo getSecondaryObjectName() restituisca HR.

Nota: i metodi in `_eventContextInformation` vengono forniti tramite l'interfaccia `ExposedEventContextInformation`. Poiché `ExposedEventContextInformation` eredita i metodi nell'API di base di CA Identity Manager, `_eventContextInformation` può chiamare questi metodi anche da un modello di messaggio di posta elettronica, insieme ai metodi contenuti nella tabella riportata sopra. Per ulteriori informazioni su questi metodi ereditati, consultare la sezione [Metodi aggiuntivi](#) (a pagina 402).

Esempio--Notifica di posta elettronica per un evento In sospeso:

```
<%  
_cc = "" ;  
_bcc = "";  
_subject = _eventContextInformation.getEventName() +  
                                     " Approval Request";  
%>  
<!-- Start of Body --->  
<html>  
<body text="Navy">
```

L'elemento seguente è stato aggiunto all'elenco di lavoro per l'approvazione:

```
<br><br><br>  
Event: <b><%= _eventContextInformation.getEventName() %></b> <br>  
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:  
<b><%= _eventContextInformation.getPrimaryObjectName() %></b><br>  
In <%= _eventContextInformation.getSecondaryObjectTypeName() %>:  
<b><%= _eventContextInformation.getSecondaryObjectName() %></b><br>  
</body>  
</html>
```

Corpo del messaggio di posta elettronica possibile:

Da: lsmith@security.com [mailto:lsmith@security.com]

A: vimperioso@security.com

Oggetto: Richiesta di approvazione CreateUserEvent

L'elemento seguente è stato aggiunto all'elenco di lavoro per l'approvazione:

Event: **CreateUserEvent**

USER: **Richard Ferrigamo**

In ORGANIZATION: **Mutui e prestiti**

Nota: il valore del campo Da deriva dal file email.properties. Per modificare il valore, modificare il file seguente:

<iam_im.ear>\config\com\netegrity\config\email.properties

dove <iam_im.ear> è la posizione di installazione di CA Identity Manager nel dominio del server applicazioni, ad esempio:

Per WebLogic:

<WebLogic_home>\user_projects\<domain>\applications\iam_im.ear

Per JBoss:

<Identity Manager_home>\jboss-3.2.2\server\default\deploy\iam_im.ear

Per WebSphere:

<im_admin_tools_dir >\WebSphere-ear\iam_im.ear

Per aggiungere informazioni aggiuntive sull'utente interessato dall'evento al messaggio di posta elettronica dell'esempio precedente, aggiungere del testo simile al seguente:

```
<% user = _eventContextInformation.getEvent().getUser(); %>
```

```
<b>User information:</b><br>
```

```
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
```

```
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
```

```
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
```

```
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
```

```
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Corpo del messaggio di posta elettronica possibile:

Da: lsmith@security.com [mailto:lsmith@security.com]

A: vimperioso@security.com

Oggetto: Richiesta di approvazione CreateUserEvent

L'elemento seguente è stato aggiunto all'elenco di lavoro per l'approvazione:

Event: **CreateUserEvent**

USER: **Richard Ferrigamo**

In ORGANIZATION: **Mutui e prestiti**

Informazioni utente:

Cognome: Ferrigamo

Nome: Richard

Nome completo: Richard Ferrigamo

Indirizzo di posta elettronica: rferrigamo@mybank.org

Appartenenza organizzazione: **Mutui e prestiti**

_taskContextInformation.

Contiene una raccolta di informazioni sull'attività attuale, come il nome dell'attività, il nome dell'organizzazione e gli eventi costitutivi. Queste informazioni vengono chiamate informazioni di *contesto* dell'attività.

Questo oggetto è disponibile per i messaggi di posta elettronica basati su modelli Completati. Per informazioni su questo modello, consultare la sezione [Modelli di messaggio di posta elettronica](#) (a pagina 382).

Metodi: tutti i metodi riportati di seguito restituiscono una stringa tranne il metodo `getExposedEventContexts()`, che ripristina un vettore Java.

di autenticazione	Descrizione
<code>getAdminName()</code>	Restituisce il nome della persona che inoltra l'attività. Obsoleto in Identity Manager 5.6. Utilizzare uno dei seguenti metodi ereditati: ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>

di autenticazione	Descrizione
<code>getExposedEventContexts()</code>	Restituisce un oggetto vettore Java di tutti gli eventi associati con l'attività. Ciascun oggetto nel vettore è un oggetto di contesto di evento. È possibile utilizzare i metodi classificati in <code>_eventContextInformation</code> per recuperare le informazioni di contesto per un dato oggetto di evento. L'oggetto restituito è un oggetto vettore Java standard. È possibile utilizzare uno qualsiasi dei metodi dell'oggetto vettore, ad esempio <code>get()</code> e <code>size()</code>, per gestire gli elementi nel vettore.
<code>getOrgName()</code>	Restituisce il nome dell'organizzazione in cui viene eseguita l'attività. Obsoleto in Identity Manager 5.6. Utilizzare il metodo ereditato <code>getObjectOrganizationFriendlyName()</code>.
<code>getTaskName()</code>	Restituisce il nome dell'attività che viene eseguita. Obsoleto in Identity Manager 5.6. Utilizzare uno dei seguenti metodi ereditati: ■ <code>getAdminTask()</code> ■ <code>getTaskFriendlyName()</code>

Nota: i metodi in `_eventContextInformation` vengono forniti tramite l'interfaccia `ExposedTaskContextInformation`. Poiché `ExposedEventContextInformation` eredita i metodi nell'API di base di Identity Manager, `_eventContextInformation` può chiamare questi metodi anche da un modello di messaggio di posta elettronica, insieme ai metodi contenuti nella tabella riportata sopra. Per ulteriori informazioni su questi metodi ereditati, consultare la sezione [Metodi aggiuntivi](#) (a pagina 402).

Esempio--Corpo di un modello di notifica di posta elettronica per una modifica di password:

```
<%  
var imsEventContexts =  
    _taskContextInformation.getExposedEventContexts();  
if(imsEventContexts != null)  
{  
    for(var i=0;i<imsEventContexts.size();i++)  
    {  
        var eventContext = imsEventContexts.get(i);  
        template.add("Hi "+ eventContext.getPrimaryObjectName()  
                    + ",");  
        template.add("<br>Your new password is: <b>"+  
                    eventContext.getPassword());<br>  
        template.add("<hr>");  
    }  
}  
%>
```

Corpo del messaggio di posta elettronica possibile:

Gentile Victor Imperioso,
La nuova password è LFH7F1226

Metodi aggiuntivi

I metodi in `_taskContextInformation` e `_eventContextInformation` vengono forniti rispettivamente tramite gli oggetti di Identity Manager `ExposedTaskContextInformation` e `ExposedEventContextInformation`.

Questi oggetti ereditano metodi nell'API di Identity Manager di base. Di conseguenza, i metodi ereditati sono disponibili anche per `_taskContextInformation` e `_eventContextInformation`.

I metodi seguenti ereditati dall'oggetto `TaskInfo` sono particolarmente utili per un modello di messaggio di posta elettronica:

- `getAdministrator()`. Recupera un oggetto `Utente` per l'amministratore che sta eseguendo l'attività corrente.
- `getAdminTask()`. Recupera un oggetto `AdminTask` per l'attività corrente.

Questi oggetti recuperati consentono di inserire informazioni specifiche di amministratore e specifiche di attività in un messaggio di posta elettronica. Ad esempio:

```
<!-- Define the E-mail Properties --->
```

```
<%
    _cc = "" ;
    _bcc = "" ;
    _subject = _eventContextInformation.getEventName() +
        " richiesta di approvazione";
%>
```

```
<!-- Start of Body --->
```

```
<html>
```

```
<body text="Navy">
```

```
The following item has been added to your work list for approval:<br>
```

```
<br>
```

```
User <b><%= _eventContextInformation.getAdministrator().
    getAttribute(Packages.com.netegrity.llsdk6.imsapi.
        managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
    from department <b><%= _eventContextInformation.
        getAdministrator().getOrg(null).getFriendlyName()
        %></b> initiated task <b><%= _eventContextInformation.
        getAdminTask().getFriendlyName() %></b>at <b><%=
        _eventContextInformation.getSessionCreateTime() %></b>
```

```
<br><br>
```

```
<font color="green">Details: </font><b><%=_eventContextInformation.
    getEventName()%></b><br>
```

```
<font color="green"><%=_eventContextInformation.
    getPrimaryObjectTypeName()%>:</font>
```

```
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>>
    was modified
```

```
<br>
```

```
<font color="green">Updated Attributes:</font>
```

```
<table border="1">
```

```
<tr>
```

```
<td><b>Name</b></td>
```

```
<td><b>Value</b></td>
```

```
</tr>
```

```
<%
    var event = _eventContextInformation.getEvent();
    if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
        var user = event.getUser();
        var attributes = user.getAttributes().keys();
        while(attributes.hasMoreElements()) {
            var attr = attributes.nextElement();
            var value = user.getAttribute(attr);
            if(user.hasAttributeChanged(attr)) {
                template.add("<tr><td>" + attr + "</td>");
                template.add("<td>" + value + "</td></tr>");
            }
        }
    }
}%>
</table>
<br>
</body>
</html>
```

Corpo del messaggio di posta elettronica possibile:

The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**

User: **John Jones** was modified

Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

Per ulteriori informazioni sui metodi ereditati disponibili per l'API di modello di messaggio di posta elettronica, consultare gli oggetti `ExposedTaskContextInformation` e `ExposedEventContextInformation` nel Javadoc di Identity Manager.

Stream di output standard di Java

Un messaggio di posta elettronica può fare anche chiamate allo stream di output standard di Java dall'interno del tag JavaScript (`<% %>`). Per esempio, la chiamata seguente invia il messaggio Completato alla console del server:

```
<%
...      // JavaScript processing
out.println("Done.");
}%>
```

Riferimenti Javadoc

Per informazioni sugli oggetti `ExposedTaskContextInformation` e `ExposedEventContextInformation`, inclusi i metodi che ereditano dall'API di Identity Manager di base, consultare il Javadoc di Identity Manager.

Le pagine Javadoc sono integrate con una versione HTML della Guida alla programmazione per Java, disponibile nel Bookshelf di Identity Manager.

Distribuzione del modello di messaggio di posta elettronica

Quando CA Identity Manager sta per inviare a messaggio di posta elettronica, cerca modelli da cui generare il messaggio di posta elettronica nella posizione principale seguente all'interno del server applicazioni:

`iam_im.ear\custom\emailTemplates`

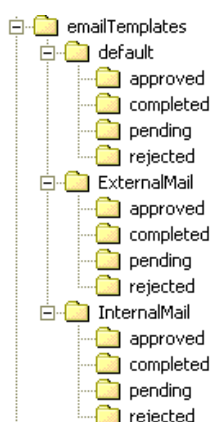
I modelli di messaggio di posta elettronica distribuiti nella posizione root sono contenuti in set di modelli che hanno la stessa struttura di directory, ovvero in ciascun set è presente una directory per ogni categoria: Approvato, Completato, In sospeso, Rifiutato.

Set di modelli

È possibile distribuire molti set di modelli di messaggio di posta elettronica in `emailTemplates`. Ad esempio, durante l'installazione, il set di modelli di messaggio di posta elettronica seguente viene creato in `iam_im.ear\custom\emailTemplates`:

`default\approved`
`default\completed`
`default\pending`
`default\rejected`

Il set di modelli di messaggio di posta elettronica predefinito contiene i modelli installati descritti nella sezione [Modelli di messaggio di posta elettronica](#) (a pagina 382). È possibile aggiungere modelli personalizzati all'interno del set predefinito. È possibile distribuire anche altri set di modelli di messaggio di posta elettronica in strutture di directory definite allo stesso livello del set predefinito. Ad esempio, iam_im.ear\custom potrebbe contenere i modelli di messaggio di posta elettronica distribuiti seguenti:



Nota: per informazioni su come CA Identity Manager sceglie un modello di messaggio di posta elettronica particolare all'interno di un set di modelli, consultare [Directory dei modelli](#) (a pagina 384).

Definizione di un set di modelli per un Ambiente

Quando si configura un messaggio di posta elettronica per un ambiente di Identity Manager, viene specificato il set di modelli di messaggio di posta elettronica che si desidera utilizzare per quell'ambiente. Per informazioni sulla configurazione dei messaggi di posta elettronica per un ambiente di Identity Manager, consultare la *Guida alla configurazione di CA Identity Manager*.

Nomi dei modelli

Le directory di un set di modelli personalizzato devono contenere modelli predefiniti con lo stesso nome di quelli installati nel set di modelli predefinito. I nomi predefiniti sono elencati in [Modelli di messaggio di posta elettronica](#) (a pagina 382). Identity Manager utilizza i modelli predefiniti quando non è in grado di trovare nessun altro modello con un nome che corrisponde all'attività o all'evento in esecuzione.

Facoltativamente, è possibile aggiungere ulteriori modelli a una o più directory di un set di modelli se si desidera che un messaggio di posta elettronica venga generato da un modello particolare. A questo scopo:

- Assegnare al modello lo stesso nome dell'attività o evento per il quale il messaggio di posta elettronica verrà generato.
- Posizionare il modello nella directory associata con lo stato di attività o evento per cui il messaggio di posta elettronica verrà generato.

Ad esempio, se si desidera che i messaggi di posta elettronica vengano generati da un modello particolare quando un `CreateUserEvent` viene rifiutato, collocare un modello denominato `CreateUserEvent.tmpl` nella directory di rifiuto del set di modelli dell'ambiente.

Capitolo 13: Rapporti

Questa sezione contiene i seguenti argomenti:

- [Panoramica di configurazione](#) (a pagina 409)
- [Processo dei rapporti](#) (a pagina 411)
- [Esecuzione di rapporti di snapshot](#) (a pagina 412)
- [Esecuzione di rapporti non di snapshot](#) (a pagina 429)
- [Imposta opzioni di segnalazione](#) (a pagina 435)
- [Creazione ed esecuzione di un rapporto di snapshot personalizzato](#) (a pagina 436)
- [Sincronizzazione di utenti, account e ruoli](#) (a pagina 450)
- [Risoluzione dei problemi](#) (a pagina 457)

Panoramica di configurazione

CA Identity Manager consente di eseguire due diversi tipi di rapporti:

Rapporti di snapshot

Include i dati provenienti dal database snapshot, contenente informazioni relative all'archivio oggetti di CA Identity Manager e all'archivio utenti di CA Identity Manager. Il rapporto Profilo utente è un esempio di rapporto snapshot. Si definiscono i dati da aggiungere al database snapshot utilizzando definizioni snapshot che specificano le informazioni da includere.

Rapporti non snapshot

Includono dati provenienti da altre origini, quali il database di controllo. In CA Identity Manager sono ad esempio inclusi rapporti di controllo predefiniti. (Visualizzati con prefisso "Audit - " nel nome nella console utente). Per impostazione predefinita, in CA Identity Manager sono inclusi solo rapporti di controllo. È tuttavia possibile creare rapporti personalizzati che includono dati provenienti da qualsiasi origine, quali il database dei flussi di lavoro o di persistenza delle attività.

Per poter eseguire i rapporti inclusi in CA Identity Manager è necessaria una configurazione iniziale. La procedura di configurazione dipende dal tipo di rapporto da eseguire.

Le fasi seguenti riassumono le procedure contenute in questo capitolo.

Per Rapporti di snapshot

1. Creare un file di definizione snapshot per i dati da aggiungere al database snapshot.
2. Acquisire i dati snapshot per il rapporto.

3. Modificare l'attività di rapporto nella console utente, quindi eseguire le seguenti azioni:
 - a. Associare una definizione snapshot all'attività.
 - b. Aggiungere all'attività l'oggetto connessione rptParamConn.
4. Richiedere il rapporto utilizzando uno dei seguenti metodi:
 - Eseguire il rapporto immediatamente.
 - Pianificare il rapporto.
5. Visualizzare il rapporto nella console utente.

Per Rapporti non snapshot:

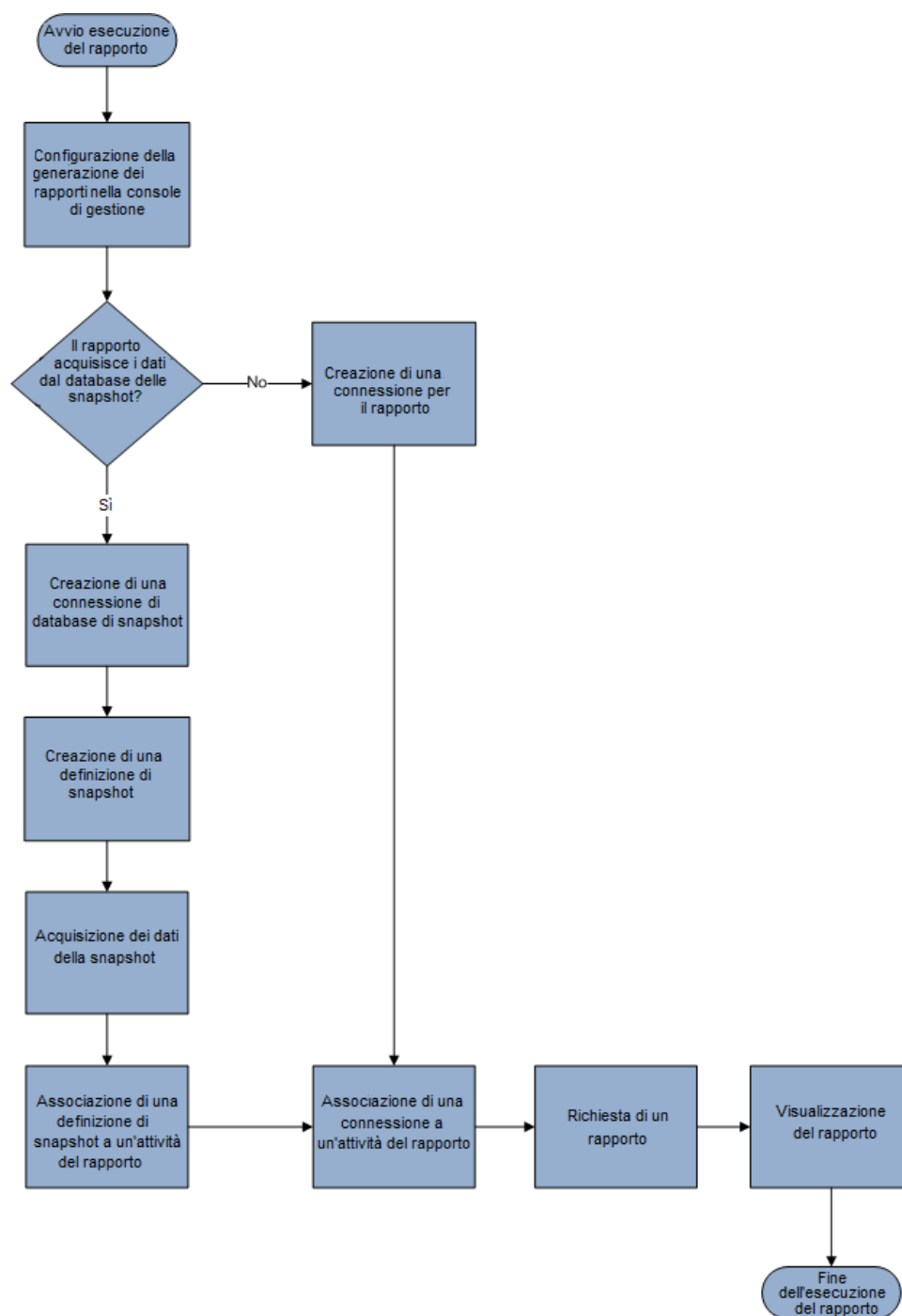
1. Creare un oggetto connessione con le informazioni relative all'origine dati per il rapporto.
2. Modificare l'attività di rapporto in CA Identity Manager, quindi aggiungere l'oggetto di connessione all'attività.
3. Richiedere il rapporto utilizzando uno dei seguenti metodi:
 - Eseguire il rapporto immediatamente.
 - Pianificare il rapporto.
4. Visualizzare il rapporto nella console utente.

Una volta completata la configurazione iniziale del rapporto, è possibile richiederlo in CA Identity Manager. Si può eseguire un rapporto immediatamente o pianificarne l'esecuzione in un momento successivo. CA Identity Manager consente inoltre di creare una pianificazione ricorrente per il rapporto.

Infine è possibile visualizzare il rapporto nella console utente o esportarlo in vari formati.

Processo dei rapporti

L'immagine seguente descrive il processo necessario per l'esecuzione e la visualizzazione dei rapporti:



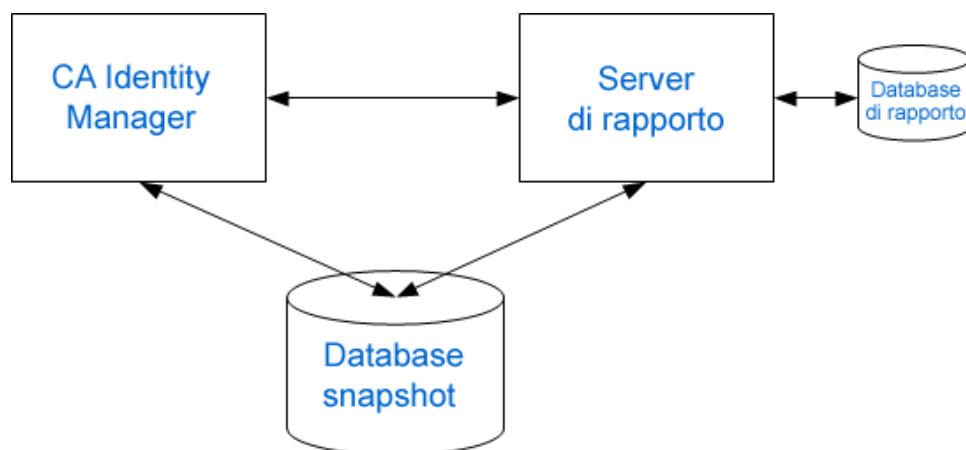
Esecuzione di rapporti di snapshot

I rapporti di CA Identity Manager consentono di rilevare lo stato attuale di un ambiente CA Identity Manager. È possibile utilizzare tali informazioni per garantire conformità con criteri aziendali interni o con normative esterne.

I rapporti di CA Identity Manager vengono creati dai dati di gestione che descrivono la relazione tra gli oggetti in un ambiente di CA Identity Manager. Di seguito sono elencati alcuni esempi di dati di gestione:

- Attributi di profilo degli utenti
- Elenco dei ruoli che contengono una determinata attività
- I membri di un ruolo o gruppo
- Le regole che comprendono un ruolo

In CA Identity Manager, la configurazione per la generazione di rapporti richiede i tre seguenti componenti principali:



Nota: Il database snapshot in questa figura potrebbe essere anche il database di controllo o il database del flusso di lavoro.

Server di rapporto

Noto anche come CA Business Intelligence, questo server genera rapporti e comunica direttamente con CA Identity Manager e il database snapshot.

Database di rapporto

Database su cui il server di rapporto di CA (BusinessObjects) archivia i propri dati.

CA Identity Manager

CA Identity Manager consente di esportare i dati di oggetto di CA Identity Manager al database di rapporto.

Database snapshot

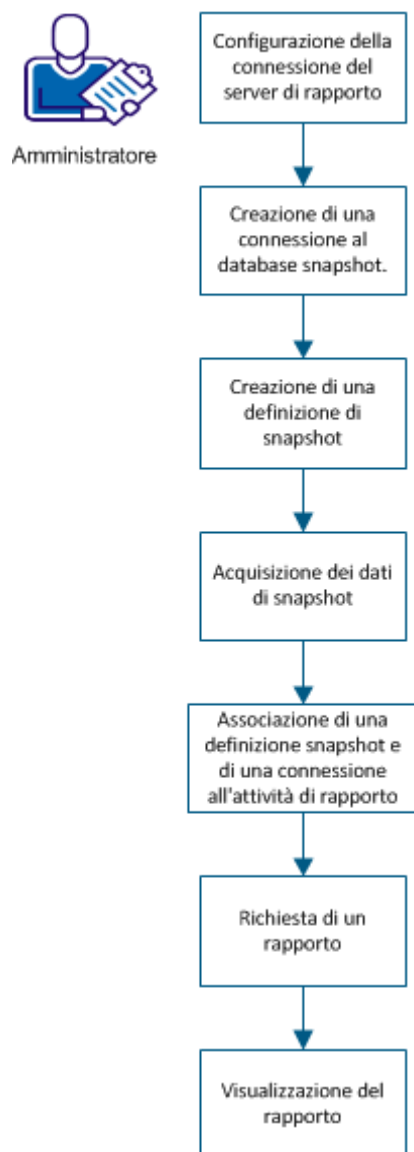
Database distinto che contiene i dati di snapshot degli oggetti in CA Identity Manager

Importante. Il server di rapporto utilizza BusinessObjects Enterprise. Se nell'ambiente è già presente un server di rapporto e si desidera utilizzarlo con CA Identity Manager, la versione minima richiesta da CA Identity Manager è CA Business Intelligence 3.2 SP5.

Un rapporto di snapshot include i dati tratti dal database snapshot, contenente informazioni dell'archivio oggetti CA Identity Manager e dell'archivio utenti. Il rapporto Profilo utente è un esempio di rapporto di snapshot. Definire i dati di snapshot da aggiungere al database snapshot e, con le definizioni snapshot, specificare le informazioni da includere.

Il grafico seguente illustra la procedura per l'esecuzione di un rapporto di snapshot:

Esecuzione di un rapporto di snapshot



Per eseguire il rapporto di snapshot, completare i passaggi seguenti:

1. [Configurazione della connessione al server di rapporto](#) (a pagina 430).
2. Creazione di una connessione al database snapshot.
3. Creazione di una definizione snapshot.
4. Acquisizione dei dati di snapshot.
5. Associazione di una definizione snapshot e di una connessione all'attività di rapporto.

6. Richiesta di un rapporto.
7. [Visualizzazione del rapporto](#) (a pagina 434).

Configurazione della connessione del server di rapporto

Configurare la connessione tra CA Identity Manager e il server di rapporto.

Nota: si consiglia di impostare tutti i sistemi interessati dalla generazione di rapporti su ora e data identiche.

Configurazione dei rapporti

1. Nella console utente, fare clic su Attività, Sistema, Generazione rapporti, Connessione al server di rapporto.
2. Inserire le impostazioni del server di rapporto. Si noti quanto segue:
 - Nome host e Porta: il nome host e il numero di porta dell'URL HTTP del sistema in cui viene installato il server di rapporto.
 - Nome della cartella rapporti: posizione dei rapporti predefiniti di CA Identity Manager.
 - ID utente: utente creato per il server di rapporto.
 - Password: password per l'utente creato nel server di rapporto.
 - Connessione protetta: selezionare la casella di controllo per abilitare la connessione SSL (Secure Socket Layer) tra CA Identity Manager e il server di rapporto.

Nota: prima di selezionare la casella di controllo Connessione protetta, verificare che sia installato il certificato dal BO Server. Per ulteriori informazioni sulla configurazione di SSL, consultare il capitolo relativo all'installazione del server di rapporto della *Guida all'installazione*.
 - Server web: impostato su non IIS per Tomcat
3. Fare clic su Verifica connessione per verificare la connessione.
4. Fare clic su Inoltra.

Viene stabilita la connessione al rapporto.

Creazione di una connessione al database snapshot

È necessario indicare a CA Identity Manager il percorso di esportazione dei dati snapshot. Creare una connessione fra CA Identity Manager e il database snapshot.

Creazione di una connessione al database snapshot

1. Nella console utente, fare clic su Attività, Rapporti, Attività snapshot, Gestisci connessione database snapshot, Crea connessione database snapshot.
2. Creare una nuova connessione al database snapshot compilando i campi necessari.
3. Fare clic su Inoltra.

Viene creata una nuova connessione al database snapshot.

Creazione di una definizione di snapshot

Una snapshot riflette lo stato degli oggetti in CA Identity Manager in un determinato momento. Si utilizzano i dati di questa snapshot per la generazione di un rapporto. Per acquisire dati oggetto di CA Identity Manager, creare una definizione di snapshot che esporti i dati nel database snapshot. Con la definizione di snapshot si definiscono le regole per caricare utenti, endpoint, ruoli di amministrazione, ruoli di provisioning, gruppi e organizzazioni.

Procedere come descritto di seguito:

1. Nella console utente, accedere a Attività, Rapporti, Attività snapshot, Gestisci definizione snapshot, Crea definizione snapshot.
2. Selezionare Crea o Copia un oggetto di tipo Tipologia di snapshot.
3. Fare clic su OK.
4. Nella scheda Profilo compilare i campi seguenti per creare un profilo di definizione di snapshot:

Nome definizione snapshot

Identifica il nome univoco assegnato alla definizione della snapshot.

Descrizione della definizione di snapshot

Visualizza le eventuali informazioni aggiuntive che si desidera includere nella descrizione della snapshot.

Abilitato

Specificare la creazione di una snapshot in base alla definizione di snapshot corrente, all'ora pianificata.

Nota: se questa opzione non è selezionata, la definizione di snapshot non viene acquisita all'ora pianificata. Inoltre, la definizione di snapshot non verrà elencata nella schermata Acquisisci dati snapshot.

Numero di snapshot mantenute

Consente di specificare il numero di snapshot memorizzate correttamente nel database delle snapshot.

Nota: se non viene specificato un valore per questo campo, verrà memorizzato un numero illimitato di snapshot.

5. Nella scheda Criteri snapshot, selezionare gli oggetti correlati ai criteri da esportare.
6. Nella scheda Impostazioni ruolo, selezionare uno o più componenti di ruolo e attributi disponibili per la snapshot da esportare.

Nota: se si seleziona l'oggetto Ruolo di accesso, Ruolo di amministrazione o Ruolo di provisioning nella scheda Criteri snapshot, selezionare gli attributi nella scheda Impostazioni ruolo.

7. Nella scheda Dettagli attributo dell'utente, selezionare uno o più attributi utente per la snapshot da esportare.

Nota: se si seleziona unicamente l'oggetto Utente nella scheda Criteri snapshot, per impostazione predefinita tutti i dati relativi agli attributi utente vengono esportati.

8. Nella scheda Attributi dell'account di endpoint, selezionare uno o più attributi account per ciascun tipo di endpoint.

Nota: per il tipo di endpoint selezionato, tutti i dati relativi agli attributi account di endpoint vengono esportati per impostazione predefinita. Per acquisire i dati correlati a un attributo specifico, selezionare l'attributo appropriato. Per ulteriori informazioni sulla selezione degli attributi necessari per l'esportazione di un tipo di endpoint, consultare la sezione relativa ai rapporti predefiniti della *Guida alla configurazione*.

9. (Facoltativo) Selezionare la casella di controllo Esporta account orfani per includere account endpoint senza alcun utente globale nel server di provisioning.

Nota: per esportare i dati di rapporto per i rapporti non standard, i rapporti di andamento account non standard e il rapporto account orfani, selezionare l'attributo exceptionAccount e la casella di controllo Esporta account orfani.

10. Fare clic su Inoltra.

CA Identity Manager è configurato per creare le snapshot degli oggetti compresi nella definizione di snapshot.

Dopo aver creato una definizione di snapshot, è possibile acquisire immediatamente dati di snapshot oppure pianificare l'esportazione dei dati di snapshot in un secondo momento. Per ulteriori informazioni, consultare la sezione Acquisizione di dati di snapshot.

Ulteriori informazioni:

[Scheda Ricorrenza](#) (a pagina 421)

Esempio: creare una definizione snapshot per i dati dei diritti dell'utente

L'esempio seguente illustra il processo per creare una definizione snapshot per un rapporto dei diritti dell'utente:

1. Nella console utente, accedere a Attività, Rapporti, Attività snapshot, Gestisci definizione snapshot, Crea definizione snapshot.
2. Selezionare Crea un nuovo oggetto di tipo Tipologia di snapshot.
3. Immettere il nome della definizione snapshot, la descrizione e il numero di snapshot mantenute.
4. Nella scheda Definizione del criterio della snapshot, fare clic su Aggiungi.

Dall'elenco a discesa, selezionare l'utente e selezionare Tutto. Analogamente, aggiungere Endpoint, Ruolo di provisioning, Ruolo di amministrazione, Ruolo di accesso, Organizzazione e Gruppo così come mostrato nella schermata seguente:

Objects to be Exported	
Access Role	
(all)	
Admin Role	
(all)	
Endpoint	
(all)	
Group	
(all)	
Organization	
(all)	
Provisioning Role	
(all)	
User	
(all)	

5. Nella scheda Role Setting (Impostazione ruolo), selezionare tutte le caselle di controllo di ruolo dell'utente.
6. Nella scheda Attributi utente, selezionare gli attributi richiesti dall'elenco Valori disponibili e spostarli nell'elenco Valori correnti.
7. Fare clic su Inoltra.

Gestione delle istantanee

CA Identity Manager consente di visualizzare, modificare ed eliminare le definizioni degli snapshot. Quando si visualizza o modifica una definizione di snapshot, vengono visualizzate le schede Profilo e Manutenzione. La scheda Manutenzione viene visualizzata solo dopo l'acquisizione di un'istananea. Nella scheda Manutenzione è possibile eliminare gli snapshot, anche se il loro stato è non riuscito.

Per visualizzare, modificare o eliminare una definizione di snapshot, passare a Rapporti, Attività snapshot, Gestisci definizione snapshot e fare clic sull'attività che si desidera eseguire.

Nota: se una definizione snapshot viene utilizzata per esportare dati nel database degli snapshot, non è possibile eliminarla. Quando viene eliminata una definizione snapshot in uso, l'esportazione dei dati nel database snapshot viene interrotta, ma la definizione snapshot sarà ancora disponibile.

Acquisizione dei dati di snapshot

Eseguire l'attività Acquisisci dati snapshot se si desidera acquisire i dati snapshot immediatamente, oppure pianificarne l'esportazione in un momento successivo o in base ad una pianificazione ricorrente. Questa attività esporta immediatamente i dati (definiti dalla definizione snapshot) nel database snapshot.

Importante. L'esportazione dei dati snapshot può richiedere molto tempo in caso di grandi volumi. Si consiglia di pianificare le snapshot nel caso di esportazione di grandi volumi di dati.

Per acquisire dati istantanea

1. Nella console utente, accedere a Attività, Rapporti, Attività snapshot, Acquisisci dati snapshot.
2. Selezionare Esegui ora per eseguire l'operazione di esplorazione dei dati immediatamente, oppure [Pianifica nuovo processo](#) (a pagina 421) per rimandare l'operazione a un momento successivo oppure in base a una pianificazione ricorrente.
3. Fare clic su Avanti.
4. Scegliere una definizione di snapshot.
5. Fare clic su Inoltra.

I dati snapshot vengono esportati nel database degli snapshot.

Nota: se l'attività Acquisisci dati snapshot sembra richiedere troppo tempo, controllare l'avanzamento dell'attività passando alla scheda Sistema e facendo clic su Visualizza attività inviate.

Scheda Ricorrenza

Utilizzare questa scheda per pianificare il processo. Di seguito sono elencati i campi presenti nella scheda:

Esegui ora

Il processo viene eseguito immediatamente.

Pianifica nuovo processo

Consente di pianificare un nuovo processo.

Modifica processo esistente

Consente di specificare che si desidera modificare un processo esistente.

Nota: questo campo viene visualizzato solo se per questa attività è già stato pianificato un processo.

Nome processo

Consente di specificare il nome del processo da creare o modificare.

Fuso orario

Consente di specificare il server del fuso orario.

Nota: se il fuso orario utilizzato è diverso da quello del server del fuso orario, viene visualizzata una casella a discesa nella quale è possibile selezionare il proprio fuso orario o quello del server per la pianificazione di un nuovo processo. Non è possibile modificare il fuso orario quando si modifica un processo esistente.

Pianificazione giornaliera

Consente di specificare che il processo venga eseguito a intervalli regolari.

Ogni (numero di giorni)

Consente di definire il numero di giorni che intercorrono tra le esecuzioni del processo.

Pianificazione settimanale

Consente di specificare che il processo venga eseguito a una determinata ora di un dato giorno o giorni della settimana.

Giorno della settimana

Consente di specificare il giorno o i giorni della settimana in cui viene eseguito il processo.

Pianificazione mensile

Consente di specificare un giorno della settimana o del mese in cui viene eseguito il processo, su base mensile.

Pianificazione annuale

Consente di specificare un giorno della settimana o del mese in cui viene eseguito il processo, su base annuale.

Pianificazione avanzata

Consente di specificare ulteriori informazioni di pianificazione.

Espressione cron

Per informazioni sulla compilazione di questo campo, consultare la pagina seguente:

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

Tempo di esecuzione

Consente di specificare l'ora del giorno, in formato a 24 ore, in cui viene eseguito il processo. Ad esempio, 14.15.

Associazione di una definizione snapshot a un'attività rapporto

Assegnare una definizione snapshot a un'attività di rapporto. In tal modo CA Identity Manager saprà quale definizione utilizzare durante l'esecuzione del rapporto. Le informazioni per i rapporti di CA Identity Manager possono inoltre provenire da varie origini e ogni rapporto deve essere associato a un'origine dati specifica, a seconda delle informazioni da includere.

Associazione di una definizione snapshot e di una connessione a un'attività rapporto

1. Nella Console utente selezionare Attività, Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
2. Cercare l'attività rapporto a cui associare una definizione snapshot.
3. Accedere alla scheda Schede e fare clic sul pulsante Modifica accanto alla scheda Associa definizioni snapshot.
4. Fare clic su Aggiungi.
5. Cercare la definizione snapshot da associare all'attività rapporto e fare clic su Seleziona.

Tenere presente quanto segue quando si associa una definizione snapshot a un'attività rapporto:

- Un rapporto può essere associato a una o più definizioni snapshot.
 - Una definizione snapshot può essere associata a più rapporti.
 - In caso di più snapshot associate a un'unica attività rapporto, queste non devono utilizzare lo stesso tempo di ricorrenza.
6. Fare clic su OK.

7. Passare alla scheda Ricerca e fare clic su Sfoglia per individuare gli schermi di ricerca.
8. Modificare la schermata di ricerca relativo all'attività rapporto e scegliere rptParamConn per il rapporto in Connection Object (Oggetto connessione).
9. Fare clic su OK.
10. Fare clic su Seleziona.
11. Fare clic su Inoltra.

Sincronizzazione account endpoint con modelli di account

Questa attività sincronizza un account endpoint dopo la modifica di un modello di account associato. Ad esempio, se un account Active Directory non ha gruppi, ma il modello di account associato può includere gruppi.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Attività, Endpoint, Gestisci endpoint, Verifica sincronizzazione account endpoint.
3. Selezionare un endpoint.

A questo punto compare una schermata che mostra gli account su tale endpoint, i modelli di account associati e quali attributi non sono sincronizzati.

4. Fare clic su Sincronizza per far corrispondere gli attributi di tali account con ciò che è definito nel modello di account.

Le modifiche effettuate ai modelli di account condizionano gli account esistenti nel modo seguente:

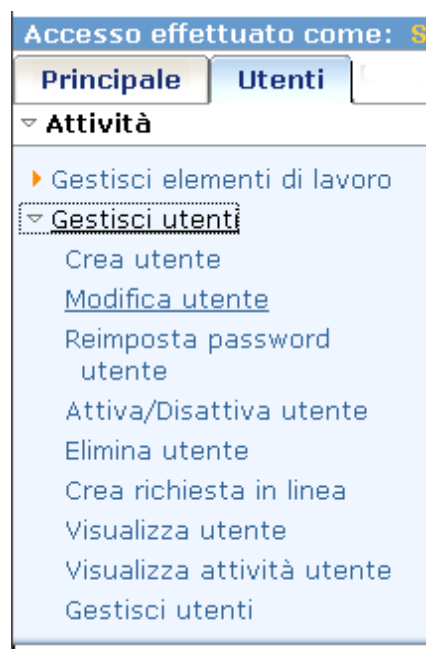
- Se si modifica il valore di un attributo di compatibilità, l'attributo account corrispondente viene aggiornato in modo da sincronizzarlo con il valore dell'attributo del modello di account. Consultare la descrizione di sincronizzazione minima e sicura.
- Alcuni attributi account vengono designati dal connettore come non aggiornati in caso di modifiche al modello di account, ad esempio l'attributo Password e determinati attributi che possono essere impostati dal tipo di endpoint unicamente durante la creazione dell'account.

Esempio di attività di amministrazione

Durante la creazione di un'attività di amministrazione vengono definiti i contenuti e il layout degli schermi associati all'attività, fra cui:

- Il nome dell'attività;
- La categoria in cui l'attività sarà visualizzata;
- Le schede e i campi da utilizzare nell'attività e le proprietà di visualizzazione dei campi;
- I campi che un amministratore può utilizzare in una query di ricerca, nonché i campi visualizzati nei risultati delle ricerche.

Per comprendere meglio gli elementi che costituiscono un'attività, si consideri l'attività Modifica utente. In questo caso, Utenti corrisponde alla categoria, Gestisci utenti a una sottocategoria e Modifica utente è l'attività. Quando si crea un'attività, vengono creati i nomi della categoria e dell'attività.



Quando si sceglie Modifica utente, viene visualizzato una schermata di ricerca. In una schermata *di ricerca* sono disponibili le opzioni per la ricerca dell'oggetto da visualizzare o modificare. Ogni opzione viene definita *filtro* e consente di specificare un limite per gli oggetti individuati dalla ricerca.

Dopo aver impostato tutti i campi disponibili nella schermata di ricerca, viene visualizzato una schermata contenente schede. Nella figura seguente sono illustrate le schede disponibili per l'attività Modifica utente. Nella scheda Profilo sono visualizzati gli attributi dell'utente, mentre nelle altre schede sono visualizzati i privilegi a livello di ruolo e di gruppo per l'utente specifico.

Per l'attività creata è necessario definire le schede da includere, nonché il relativo ordine e i contenuti.

Modifica utente: *liang*

Profilo	Ruoli di accesso	Ruoli di amministrazione	Gruppi	Delega elementi di lavoro

• = Obbligatorio

Organizzazione

ID utente

Attivato ☒

• **Nome**

• **Cognome**

• **Nome completo**

Posta elettronica

Ad esempio, utilizzando l'attività Modifica utente come modello è possibile creare un'attività Modifica appaltatore, per la quale sono state apportate modifiche:

- Ai campi della scheda Profilo;
- Alle schede da includere nell'attività e ai contenuti corrispondenti;
- Alla categoria in cui l'attività sarà visualizzata.

È possibile creare questa attività all'interno della nuova categoria Appaltatore.

Accesso effettuato come: SuperAdmin	
Principale	Contraente
Utenti	
▼ Attività	
▶ Gestisci Contraenti Modifica Contraente	

Nell'attività Modifica appaltatore sono disponibili alcuni campi della scheda Profilo dell'attività Modifica utente, oltre ad altri campi, ad esempio la data di inizio del contratto e la società dell'appaltatore. Gli amministratori potranno cercare un appaltatore in base al nome dell'appaltatore, alla società e alla data di inizio del contratto.

Modify Contractor: *jhansen*

Profile	Groups	Contractor Roles
User ID jhansen		
Enabled ☒		
• First Name	Julia	
• Last Name	Hansen	
Email	jhansen@wxyz.com	
Start Date	10/19/2007	
Company		

La nuova attività include anche una scheda Ruoli appaltatore, che consente di aggiungere ruoli per gli appaltatori.

Richiesta di un rapporto

Per visualizzare il rapporto, richiedere il rapporto a un utente con privilegi di amministratore per i rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere tempi lunghi o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Procedere come descritto di seguito:

1. Accedere alla console utente con privilegi utente per le attività di rapporto.
2. Selezionare Attività, Rapporti, Attività di rapporto e Richiedi un rapporto.
Viene visualizzato un elenco di rapporti.
3. Selezionare il rapporto che si desidera richiedere.
Verrà visualizzato una schermata di parametri.

Fornire le informazioni richieste sui parametri.

Nota: se si esegue un rapporto snapshot e non sono disponibili snapshot per il rapporto, è necessario innanzitutto acquisire una snapshot.

- In alcuni rapporti viene visualizzato lo stato del sistema in un determinato punto nel tempo. Quando si richiede un rapporto di questo tipo, si seleziona un punto nel tempo in cui visualizzare i dati del rapporto. Questo punto nel tempo viene chiamato *snapshot*.

Nota: le date e gli orari selezionabili per la snapshot sono prestabiliti. In genere, la configurazione delle snapshot viene eseguita dall'amministratore di sistema o da un altro utente con privilegi di amministrazione dei rapporti. Se non è disponibile alcuna snapshot per il rapporto che si desidera richiedere, contattare un amministratore di sistema.

- Alcuni rapporti visualizzano le attività corrispondenti a un determinato periodo di tempo. Solitamente, i titoli di questi rapporti iniziano con la parola *Verifica*. Quando si richiede un rapporto di questo tipo, è necessario selezionare il punto nel tempo per cui si desidera visualizzare i dati nel rapporto. Ad esempio, è possibile eseguire il rapporto di ripristino password basato su verifica per i 30 giorni precedenti.

4. Fare clic su Pianifica rapporto e selezionare una pianificazione per il rapporto.

Ora

Consente di specificare che il rapporto deve essere eseguito immediatamente.

Una volta

Specifica che il rapporto viene eseguito una volta, durante un determinato periodo di tempo. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

Nota: selezionare questa opzione se il rapporto richiesto necessita di una grande quantità di dati. Per risparmiare risorse di sistema, scegliere un periodo con minore attività di sistema.

5. Fare clic su Inoltra.

La richiesta di rapporto viene inoltrata. In base alla configurazione del proprio ambiente, la richiesta viene eseguita subito oppure dopo l'approvazione da parte di un amministratore.

In genere, prima che la richiesta del rapporto sia completata dal sistema, è necessaria l'approvazione di un amministratore di sistema o di un altro utente con privilegi di amministrazione dei rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere molto tempo o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Visualizzazione del rapporto

In base alla configurazione dell'ambiente in uso, è possibile che rapporto non venga visualizzato fino all'approvazione della richiesta da parte di un amministratore. Se il rapporto richiesto è in attesa di approvazione, il sistema invia un avviso di posta elettronica. Il rapporto che si desidera visualizzare non compare nell'elenco di ricerca finché non riceve l'approvazione.

Nota: per visualizzare i rapporti in CA Identity Manager utilizzando l'attività Visualizza rapporti personali, attivare i cookie di sessione di terze parti nel browser.

Procedere come descritto di seguito:

1. In Console utente, selezionare Attività, Rapporti, Attività di rapporto e fare clic su Visualizza rapporti personali.

2. Individuare il rapporto generato che si desidera visualizzare.

Verranno visualizzate le istanze del rapporto di ricorrenza generato e del rapporto su richiesta.

Nota: Se lo stato del rapporto è In sospeso/Ricorrente, il rapporto non viene generato e il suo completamento può richiedere tempi lunghi.

3. Selezionare il rapporto che si desidera visualizzare.
4. (Facoltativo) Fare clic su Esporta questo rapporto nell'angolo superiore sinistro per esportare il rapporto nei formati seguenti:

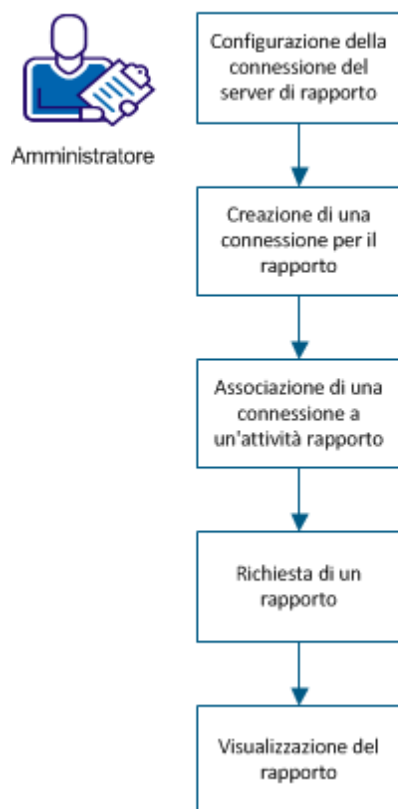
- Crystal Reports
- PDF
- Microsoft Excel (97-2003)
- Microsoft Excel (97-2003) - Solo dati
- Microsoft Excel (97-2003) - Modificabile
- Rich Text Format (RTF)
- Separated Values (CSV)
- XML

Esecuzione di rapporti non di snapshot

Un rapporto non di snapshot include dati tratti da altre origini dati, come i database di controllo, del flusso di lavoro o di persistenza delle attività. Nella console utente CA Identity Manager include rapporti di controllo predefiniti con il prefisso Audit- nel nome. Per impostazione predefinita, CA Identity Manager include solo rapporti di controllo, ma è possibile creare rapporti personalizzati per includere dati da qualsiasi origine dati.

Questo scenario descrive la procedura per configurare una connessione al database di rapporto ed eseguire un rapporto non di snapshot per un amministratore con privilegi avanzati.

Esecuzione di un rapporto non di snapshot



Il diagramma seguente illustra il processo di esecuzione di un rapporto di snapshot:

Per eseguire il rapporto non di snapshot, completare i passaggi seguenti:

1. [Configurare la connessione al server di rapporto.](#) (a pagina 430)
2. Creare una connessione per il rapporto.
3. Associare una connessione all'attività rapporto.
4. Richiedere un rapporto.

5. [Visualizzare il rapporto.](#) (a pagina 434)

Configurazione della connessione del server di rapporto

Per raccogliere i dati dal server di rapporto, è necessario configurare la connessione al server di rapporto. Prima di iniziare la procedura, raccogliere le informazioni seguenti sul server di rapporto:

Nome	Descrizione
Nome host	Nome host del computer su cui è installato il server di rapporto
Porta	Nome della porta del computer su cui è installato il server di rapporto
Nome della cartella rapporti	Posizione dei rapporti predefiniti di CA Identity Manager.
ID utente	Specifica l'utente creato per il server di rapporto.
Password	Specifica la password per l'utente creato nel server di rapporto.
Connessione protetta	Specifica la connessione protetta per il server di rapporto. Selezionare la casella di controllo per abilitare la connessione SSL (Secure Sockets Layer) tra CA Identity Manager e il server di rapporto. Nota: prima di selezionare la casella di controllo Connessione protetta, verificare che sia installato il certificato dal BO Server. Per ulteriori informazioni sulla configurazione di SSL, consultare il capitolo relativo all'installazione del server di rapporto della <i>Guida all'installazione</i>.
Server Web	Specifica il server Web. Impostare su non IIS per Tomcat.

Nota: si consiglia di impostare tutti i sistemi interessati dalla generazione di rapporti su ora e data identiche.

Procedere come descritto di seguito:

1. Nella console utente, fare clic su Sistema, Generazione rapporti, Connessione al server di rapporto.
2. Inserire le impostazioni del server di rapporto.
3. Fare clic su Verifica connessione per verificare la connessione.
4. Fare clic su Inoltra.

Viene stabilita la connessione al rapporto.

Creazione di una connessione per il rapporto

Le informazioni per i rapporti CA Identity Manager possono provenire da varie origini. Per specificare i dettagli di connessione a un'altra origine dati per il rapporto, creare una connessione JDBC in CA Identity Manager.

Procedere come descritto di seguito:

1. Nella console utente, selezionare Attività, Sistema, Gestione connessione JDBC, Crea connessione JDBC.
2. Creare un nuovo oggetto connessione oppure selezionare un oggetto connessione basato su una specifica origine dati JNDI.
3. Compilare tutti i campi necessari e fare clic su Inoltra.
Verrà creata una nuova connessione JDBC.

Importante. si consiglia di *non* utilizzare il database dell'archivio oggetti CA Identity Manager per la generazione dei rapporti.

Associazione di una connessione a un'attività di rapporto

Le informazioni per i rapporti di CA Identity Manager vengono acquisite da varie origini e ogni rapporto deve essere associato a un'origine dati specifica, a seconda delle informazioni da includere.

Associazione di una connessione a un'attività di rapporto

1. Nella Console utente selezionare Attività, Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
2. Cercare l'attività rapporto a cui associare una connessione.
3. Passare alla scheda Ricerca e fare clic su Sfoglia per individuare gli schermi di ricerca.
4. Modificare la schermata di ricerca relativo all'attività rapporto e scegliere una connessione per il rapporto in Connection Object (Oggetto connessione).
5. Fare clic su OK.
6. Fare clic su Seleziona.
7. Fare clic su Inoltra.

Richiesta di un rapporto

Per visualizzare il rapporto, richiedere il rapporto a un utente con privilegi di amministratore per i rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere tempi lunghi o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Procedere come descritto di seguito:

1. Accedere alla console utente con privilegi utente per le attività di rapporto.
2. Selezionare Attività, Rapporti, Attività di rapporto e Richiedi un rapporto.

Viene visualizzato un elenco di rapporti.

3. Selezionare il rapporto che si desidera richiedere.

Verrà visualizzato una schermata di parametri.

Fornire le informazioni richieste sui parametri.

Nota: se si esegue un rapporto snapshot e non sono disponibili snapshot per il rapporto, è necessario innanzitutto acquisire una snapshot.

- In alcuni rapporti viene visualizzato lo stato del sistema in un determinato punto nel tempo. Quando si richiede un rapporto di questo tipo, si seleziona un punto nel tempo in cui visualizzare i dati del rapporto. Questo punto nel tempo viene chiamato *snapshot*.

Nota: le date e gli orari selezionabili per la snapshot sono prestabiliti. In genere, la configurazione delle snapshot viene eseguita dall'amministratore di sistema o da un altro utente con privilegi di amministrazione dei rapporti. Se non è disponibile alcuna snapshot per il rapporto che si desidera richiedere, contattare un amministratore di sistema.

- Alcuni rapporti visualizzano le attività corrispondenti a un determinato periodo di tempo. Solitamente, i titoli di questi rapporti iniziano con la parola *Verifica*. Quando si richiede un rapporto di questo tipo, è necessario selezionare il punto nel tempo per cui si desidera visualizzare i dati nel rapporto. Ad esempio, è possibile eseguire il rapporto di ripristino password basato su verifica per i 30 giorni precedenti.

4. Fare clic su Pianifica rapporto e selezionare una pianificazione per il rapporto.

Ora

Consente di specificare che il rapporto deve essere eseguito immediatamente.

Una volta

Specifica che il rapporto viene eseguito una volta, durante un determinato periodo di tempo. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

Nota: selezionare questa opzione se il rapporto richiesto necessita di una grande quantità di dati. Per risparmiare risorse di sistema, scegliere un periodo con minore attività di sistema.

5. Fare clic su Inoltra.

La richiesta di rapporto viene inoltrata. In base alla configurazione del proprio ambiente, la richiesta viene eseguita subito oppure dopo l'approvazione da parte di un amministratore.

In genere, prima che la richiesta del rapporto sia completata dal sistema, è necessaria l'approvazione di un amministratore di sistema o di un altro utente con privilegi di amministrazione dei rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere molto tempo o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Visualizzazione del rapporto

In base alla configurazione dell'ambiente in uso, è possibile che rapporto non venga visualizzato fino all'approvazione della richiesta da parte di un amministratore. Se il rapporto richiesto è in attesa di approvazione, il sistema invia un avviso di posta elettronica. Il rapporto che si desidera visualizzare non compare nell'elenco di ricerca finché non riceve l'approvazione.

Nota: per visualizzare i rapporti in CA Identity Manager utilizzando l'attività Visualizza rapporti personali, attivare i cookie di sessione di terze parti nel browser.

Procedere come descritto di seguito:

1. In Console utente, passare a Rapporti, Attività di rapporto e fare clic su Visualizza rapporti personali.
2. Individuare il rapporto generato che si desidera visualizzare.

Verranno visualizzate le istanze del rapporto di ricorrenza generato e del rapporto su richiesta.

Nota: Se lo stato del rapporto è In sospeso/Ricorrente, il rapporto non viene generato e il suo completamento può richiedere tempi lunghi.

3. Selezionare il rapporto che si desidera visualizzare.
4. (Facoltativo) Fare clic su Esporta questo rapporto nell'angolo superiore sinistro per esportare il rapporto nei formati seguenti:
 - Crystal Reports
 - PDF
 - Microsoft Excel (97-2003)
 - Microsoft Excel (97-2003) - Solo dati
 - Microsoft Excel (97-2003) - Modificabile
 - Rich Text Format (RTF)
 - Separated Values (CSV)
 - XML

Imposta opzioni di segnalazione

Configurare il numero di istanze rapporto che possono essere generate da un utente per un rapporto specifico.

Come modificare le opzioni dei rapporti

1. Selezionare Attività, Rapporti, Attività di rapporto, Imposta opzioni di segnalazione.

In CA Identity Manager viene effettuata la connessione al server di rapporto IAM e viene recuperato un elenco di tutti i rapporti.

2. Scegliere un rapporto e fare clic su Modifica.

Verrà visualizzato il riquadro Attributi del rapporto.

3. Modificare i seguenti campi:

Nome

Specifica il nome visualizzato per il rapporto selezionato.

Numero di istanze

Specifica il numero di istanze consentite che possono essere generate da un utente per il rapporto in questione.

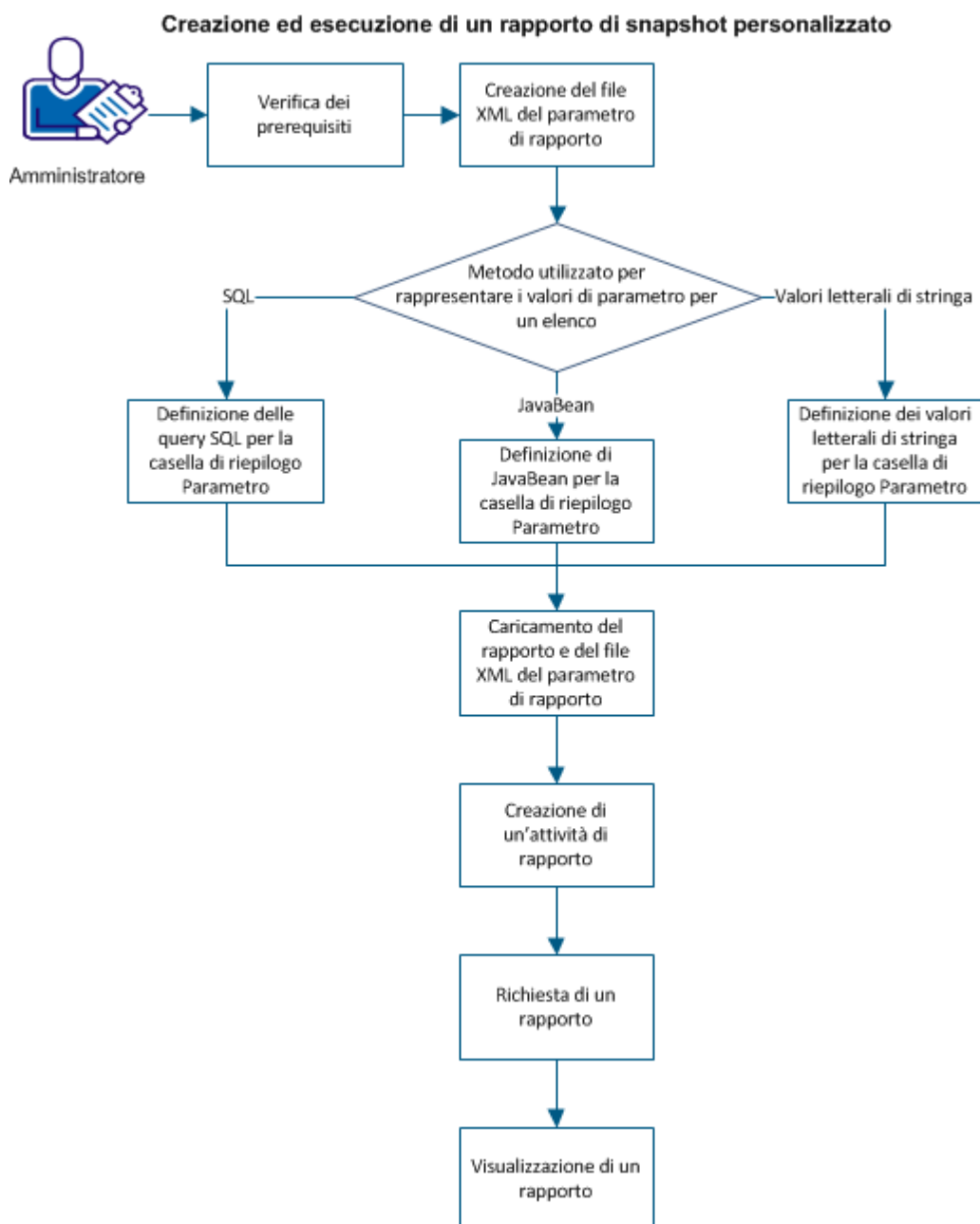
4. Fare clic su OK.

Gli attributi del rapporto vengono modificati.

Creazione ed esecuzione di un rapporto di snapshot personalizzato

CA Identity Manager consente di creare e personalizzare i rapporti in base alle esigenze aziendali. CA Identity Manager fornisce un file .xml per i parametri di rapporto che comprende tutti i parametri correlati agli attributi di generazione rapporti. A seconda delle esigenze aziendali è possibile scegliere gli attributi necessari in modo da inserire i dati del rapporto dall'origine dati di snapshot.

La figura seguente illustra la procedura per creare ed eseguire un rapporto di snapshot personalizzato:



L'amministratore di sistema deve completare i passaggi seguenti:

1. [Verifica dei prerequisiti](#) (a pagina 438)
2. [Creazione del file .xml dei parametri di rapporto](#) (a pagina 438)
3. Utilizzare uno dei metodi seguenti per rappresentare i valori di parametro per un elenco:
 - [Definizione delle query SQL per la casella di riepilogo Parametro](#) (a pagina 441)

- [Definizione dei bean Java per la casella di riepilogo Parametro](#) (a pagina 442)
- [Definizione dei valori letterali di stringa per la casella di riepilogo Parametro](#) (a pagina 442)
- 4. [Caricamento del rapporto e del file .xml dei parametri di rapporto](#) (a pagina 442)
- 5. Creazione dell'attività di rapporto
- 6. Richiesta di un rapporto
- 7. [Visualizzazione di un rapporto](#) (a pagina 434)

Creazione di un rapporto in Crystal Reports

Per utilizzare rapporti personalizzati in CA Identity Manager, creare un rapporto (file RPT) in Crystal Reports Developer. Per ulteriori informazioni sulla creazione di un rapporto in Crystal Reports, fare riferimento alla documentazione di Crystal Reports.

Nota: Per fare riferimento allo schema di CA Identity Manager e creare rapporti personalizzati, lo schema del database di CA Identity Manager è disponibile nella seguente posizione:

C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\db\objectstore

Creazione del file XML del parametro di rapporto

Un parametro è uno dei campi di un rapporto che è possibile utilizzare per filtrare i rapporti. È possibile generare un rapporto filtrando i dati mediante dei parametri. Per permettere la personalizzazione della schermata di ricerca del rapporto, ciascun rapporto (file RPT) è associato a un file XML del parametro di rapporto. In CA Identity Manager è possibile creare attività di rapporto e schermata di ricerca in modo che un utente possa immettere o selezionare i dati richiesti durante la generazione di un rapporto.

Nota: un file XML del parametro di rapporto è necessario solo se il rapporto interroga gli attributi nell'oggetto.

Il file XML del parametro di rapporto deve avere lo stesso nome del rapporto (file RPT) con un'estensione .xml. Ad esempio, se si carica un rapporto chiamato test1.rpt nel server di rapporto, il file XML deve essere chiamato test1.xml.

Il file XML del parametro di rapporto contiene i seguenti elementi:

<product>

Identifica il prodotto per il quale vengono utilizzati i parametri. È possibile creare diversi parametri per più prodotti utilizzando lo stesso file XML di parametro.

<screen>

Consente di definire i parametri visualizzati in una schermata. È possibile utilizzare l'elemento schermata per associare i parametri a una schermata specifica. L'ID della schermata è un valore alfanumerico e univoco e viene utilizzato per identificare le schermate e i relativi parametri.

<parameters>

Consente di specificare la raccolta di parametri per una schermata.

<param>

Consente di definire l'elemento parametro che invia specifici dati al rapporto. Nell'elemento <param> vengono utilizzati gli attributi seguenti:

id

Consente di definire il parametro del rapporto al quale associarsi.

Nota: L'ID deve avere lo stesso nome del parametro in Crystal Reports.

nome

Questo campo attualmente non viene utilizzato da CA Identity Manager. Impostare questo attributo sullo stesso valore dell'ID.

displaytext

Consente di specificare il testo intuitivo da visualizzare nella schermata per il parametro.

type

Consente di definire il tipo di parametro. La schermata mostra le modifiche in base a questo attributo. I tipi di parametro supportati sono i seguenti:

– **Casella di testo**

Esempio: <param id="param1" displaytext="First Name" name="param1" type="string"/>

– **Data e ora**

Esempio: <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

<param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

<param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

– **Elenco a discesa**

Esempio: `<param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>`

– **Casella di riepilogo**

Esempio: `<param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>`

– **Casella di opzione**

Esempio: `<param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>`

`<param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>`

`<param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>`

– **Casella di controllo**

Esempio: `<param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>`

row

Consente di definire quante righe sono visibili in una casella di riepilogo.

Impostazione predefinita: 5

default

Consente di definire il valore predefinito visualizzato nella schermata per un dato parametro. È possibile utilizzare questo attributo con la stringa, la casella di riepilogo e i tipi di elenco a discesa.

Definizione delle query SQL per la casella di riepilogo Parametro

È possibile definire query SQL come parte di una casella di riepilogo o di una casella a discesa nel file XML del parametro di rapporto. Quando si associa un parametro al rapporto e si crea un'attività di rapporto, il parametro viene mostrato nella casella di riepilogo o nella casella a discesa. Per utilizzare SQL nel parametro della casella a discesa o della casella di riepilogo, fornire una dichiarazione SQL valida nell'attributo SQL.

Esempio:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like 'S%"/>
```

Nell'esempio precedente, vengono forniti al rapporto tutti i cognomi degli utenti il cui nome inizia per S.

Tuttavia, la condizione del nome che inizia per S è statica. Questa query non è abbastanza flessibile per consentire all'utente di caricare il valore in base al valore di parametro, immesso in una delle schermate precedenti, che è stato utilizzato nello stesso gruppo di parametri di rapporto. Per utilizzare il valore precedente immesso in un'altra schermata, è possibile aumentare l'istruzione SQL con `##<parameter id>##`.

Ad esempio, se si dispone di un parametro con `id=User`, che era di tipo String:

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

Se si desidera utilizzare il valore immesso per quel parametro in SQL, l'istruzione SQL può essere come segue:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like '##User##'"/>
```

CA Identity Manager sostituisce `##User##` con il valore immesso per il parametro con `id=User`.

Nota: il valore di parametro da sostituire non può essere nella stessa schermata del parametro SQL. Ad esempio, se `lstlastname2` si trova nella schermata 3, il parametro Utente dovrebbe trovarsi in una delle schermate precedenti.

Definizione dei bean Java per la casella di riepilogo Parametro

In caso di errori durante l'utilizzo di SQL, è possibile utilizzare i componenti JavaBeans per calcolare i valori e fornire l'elenco delle coppie <key, value> a CA Identity Manager. I componenti JavaBeans devono trovarsi nel classpath di CA Identity Manager.

Esempio:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2" type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

Nell'esempio precedente, TestDataCollector recupera i valori secondo le proprie modalità e invia i dati dell'elenco a discesa al rapporto. Le coppie <chiave, valore> sono separate da %1F.

Assicurarsi che il componente JavaBean si trovi nella directory iam_im.ear\custom.

Nota: per ulteriori informazioni sull'implementazione di JavaBeans, consultare la [documentazione di BusinessObjects](#).

Definizione dei valori letterali di stringa per la casella di riepilogo Parametro

Il modo più semplice per rappresentare i valori di parametro di un elenco o una casella a discesa è mediante i valori letterali di stringa. Il valore di chiave è delimitato da %1F e ciascuna coppia <key, value> è separata da %1E.

Esempio:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

Caricamento del rapporto e del file XML del parametro di rapporto

Dopo aver creato il rapporto (RPT) e il corrispondente file .xml dei parametri di rapporto, caricare entrambi i file nel server di rapporto (BusinessObjects).

Procedere come descritto di seguito:

1. Accedere alla console di gestione centrale di BusinessObjects.
2. Fare clic su Folders.
3. Selezionare la cartella Rapporti IM.
4. Creare un pacchetto di oggetti.
5. Nel nuovo pacchetto di oggetti, accedere e aggiungere Crystal Reports.

6. Accedere al nuovo rapporto (RPT) creato.

Nota: Assicurarsi di aver selezionato la cartella dei rapporti di IM per salvare il rapporto.

7. Fare clic su OK.

Il file di Crystal Reports viene aggiunto.

8. Nel nuovo pacchetto di oggetti, aggiungere un nuovo documento locale e individuare il nuovo file .xml dei parametri di rapporto.

9. Selezionare il tipo di file *Text*.

10. Fare clic su OK.

Il rapporto e il file .xml dei parametri di rapporto vengono caricati. Ai fini della verifica, accedere alla cartella dei rapporti di IM e controllare che siano disponibili entrambi i file nuovi.

Creazione dell'attività di rapporto

Le attività relative di rapporto vengono utilizzate per creare, gestire, visualizzare ed eliminare i modelli dei rapporti generati nella Console utente.

Procedere come descritto di seguito:

1. Nella Console utente selezionare Attività, Ruoli e attività, Attività di amministrazione, Crea attività di amministrazione.
2. Selezionare Crea una nuova attività amministrativa e fare clic su OK.
3. Nella scheda Profilo, completare i seguenti campi:

Nome

Consente di definire il nome del rapporto. Ciascun nome di attività di rapporto deve essere univoco.

Tag

Definisce un identificatore univoco per l'attività. Viene utilizzato in un URL, un servizio Web o un file di proprietà. Deve consistere di lettere, numeri e/o sottolineature e iniziare con una lettera o sottolineatura.

Categoria

Specifica la categoria a cui l'attività attuale appartiene.

Nota: Selezionare la categoria Rapporti.

Categoria 2

Specifica la categoria secondaria a cui appartiene l'attività attuale. Immettere qualsiasi stringa in questo campo.

Oggetto principale

Consente di specificare l'oggetto nel quale verrà eseguita l'attività.

Nota: Selezionare Istanza di rapporto come oggetto primario.

Azione

Consente di specificare l'azione che viene eseguita sull'oggetto primario.

Nota: Selezionare l'azione Crea.

4. Per creare una nuova schermata di ricerca per l'attività di rapporto, completare i passaggi seguenti:
 - a. Nella scheda Cerca fare clic su Sfoglia per individuare le schermate di ricerca. Verrà visualizzato l'elenco degli schermi di ricerca disponibili.
 - b. Fare clic su Nuovo. Viene visualizzato il riquadro Crea schermata.
 - c. Selezionare Schermata di selezione Modello rapporto dall'elenco, quindi fare clic su OK.

CA Identity Manager si connette al server di rapporto e visualizza tutti i rapporti.

- d. Completare i seguenti campi:

Nome

Consente di definire il nome del rapporto. Ciascun nome di attività di rapporto dovrebbe essere univoco.

Tag

Agisce come ID univoco in un'attività. Può contenere caratteri ASCII (dalla A alla Z oppure dalla a alla z), cifre (da 0 a 9) oppure caratteri di sottolineatura e deve iniziare con una lettera o un carattere di sottolineatura.

Title

Definisce il titolo della nuova schermata di ricerca. Il titolo deve essere univoco.

Modello rapporto

Identifica il rapporto da associare alla schermata di ricerca.

Nota: Scegliere uno dei rapporti aggiunti al server di rapporto.

Oggetto di connessione per il rapporto

Definisce i dettagli di connessione dell'origine dati da utilizzare per il rapporto.

5. Fare clic su OK.

La nuova schermata di ricerca viene creata per i rapporti.

6. Durante la creazione della scheda Schede per l'attività di rapporto, completare i passaggi seguenti:

- a. Fare clic su Schede.

Vengono mostrate le schede visibili all'utente.

- b. Selezionare Controller scheda standard.

- c. Se il rapporto utilizza una definizione snapshot, completare i passaggi seguenti:

- a. Nella finestra Indicare le schede da visualizzare in questa attività, selezionare Associa definizioni snapshot.

La scheda Associa definizioni snapshot viene aggiunta all'elenco delle schede.

- b. Fare clic su  per modificare la scheda Associa definizioni snapshot.

- c. Fare clic su Aggiungi per associare l'attività di rapporto a una definizione snapshot.

Viene visualizzato l'elenco delle definizioni snapshot disponibili.

- d. Selezionare una definizione snapshot e fare clic su OK.

L'attività di rapporto viene associata a una definizione snapshot.

- d. Fare clic su Inoltra.

Viene creata l'attività di rapporto.

- e. Assegnare la nuova attività di rapporto a un ruolo di amministrazione.

Gli utenti con il ruolo di amministrazione di CA Identity Manager possono utilizzare la nuova attività di rapporto.

L'attività di rapporto è ora pronta per l'utilizzo da parte dell'amministratore.

Nota: un rapporto (file RPT) può essere associato a *una* sola attività di rapporto.

Richiesta di un rapporto

Per visualizzare il rapporto, richiedere il rapporto a un utente con privilegi di amministratore per i rapporti. In genere, prima che la richiesta del rapporto sia completata dal sistema, è necessaria l'approvazione di un amministratore di sistema o di un altro utente con privilegi di amministrazione dei rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere tempi lunghi o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con diritti di accesso alle attività relative ai rapporti.
2. Dal menu di navigazione, selezionare Attività, Rapporti, Attività di rapporto, Richiedi un rapporto.

Viene visualizzato un elenco di rapporti.

3. Selezionare il rapporto che si desidera richiedere.

Verrà visualizzato una schermata di parametri.

4. Fornire le informazioni richieste sui parametri.

Nota: se si esegue un rapporto snapshot e non sono disponibili snapshot per il rapporto, è necessario innanzitutto acquisire una snapshot.

- In alcuni rapporti viene visualizzato lo stato del sistema in un determinato punto nel tempo. Quando si richiede un rapporto di questo tipo, si seleziona un punto nel tempo in cui visualizzare i dati del rapporto. Questo punto nel tempo viene chiamato *snapshot*.

Nota: le date e gli orari selezionabili per la snapshot sono prestabiliti. In genere, la configurazione delle snapshot viene eseguita dall'amministratore di sistema o da un altro utente con privilegi di amministrazione dei rapporti. Se non è disponibile alcuna snapshot per il rapporto che si desidera richiedere, contattare un amministratore di sistema.

- Alcuni rapporti visualizzano le attività corrispondenti a un determinato periodo di tempo. Solitamente, i titoli di questi rapporti iniziano con la parola *Verifica*. Quando si richiede un rapporto di questo tipo, è necessario selezionare il punto nel tempo per cui si desidera visualizzare i dati nel rapporto. Ad esempio, è possibile eseguire il rapporto di ripristino password basato su verifica per i 30 giorni precedenti.

5. Fare clic su Pianifica rapporto e selezionare una pianificazione per il rapporto.

Ora

Consente di specificare che il rapporto deve essere eseguito immediatamente.

Una volta

Specifica che il rapporto viene eseguito una volta, durante un determinato periodo di tempo. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

Nota: selezionare questa opzione se il rapporto richiesto necessita di una grande quantità di dati. Per risparmiare risorse di sistema, scegliere un periodo con minore attività di sistema.

6. Fare clic su Inoltra.

La richiesta di rapporto viene inoltrata. In base alla configurazione del proprio ambiente, la richiesta viene eseguita subito oppure dopo l'approvazione da parte di un amministratore.

Visualizzazione del rapporto

In base alla configurazione dell'ambiente in uso, è possibile che rapporto non venga visualizzato fino all'approvazione della richiesta da parte di un amministratore. Se il rapporto richiesto è in attesa di approvazione, il sistema invia un avviso di posta elettronica. Il rapporto che si desidera visualizzare non compare nell'elenco di ricerca finché non riceve l'approvazione.

Nota: per visualizzare i rapporti in CA Identity Manager utilizzando l'attività Visualizza rapporti personali, attivare i cookie di sessione di terze parti nel browser.

Procedere come descritto di seguito:

1. In Console utente, selezionare Attività, Rapporti, Attività di rapporto e fare clic su Visualizza rapporti personali.

2. Individuare il rapporto generato che si desidera visualizzare.

Verranno visualizzate le istanze del rapporto di ricorrenza generato e del rapporto su richiesta.

Nota: Se lo stato del rapporto è In sospeso/Ricorrente, il rapporto non viene generato e il suo completamento può richiedere tempi lunghi.

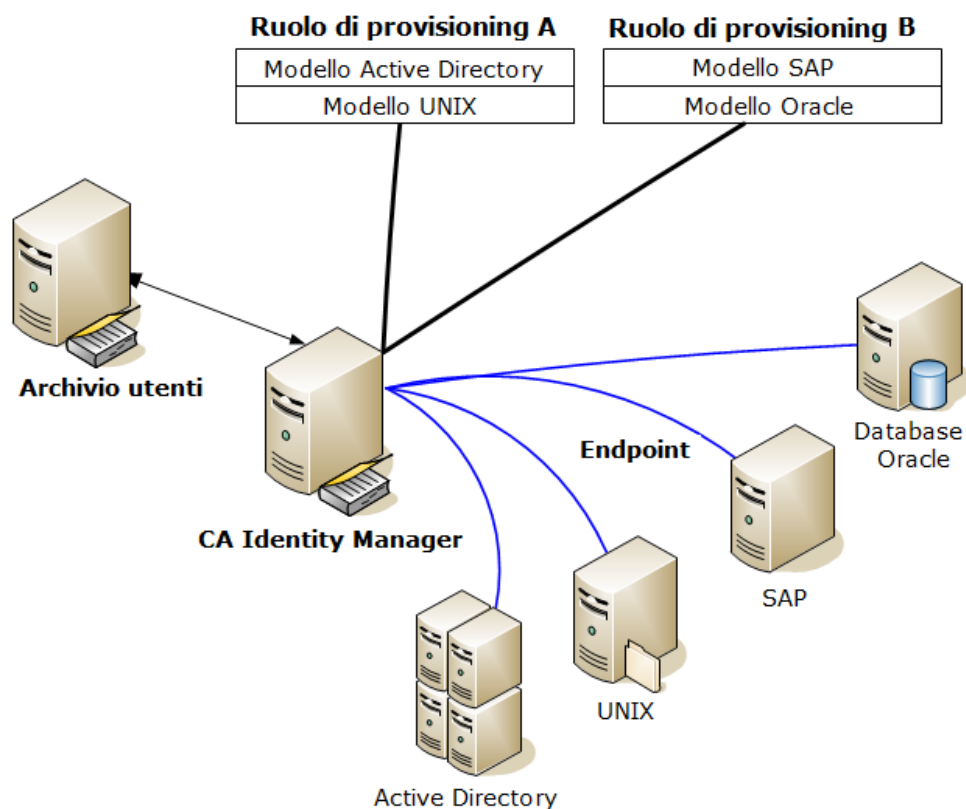
3. Selezionare il rapporto che si desidera visualizzare.
4. (Facoltativo) Fare clic su Esporta questo rapporto nell'angolo superiore sinistro per esportare il rapporto nei formati seguenti:

- Crystal Reports
- PDF
- Microsoft Excel (97-2003)
- Microsoft Excel (97-2003) - Solo dati
- Microsoft Excel (97-2003) - Modificabile
- Rich Text Format (RTF)
- Separated Values (CSV)
- XML

Sincronizzazione di utenti, account e ruoli

L'integrazione di account ed endpoint multipli in un sistema singolo di gestione degli utenti può causare una perdita di sincronizzazione. I ruoli di provisioning o i modelli di account che vengono assegnati a un utente possono differire dagli account attualmente esistenti per tale utente.

Ad esempio, considerare una situazione con due ruoli di provisioning, uno con i modelli di account UNIX e Active Directory e un altro con i modelli SAP e Oracle. L'utente john_smith ha il ruolo di provisioning A, che contiene i modelli di account UNIX e Active Directory, ma tale utente ha solo un account Active Directory. È possibile che il modello di account UNIX sia stato aggiunto al ruolo dopo essere stato aggiunto all'utente. Perciò, l'amministratore sincronizza l'utente con la definizione attuale di ruolo.



Le situazioni seguenti costituiscono altri motivi che possono causare la perdita di sincronizzazione con i ruoli di provisioning o i modelli di account:

- I precedenti tentativi di creare gli account necessari non sono andati a buon fine a causa di problemi legati all'hardware o al software nella propria rete, causando la perdita di account.
- I ruoli di provisioning e i modelli di account cambiano, creando account extra o mancanti.
- Gli account sono stati assegnati a modelli di account dopo la loro creazione, quindi gli account esistono, ma non sono sincronizzati con i relativi modelli di account.
- La creazione di un nuovo account viene ritardata, in quanto era stato specificato che l'account sarebbe stato creato successivamente.
- È stato acquisito un endpoint. Durante l'esplorazione e la correlazione, il Server di provisioning non ha assegnato automaticamente ruoli di provisioning agli utenti. Aggiornare il ruolo per indicare gli utenti che necessitano di account sull'endpoint. Qualsiasi account messo in correlazione con un utente viene classificato come account extra quando l'utente viene sincronizzato.
- È stato assegnato un account esistente a un utente, copiando l'account sull'utente.
- È stato creato un account per un utente, invece di assegnare l'utente a un ruolo. Ad esempio è stato copiato un utente su un modello di account che non è in un ruolo di provisioning per tale utente. L'account viene classificato come account extra o come account con un modello di account extra. Se si copia l'utente su un endpoint per creare un account utilizzando il modello di account predefinito, tale account potrebbe essere un account extra.

Le sezioni seguenti spiegano come eseguire i tre tipi di sincronizzazione:

1. [Sincronizzazione utente con ruoli](#) (a pagina 175).
2. [Sincronizzazione utente con modelli account](#) (a pagina 175).
3. [Sincronizzazione account endpoint con modelli account](#) (a pagina 177).

Sincronizzazione utente con ruoli

Questa attività crea, aggiorna o elimina gli account, in modo che siano conformi ai ruoli di provisioning assegnati a un utente. Ad esempio, gli amministratori utilizzano strumenti nativi su un endpoint, per aggiungere o eliminare account, ma l'endpoint non è ancora stato riesplorato per aggiornare la directory di provisioning. Perciò gli utenti hanno account extra o mancanti. Questa attività assicura inoltre che ciascun account appartiene ai modelli di account corretti.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Utenti, Sincronizzazione, Verifica sincronizzazione ruolo.
3. Selezionare un utente.

Viene visualizzata una schermata che mostra gli account previsti, gli account extra e gli account mancanti.

4. Fare clic su Sincronizza per far corrispondere gli account con il modello in questo ruolo.

- a. È possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account per l'utente prescrive lo stesso account, l'account viene creato unendo tutti i modelli di account interessati.

Questo account viene assegnato ai modelli di account attualmente non sincronizzati con l'account.

- b. È possibile selezionare una casella di controllo per eliminare gli account extra. Tuttavia, gli utenti possono avere motivi legittimi per avere questi account. In questo caso lasciare questa opzione deselezionata.

Su determinati endpoint la funzione di eliminazione dell'account è disattivata, per questo motivo l'account non viene eliminato.

Sincronizzazione utente con modelli account

Questa attività sincronizza gli attributi per gli account endpoint con i modelli di account associati per un determinato utente. Tuttavia la sincronizzazione completa dipende dai seguenti fattori:

- La sincronizzazione completa dell'account si verifica in due situazioni. Un modello di account utilizza una [sincronizzazione sicura](#) (a pagina 178) o due o più modelli di account sono stati aggiunti a un account.
- Se un modello di account utilizza una [sincronizzazione minima](#) (a pagina 178), tale attività avvia una sincronizzazione account che coinvolge solamente questo modello. Se l'account non fosse stato precedentemente sincronizzato con altri modelli di account prima di questo aggiornamento, potrebbe essere ancora non sincronizzato anche in seguito.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Utenti, Sincronizzazione, Verifica sincronizzazione modello account.
3. Selezionare un utente.

Viene visualizzata una schermata che mostra gli account previsti, gli account extra e gli account mancanti.

4. Fare clic su Sincronizza per far corrispondere gli account con il modello.
 - a. È possibile selezionare una casella di controllo per creare l'account sull'endpoint. Se più di un modello di account per l'utente prescrive lo stesso account, l'account viene creato unendo i modelli di account interessati.

Questo account viene assegnato ai modelli di account non sincronizzati con l'account. La sincronizzazione dell'account non è necessaria sugli account appena creati.

- b. È possibile selezionare una casella di controllo per eliminare gli account extra. Tuttavia, gli utenti possono avere motivi legittimi per avere questi account. In questo caso lasciare questa opzione deselezionata.

Su determinati endpoint la funzione di eliminazione dell'account è disattivata, per questo motivo l'account non viene eliminato.

Sincronizzazione account endpoint con modelli di account

Questa attività sincronizza un account endpoint dopo la modifica di un modello di account associato. Ad esempio, se un account Active Directory non ha gruppi, ma il modello di account associato può includere gruppi.

Procedere come descritto di seguito:

1. Accedere alla console utente.
2. Selezionare Endpoint, Gestisci endpoint, Verifica sincronizzazione account endpoint.
3. Selezionare un endpoint.

A questo punto compare una schermata che mostra gli account su tale endpoint, i modelli di account associati e quali attributi non sono sincronizzati.

4. Fare clic su Sincronizza per far corrispondere gli attributi di tali account con ciò che è definito nel modello di account.

Le modifiche effettuate ai modelli di account condizionano gli account esistenti nel modo seguente:

- Se si modifica il valore di un attributo di compatibilità, l'attributo account corrispondente viene aggiornato in modo da sincronizzarlo con il valore dell'attributo del modello di account. Consultare la descrizione di sincronizzazione minima e sicura.

- Alcuni attributi account vengono designati dal connettore come non aggiornati in caso di modifiche al modello di account, ad esempio l'attributo Password e determinati attributi che possono essere impostati dal tipo di endpoint unicamente durante la creazione dell'account.

Aggiornamento degli attributi

Quando vengono modificati gli attributi di compatibilità in un modello di account, è possibile che l'attributo corrispondente negli account venga modificato. Questa modifica ha un impatto sugli attributi dell'account. L'impatto si basa sui seguenti fattori:

- Se la definizione del modello di account prevede l'utilizzo della sincronizzazione minima o sicura.
- Se l'account appartiene a più modelli di account.

Sincronizzazione minima

La sincronizzazione minima assicura che gli utenti dispongano degli attributi di compatibilità minimi richiesti per i relativi account. Si tratta della sincronizzazione predefinita nella maggior parte dei tipi di endpoint. Se si aggiorna un modello che utilizza la sincronizzazione minima, CA Identity Manager aggiorna gli attributi di capacità nel modo seguente:

- Se viene aggiornato un campo numerico in un modello di account e il nuovo numero è maggiore di quello nell'account, il valore nell'account viene modificato in modo che corrisponda al nuovo numero.
- Se una casella di controllo in un modello di account non era selezionata e successivamente viene selezionata, la casella di controllo viene aggiornata in tutti gli account in cui non è selezionata.
- Se viene modificato un elenco in un modello di account, vengono aggiornati tutti gli account per includere tutti i valori presenti nel nuovo elenco che non erano inclusi nell'elenco di valori dell'account.

Se un account appartiene ad altri modelli di account, a prescindere dal fatto che tali modelli utilizzino la sincronizzazione minima o sicura, in CA Identity Manager viene consultato solo il modello modificato. Questa procedura risulta più efficiente rispetto al controllo di tutti i modelli di account. Poiché con la sincronizzazione minima vengono solo aggiunte compatibilità agli account, in genere non è necessario consultare altri modelli di account.

Nota: in caso di propagazione da un modello di account con sincronizzazione minima, le modifiche che comportano la rimozione o la riduzione di compatibilità possono lasciare alcuni account privi di sincronizzazione. Tenere presente che la sincronizzazione minima non determina mai la rimozione o la riduzione di compatibilità. Senza consultare altri modelli per un account, la propagazione non considera se la sincronizzazione minima è sufficiente.

In questa situazione, utilizzare Sincronizza utente con modelli account per sincronizzare l'account con i rispettivi modelli di account.

Sincronizzazione sicura

La sincronizzazione sicura garantisce che gli account presentino gli stessi attributi account specificati nel modello di account.

Ad esempio, a un modello di account UNIX esistente è stato aggiunto un gruppo. All'inizio, il modello di account inseriva gli account nel gruppo del personale. Adesso si desidera inserire gli account nei gruppi del personale e del sistema. Tutti gli account associati al modello di account si considerano sincronizzati quando ciascuno è inserito in entrambi i gruppi del personale e del sistema (e in nessun altro gruppo). Gli account non presenti nel gruppo del personale sono aggiunti a entrambi i gruppi.

Tra gli altri fattori da considerare vi sono le seguenti situazioni:

- Se il modello di account utilizza la sincronizzazione sicura, qualsiasi account che appartiene ad altri gruppi, diversi da quelli del personale e del sistema, viene rimosso da quei gruppi extra.
- Se il modello di account utilizza la sincronizzazione minima, gli account vengono aggiunti ai gruppi del personale e del sistema. Qualsiasi account con gruppi aggiuntivi definiti resta inserito in questi gruppi.

Nota: Sincronizzare regolarmente gli account con i relativi modelli per far sì che gli account rimangano sincronizzati con i relativi modelli di account.

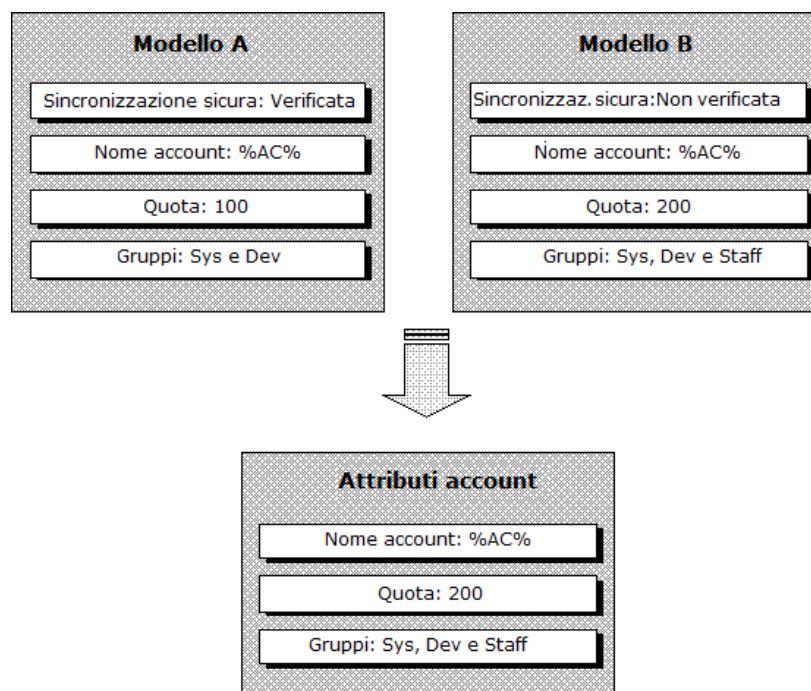
Account con più modelli

La sincronizzazione dipende anche se l'account appartiene a più modelli di account. Se un account ha un solo modello di account che utilizza la sincronizzazione sicura, ogni attributo viene aggiornato in modo che corrisponda esattamente a quanto restituito dal valore dell'attributo del modello di account. Si ottiene lo stesso risultato come se l'attributo fosse un attributo iniziale.

Un account può appartenere a più modelli di account, come nel caso di un utente che appartiene a più ruoli di provisioning, ognuno dei quali prevede un certo livello di accesso sullo stesso endpoint gestito. In questo caso, CA Identity Manager associa quei modelli di account in un unico modello di account valido che definisce il soprainsieme di compatibilità prese dai singoli modelli di account. Questo modello di account utilizza una sincronizzazione minima se tutti i singoli modelli di account sono minimi, oppure la sincronizzazione sicura se un singolo modello di account è sicuro.

Nota: in genere viene utilizzata solo la sincronizzazione minima o solo quella sicura per i modelli di account che controllano un account, a seconda se i propri ruoli aziendali definiscono completamente gli accessi necessari per gli utenti. Se gli utenti non rientrano in ruoli ben precisi ed è richiesta flessibilità per concedere compatibilità aggiuntive agli account utente, utilizzare la sincronizzazione minima. Se è possibile definire ruoli per specificare esattamente gli accessi necessari agli utenti, utilizzare la sincronizzazione sicura.

L'esempio seguente mostra l'associazione di più modelli di account in un singolo modello di account valido. In questo esempio, un modello di account viene contrassegnato per la sincronizzazione minima e l'altro per la sincronizzazione sicura. Di conseguenza, il modello di account valido creato combinando i due modelli di account viene considerato come un modello di account con sincronizzazione sicura. L'attributo Quota, espresso con un numero intero, adotta il valore maggiore dai due modelli di account, mentre l'attributo Gruppi con più valori adotta l'unione dei valori tratti dai due criteri.



Attributi solo per i nuovi account

In un modello di account, alcuni attributi vengono applicati solo durante la creazione dell'account. Ad esempio, l'attributo Password è un'espressione di regola che definisce la password per i nuovi account. Questa espressione di regola non aggiorna mai la password di un account. Le modifiche apportate all'espressione di regola per la password interessano solo sugli account creati successivamente all'impostazione di tale espressione.

Analogamente, un'espressione di regola modello per un attributo di account di sola lettura interessa solo gli account creati successivamente all'impostazione di tale espressione. La sua modifica non incide sugli account esistenti.

Risoluzione dei problemi

Nella sezione seguente sono riportati gli argomenti relativi alla risoluzione dei problemi che riguardano la creazione dei rapporti.

La visualizzazione di un rapporto ridirige alla pagina di accesso di Infoview

Quando si visualizza un rapporto in CA Identity Manager, l'utente viene reindirizzato alla pagina di accesso Infoview di BusinessObjects.

Visualizzare il rapporto se ridiretto

1. Accertarsi di utilizzare il nome dominio completo del server di rapporto CA (BusinessObjects).
2. Fare clic con il tasto destro del mouse sulla pagina Web di accesso a Infoview e selezionare View source (Visualizza origine).
3. Trovare l'URL del rapporto.
4. Copiare l'URL in una nuova finestra del browser.
5. Se non si riesce a visualizzare il rapporto, utilizzare uno strumento di analisi HTTP per fornire ulteriori informazioni.
6. Se si visualizza il rapporto, provare a correggere le impostazioni del browser in uno dei modi seguenti:
 - Accettare cookie di terze parti.
 - Accettare cookie di sessione.
 - Rimuovere impostazioni di protezione avanzata.

Generazione di account utente per oltre 20.000 record

Se esistono più di 20.000 record, sono necessari dei passaggi aggiuntivi per generare un rapporto account utente.

Per generare un rapporto account utente per oltre 20.000 record

1. Aprire la console di gestione centrale di BusinessObjects (Oggetti aziendali).
2. Fare clic su Server e selezionare *nomeserver.pageserver*.
3. Selezionare un numero illimitato di record per le voci dei record del database da leggere durante l'anteprima o l'aggiornamento di un rapporto.
4. Utilizzando Crystal Reports, aprire il rapporto degli account utente.
5. Da Database, impostare la posizione dell'origine dati nel database snapshot.
6. Salvare le modifiche.
7. Da Database, Datasource Expert, fare clic con il pulsante destro del mouse su Comando nella parte destra della finestra.
Verrà visualizzata la sintassi SQL sul lato sinistro e l'elenco Parametro.
8. Immettere il nome del parametro così come visualizzato nel campo dei parametri nel modello di rapporto.
9. Modificare la query sul lato sinistro e aggiungere il parametro alla query.
Ad esempio, se si ha il parametro reportid, la query sarà:

```
Select * from endPointAttributes, endpointview, imreport6  
where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and  
endPointAttributes.imr_reportid = endpointview.imr_reportid  
    endpointview.imr_reportid = imreport6.imr_reportid and  
    imreport6.imr_reportid = {?reportid}
```
10. Salvare il rapporto.

Capitolo 14: Criteri di identità

Questa sezione contiene i seguenti argomenti:

[Criteri di identità](#) (a pagina 459)

[Criteri di identità preventivi](#) (a pagina 482)

[Combinazione di criteri di identità e criteri di identità preventivi](#) (a pagina 492)

Criteri di identità

Un criterio di identità è un insieme di modifiche di business che si verificano quando un utente soddisfa una determinata condizione o regola. È possibile utilizzare set di criteri di identità per svolgere le seguenti attività:

- Automazione di specifiche attività di gestione dell'identità, ad esempio l'assegnazione di ruoli e di appartenenza ai gruppi, l'allocazione di risorse o la modifica degli attributi dei profili utenti.
- Applicazione dell'imposizione di mansioni. Ad esempio, è possibile creare un set di criteri di identità per impedire ai membri del ruolo Firmatario assegni di venire associati al ruolo Approvatore assegni, nonché per impedire ai dipendenti della società di emettere assegni con un importo maggiore di € 10.000.
- Applicazione della conformità. Ad esempio, è possibile sottoporre a revisione gli utenti associati ad uno specifico ruolo e con un reddito superiore a € 100.000.

I criteri di identità che applicano la conformità vengono definiti *criteri di conformità*.

Le modifiche aziendali associate ad un criterio di identità includono:

- Assegnazione o revoca di ruoli, compresi i ruoli di provisioning (se si utilizza solo una directory di provisioning)
- Assegnazione o revoca dell'appartenenza a gruppi
- Aggiornamento degli attributi in un profilo utente

Ad esempio, una società può creare un criterio di identità in base al quale tutti i vicepresidenti appartengono al gruppo Membro country club e sono associati al ruolo Approvatore stipendi. Quando il titolo di un utente viene modificato in Vicepresidente e tale utente viene sincronizzato con il criterio di identità, CA Identity Manager aggiunge tale utente al gruppo e al ruolo appropriati. Quando un vicepresidente viene promosso a CEO, non soddisferà più la condizione definita dal criterio di identità Vicepresidente e pertanto le modifiche applicate da tale criterio verranno revocate, mentre verranno applicate le nuove modifiche in base al criterio CEO.

Le azioni di modifica che si verificano in base ad un criterio di identità contengono eventi che possono essere inseriti in un controllo a livello di flusso di lavoro e sottoposti a verifica. Nell'esempio precedente, il ruolo Approvatore stipendi assegna privilegi molto significativi ai relativi membri. Per proteggere il ruolo di Approvatore stipendi, l'azienda può creare un processo del flusso di lavoro che richiede una serie di approvazioni prima che il ruolo venga assegnato e configurare CA Identity Manager in modo che verifichi l'assegnazione del ruolo.

Per semplificare la gestione dei criteri di identità, tali criteri vengono raggruppati in set. Ad esempio, i criteri Vicepresidente e CEO possono essere inclusi nel set di criteri di identità Privilegi dirigenti.

Nota: In CA Identity Manager è disponibile un ulteriore tipo di criteri di identità, i cosiddetti *criteri di identità preventivi* (a pagina 482). Tali criteri, che vengono eseguiti prima dell'inoltro di un'attività, consentono all'amministratore di verificare la presenza di violazioni dei criteri prima di assegnare privilegi o modificare attributi del profilo. Se esiste una violazione, l'amministratore potrà cancellarla prima di inoltrare l'attività.

Pianificazione del set di criteri di identità

Un set di criteri di identità contiene uno o più criteri di identità. Prima di creare un set di criteri di identità, utilizzare la seguente tabella come riferimento per creare i singoli criteri inclusi nel set.

Domanda	Risposta
Qual è il nome che si desidera assegnare al criterio di identità?	
A quali utenti il criterio di identità può essere applicato?	
Quando un criterio di identità viene applicato ad un utente, quali azioni devono essere eseguite da CA Identity Manager?	
Quando un criterio di identità applicato ad un utente non è più valido, quali azioni devono essere eseguite da CA Identity Manager?	
CA Identity Manager deve applicare le modifiche previste da un criterio di identità più volte oppure solo la prima volta che un utente soddisfa le condizioni definite nel criterio?	

Dopo aver completato la precedente tabella per ogni criterio di identità incluso in un set di criteri, verificare che non siano presenti conflitti tra i singoli criteri. Ad esempio, accertarsi che un criterio non conceda un privilegio revocato da un altro criterio.

Creazione di un set di criteri di identità

Per creare un set di criteri di identità, è necessario disporre del ruolo Gestore sistema oppure di un ruolo contenente l'attività Crea set di criteri di identità.

Per creare un set di criteri di identità, attenersi alla seguente procedura.

1. [Definizione del profilo del set di criteri di identità](#) (a pagina 461)
2. [Creazione di una regola membri del set di criteri](#) (a pagina 462)
3. [Creazione di un criterio di identità](#) (a pagina 462)
4. [Definizione dei proprietari del set di criteri di identità](#) (a pagina 471)

Nota: per usare criteri per un ambiente CA Identity Manager, abilitare i criteri di identità nella console di gestione di CA Identity Manager. Per ulteriori informazioni, vedere la *Configuration Guide*.

Definizione del profilo del set di criteri di identità

Nella scheda Profilo è possibile definire le proprietà di base di un set di criteri di identità.

Per definire un set di criteri di identità

1. Selezionare Criteri, Gestisci criteri di identità, Crea set di criteri di identità nella console utente.

È necessario essere connessi a CA Identity Manager come utente con privilegi adatti alla gestione dei criteri di identità. Il ruolo predefinito Gestione sistema include tali privilegi.
2. Scegliere di creare un nuovo set di criteri di identità oppure di creare una copia di un set di criteri di identità esistente.
3. Digitare il nome da assegnare al set di criteri di identità.
4. Specificare una categoria per il set di criteri di identità.

La categoria consente di raggruppare diversi set di criteri di identità con finalità simili per il reporting. Il campo Categoria è obbligatorio.
5. Facoltativamente, digitare una descrizione da associare al set di criteri di identità.
6. Se non si desidera rendere il set di criteri di identità disponibile per l'utilizzo, deselezionare la casella di controllo Attivato.
7. Una volta completata la scheda Profilo, selezionare la scheda Criteri per creare i criteri per il set di criteri di identità.

Ulteriori informazioni:

[Creazione di un criterio di identità](#) (a pagina 462)

[Creazione di una regola membri del set di criteri](#) (a pagina 462)

Creazione di una regola membri del set di criteri

È possibile creare una regola membri del set di criteri in modo che quest'ultimo valga solo per determinati utenti. La regola viene valutata prima dei criteri di identità nel set, con un considerevole risparmio di tempo. Ad esempio, se la regola membri limita la valutazione dei criteri di identità al 10% degli utenti, il tempo necessario per la valutazione risulterebbe ridotto del 90%.

Per creare una regola membri del set di criteri

1. Selezionare la scheda Criteri.
2. Fare clic sul simbolo di modifica sotto a Regola membri del set di criteri.
3. Immettere una regola per applicarle il criterio solo a determinati utenti.
4. Fare clic su OK.

Ulteriori informazioni:

[Creazione di un criterio di identità](#) (a pagina 462)

Creazione di un criterio di identità

Dopo aver definito il profilo e la regola membro del set di criteri di identità, è possibile definire i criteri di identità da includere in tale set.

Nota: nelle implementazioni di grandi dimensioni, la valutazione delle regole dei criteri di identità può richiedere molto tempo. Per ridurre il tempo necessario alla valutazione delle regole che includono attributi utente, è possibile attivare l'opzione di valutazione in memoria. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Come creare un criterio di identità

1. Selezionare la scheda Criteri.
2. Fare clic su Aggiungi.
3. Immettere il nome da assegnare al criterio di identità.
4. Selezionare la casella di controllo Applicare una volta se si desidera applicare il criterio solo quando un utente lo soddisfa per la prima volta.

5. Selezionare la casella di controllo Compatibilità per contrassegnare il criterio come criterio di compatibilità.

Se questa casella di controllo è selezionata:

- In CA Identity Manager è possibile generare rapporti relativi agli utenti non sincronizzati con i criteri di compatibilità.
- L'azione Violazione compatibilità è disponibile nella casella di riepilogo Azione su Applica criteri/Azione su Rimuovi criteri.

6. Identificare gli utenti ai quali applicare il criterio nella sezione Condizione criteri.
7. Nella sezione Azione su Applica criteri, definire le azioni eseguite da CA Identity Manager quando il criterio di identità viene applicato ad un utente.
8. Nella sezione Azione su Rimuovi criteri, definire le azioni eseguite da CA Identity Manager quando un utente non soddisfa più le condizioni definite dal criterio di identità.
9. Fare clic su OK.

Nota: prima di utilizzare un set di criteri di identità creato, è necessario abilitare i criteri di identità nella console di gestione. Per ulteriori informazioni, vedere la *Configuration Guide*.

Impostazione dell'opzione Applicare una volta

CA Identity Manager applica un criterio di identità in base all'impostazione dell'opzione Applicare una volta.

Attivazione dell'impostazione dell'opzione Applicare una volta

Se l'impostazione dell'opzione Applicare una volta è attivata, CA Identity Manager applica le modifiche associate al criterio di identità quando un utente soddisfa *per la prima volta* le condizioni definite dal criterio. Le azioni di modifica associate al criterio si verificano solo una volta. Pertanto, CA Identity Manager non applica gli aggiornamenti del criterio agli utenti se tale criterio è stato precedentemente applicato.

Quando un utente non soddisfa più le condizioni definite nel criterio, CA Identity Manager esegue le azioni di rimozione definite nel criterio.

L'impostazione dell'opzione Applicare una volta viene in genere utilizzata durante la fornitura delle risorse. Ad esempio, è possibile disporre di un criterio che assegna un telefono cellulare ai manager. Quando un utente diventa manager, gli viene assegnato un telefono cellulare. CA Identity Manager assegna un telefono cellulare solo una volta e non ogni volta che il criterio viene valutato. Se il criterio relativo al telefono cellulare viene aggiornato in modo da includere un modello di telefono più nuovo, CA Identity Manager non assegna nuovi telefoni cellulari ai manager esistenti.

Nota: la fornitura di risorse è disponibile quando CA Identity Manager viene integrato ad un server di fornitura.

Disattivazione dell'impostazione dell'opzione Applicare una volta

Se l'impostazione dell'opzione Applicare una volta non è attivata, le azioni di modifica associate al criterio di identità vengono applicate ogni volta che un criterio di identità viene valutato. Ciò significa che CA Identity Manager applica le azioni di modifica per ogni utente che soddisfa le condizioni definite nel criterio indipendentemente dal fatto che le azioni di modifica siano state precedentemente applicate.

In genere, l'impostazione dell'opzione Applicare una volta viene disattivata in un criterio di identità che applica la conformità. Ad esempio, è possibile creare un criterio di identità per limitare la capacità di spesa dei manager a € 5.000. Se CA Identity Manager rileva un manager con una capacità di spesa impostata su € 10.000, la reimposta automaticamente su € 5.000. Ogni volta che un manager viene sincronizzato in base al criterio di identità, CA Identity Manager verifica che la relativa capacità di spesa sia impostata correttamente.

Se ad un profilo utente viene apportata una modifica manuale che genera un conflitto con un'azione di modifica, CA Identity Manager sovrascrive la modifica quando l'utente viene sincronizzato in base al criterio.

Nell'esempio precedente, se qualcuno aumenta manualmente la capacità di spesa di un manager a € 10.000, CA Identity Manager la reimposta automaticamente su € 5.000 quando il manager viene sincronizzato in base al criterio.

Nella seguente tabella vengono elencati gli effetti dell'attivazione o disattivazione dell'impostazione dell'opzione Applicare una volta.

Se l'opzione Applicare una volta è...	Descrizione
Attivato	■ Le azioni di modifica associate al criterio di identità si verificano solo una volta ■ Le modifiche manuali apportate dopo avere applicato il criterio di identità vengono conservate ■ Gli aggiornamenti non vengono applicati agli utenti che soddisfano le condizioni di un criterio di identità se CA Identity Manager ha precedentemente applicato il criterio ■ Quando un utente non soddisfa più le condizioni definite in un criterio di identità, CA Identity Manager esegue le azioni di rimozione corrispondenti
Disabilitato	■ Le azioni di modifica associate al criterio di identità vengono applicate ogni volta che un utente viene sincronizzato in base al criterio ■ Le modifiche manuali vengono sovrascritte quando il criterio di identità viene applicato ■ Gli aggiornamenti al criterio vengono applicati quando un utente viene sincronizzato ■ Quando un utente non soddisfa più le condizioni definite in un criterio di identità, CA Identity Manager esegue le azioni di rimozione corrispondenti

Condizioni dei criteri

Le condizioni dei criteri sono le regole che determinano i gruppi di utenti a cui si applica un criterio di identità.

Nella tabella riportata di seguito vengono descritte le opzioni disponibili.

Sintassi	Condizione	Esempio
(all)	Il criterio di identità viene applicato a tutti gli utenti.	
dove <filtro utente>	L'utente deve soddisfare uno o più valori dell'attributo.	Utenti dove titolo=responsabile e località=est

Sintassi	Condizione	Esempio
in <regola organizzazione>	L'utente deve appartenere alle organizzazioni indicate. Nota: se si utilizza questa opzione, CA Identity Manager visualizza una nuova casella di riepilogo dove è possibile selezionare le seguenti opzioni: ■ organization <organizzazione> [and lower]: consente di utilizzare uno schermo di ricerca per le organizzazioni per cercare un'organizzazione e, facoltativamente, includere le corrispondenti organizzazioni secondarie. ■ Organizations where <filtro organizzazione> [and lower]: consente di specificare un filtro per selezionare una o più organizzazioni.	Utenti nell'organizzazione Vendite e inferiori
dove <filtro utente> e che sono in <regola organizzazione>	L'utente deve corrispondere ad attributi utente specifici, nonché appartenere ad un'organizzazione specifica.	title=manager and organization=Sales*
who are members of <regola membro gruppo>	L'utente deve appartenere a un gruppo che soddisfa una condizione specificata dagli attributi del gruppo. Nota: se si utilizza questa opzione, CA Identity Manager visualizza una nuova casella di riepilogo dove è possibile selezionare le seguenti opzioni: ■ gruppo <gruppo>: utilizzare uno schermo di ricerca dei gruppi per selezionare un gruppo. ■ group where <filtro gruppo>: consente di specificare un filtro che seleziona uno o più gruppi.	Gli utenti che sono membri di gruppi in cui titolare=CIO

Sintassi	Condizione	Esempio
membri di <regola di ruolo>	L'utente deve essere un membro di un ruolo. Il ruolo può essere: ■ un ruolo di accesso ■ un ruolo di amministrazione ■ un ruolo di fornitura Nota: per utilizzare i ruoli di fornitura, CA Identity Manager deve essere integrato con un server di fornitura. Per ulteriori informazioni, vedere la <i>Guida all'installazione</i>.	Utenti membri di ruolo Assistenza tecnica
amministratori di <regola di ruolo>	L'utente deve essere amministratore di un ruolo. Il ruolo può essere: ■ un ruolo di accesso ■ un ruolo di amministrazione ■ un ruolo di fornitura Nota: per utilizzare i ruoli di fornitura, CA Identity Manager deve essere integrato con un server di fornitura. Per ulteriori informazioni, vedere la <i>Guida all'installazione</i>.	Utenti amministratori di ruolo Responsabile vendite
titolari di <regola di ruolo>	L'utente deve essere titolare di un ruolo. Il ruolo può essere: ■ un ruolo di accesso ■ un ruolo di amministrazione ■ un ruolo di fornitura Nota: per utilizzare i ruoli di fornitura, CA Identity Manager deve essere integrato con un server di fornitura. Per ulteriori informazioni, vedere la <i>Guida all'installazione</i>.	Utenti titolari di ruolo Manager utente
returned by the query <query LDAP>	L'utente deve soddisfare una condizione basata su una query LDAP.	Utenti che soddisfano le condizioni di una query LDAP. Ad esempio (departmentNumber=Accounts)

Sintassi	Condizione	Esempio
in <administrative-union-constraint>	L'utente deve soddisfare almeno una delle condizioni incluse in un elenco di condizioni. In un vincolo di unione amministrativa è possibile includere i seguenti tipi di filtri: ■ Membro del ruolo di accesso/amministrazione/fornitura ■ Amministratore del ruolo di accesso/amministrazione/fornitura ■ Titolare del ruolo di accesso/amministrazione/fornitura ■ Membro di un gruppo	Utenti membri <i>oppure</i> titolari del ruolo Certifica manager.
in <vincolo intersezione amministrativa>	L'utente deve soddisfare tutte le condizioni incluse in un elenco di condizioni. In un vincolo di unione amministrativa è possibile includere i seguenti tipi di filtri: ■ Membro del ruolo di accesso/amministrazione/fornitura ■ Amministratore del ruolo di accesso/amministrazione/fornitura ■ Titolare del ruolo di accesso/amministrazione/fornitura ■ Membro di un gruppo	Utenti membri del ruolo Iniziatore contratto e del ruolo Approvatore contratto.

Azioni in caso di applicazione/rimozione dei criteri

È possibile definire le azioni di modifica che CA Identity Manager esegue nella valutazione del criterio di identità. Le opzioni possibili sono:

Azione su Applica criteri

Una serie di azioni eseguite da CA Identity Manager quando un utente soddisfa le condizioni definite dal criterio.

Azione su Rimuovi criteri

Una serie di azioni eseguite da CA Identity Manager quando un utente non soddisfa più le condizioni definite dal criterio.

Le azioni eseguite da CA Identity Manager quando i criteri di identità vengono applicati o rimossi sono uguali. Per ulteriori informazioni, vedere la seguente tabella.

Azione di modifica	Descrizione
Aggiungi al gruppo <nome gruppo>	Consente di aggiungere gli utenti ad un gruppo. Se si seleziona questa opzione, CA Identity Manager visualizza una schermata dove è possibile cercare il gruppo desiderato.
Aggiungi al gruppo <nome gruppo> nell'organizzazione dell'utente	Consente di aggiungere gli utenti ad un gruppo locale. Se si seleziona questa opzione, CA Identity Manager visualizza una casella di testo dove è possibile immettere il nome del gruppo desiderato.
Imposta <attributo utente di valore singolo> su <valore>	Consente di impostare il valore di un attributo in un profilo utente. Se esiste già un valore, CA Identity Manager lo sovrascrive con il valore specificato nell'azione di modifica.
Aggiungi <valore> a <attributo utente multivalore>	Consente di aggiungere un valore ad un attributo utente multivalore. Questa opzione non sovrascrive eventuali valori esistenti.
Rendi membro del ruolo di accesso	Consente di assegnare gli utenti ad un ruolo di accesso.
Rendi amministratore del ruolo di accesso	Consente di impostare gli utenti come amministratori di un ruolo di accesso
Rendi membro del ruolo di amministrazione	Consente di impostare gli utenti come membri di un ruolo di amministrazione
Rendi amministratore del ruolo di amministrazione	Consente di impostare gli utenti come amministratori di un ruolo di amministrazione
Rendi membro del ruolo di fornitura	Consente di impostare gli utenti come membri di un ruolo di fornitura, ruolo che crea account endpoint associati. Nota: per utilizzare i ruoli di fornitura, CA Identity Manager deve essere integrato con un server di fornitura. Per ulteriori informazioni, vedere la <i>Guida all'installazione</i> relativa al server delle applicazioni in uso.
Rendi amministratore del ruolo di fornitura	Consente di impostare gli utenti come amministratori di un ruolo di fornitura. Nota: per utilizzare i ruoli di fornitura, CA Identity Manager deve essere integrato con un server di fornitura. Per ulteriori informazioni, vedere la <i>Guida all'installazione</i> relativa al server delle applicazioni in uso.

Azione di modifica	Descrizione
Rimuovi dal gruppo <nome gruppo> [...]	Consente di rimuovere gli utenti da un gruppo. Se si seleziona questa opzione, CA Identity Manager visualizza una schermata dove è possibile cercare il gruppo desiderato.
Rimuovi dal gruppo <nome gruppo> nell'organizzazione dell'utente	Consente di rimuovere gli utenti da un gruppo locale. Se si seleziona questa opzione, CA Identity Manager visualizza una casella di testo dove è possibile immettere il nome del gruppo desiderato.
Rimuovi <valore> da <attributo utente multivalore>	Consente di rimuovere un valore da un attributo utente multivalore.
Rimuovi membro dal ruolo di accesso	Consente di revocare un ruolo di accesso.
Rimuovi amministratore dal ruolo di accesso	Consente di revocare i privilegi dell'amministratore per un ruolo di accesso specifico
Rimuovi membro dal ruolo di amministrazione	Consente di revocare un ruolo di amministrazione.
Rimuovi amministratore dal ruolo di amministrazione	Consente di revocare i privilegi dell'amministratore per un ruolo di amministrazione specifico
Rimuovi membro dal ruolo di fornitura	Consente di revocare un ruolo di fornitura.
Rimuovi amministratore dal ruolo di fornitura	Consente di revocare i privilegi dell'amministratore per un ruolo di fornitura specifico.
Invia messaggio di verifica	Consente di inviare il messaggio creato al database di verifica. È possibile che questo messaggio venga visualizzato in un rapporto precedentemente creato.
Violazione conformità	Consente di inviare il messaggio creato al database di verifica. Se viene creato un rapporto relativo alla conformità, il messaggio viene visualizzato ogni volta che il criterio di identità viene applicato/rimosso a/da un utente. Per ulteriori informazioni sulle procedure di controllo, vedere la <i>Guida alla configurazione</i> . Nota: è necessario selezionare la casella di controllo Compatibilità nella scheda Profilo affinché il set di criteri di identità sia in grado di utilizzare l'opzione Violazione conformità.

Azione di modifica	Descrizione
Accetta (Solo per le azioni di applicazione dei criteri)	Consente di inoltrare l'attività nel caso di una violazione dei criteri di identità preventivi. Se si seleziona questa azione, è necessario fornire un messaggio che CA Identity Manager scriverà nel database di verifica e verrà visualizzato in Visualizza attività inviate quando si verifica una violazione.
Rifiuta (Solo per le azioni di applicazione dei criteri)	Consente di impedire l'inoltro di un'attività quando si verifica una violazione dei criteri di identità. Questa azione viene utilizzata con i criteri di identità preventivi, per evitare che gli utenti ricevano privilegi che possono risultare in un conflitto di interessi o in una frode. Se si seleziona questa azione è necessario fornire un messaggio che verrà visualizzato in CA Identity Manager quando si verifica una violazione. Il messaggio viene archiviato nel database di verifica e visualizzato nella console utente.
Avviso (Solo per le azioni di applicazione dei criteri)	Consente di attivare un processo del flusso di lavoro quando si verifica una violazione dei criteri di identità preventivi, se si associa tale violazione ad un criterio di approvazione del flusso di lavoro. CA Identity Manager consente l'inoltro dell'attività indipendentemente dalla configurazione del flusso di lavoro. Nota: per informazioni sull'associazione di un processo del flusso di lavoro a un criterio di identità preventivo, vedere Flusso di lavoro e criteri di identità preventivi. (a pagina 488) Se si seleziona questa azione è necessario fornire un messaggio che verrà visualizzato in CA Identity Manager quando si verifica una violazione. Il messaggio viene archiviato nel database di verifica e visualizzato in Visualizza attività inviate.

Ulteriori informazioni:

[Criteri di identità preventivi](#) (a pagina 482)

[Flusso di lavoro e criteri di identità preventivi](#) (a pagina 488)

Definizione dei proprietari del set di criteri di identità

Nella scheda Proprietari definire le regole che determinano chi può essere il proprietario del set di criteri di identità. Un proprietario di un set di criteri di identità può modificare le informazioni di base relative al set di criteri, nonché aggiungere, modificare o rimuovere i criteri di identità all'interno del set.

Per completare la scheda Proprietari:

1. Definire le regole proprietari che determinano gli utenti che possono modificare il set di criteri di identità.
2. Fare clic su Inoltra.

Gestione di un set di criteri di identità

In CA Identity Manager sono disponibili le seguenti attività finalizzate alla gestione di un set di criteri di identità:

- Visualizza set di criteri di identità
- Modifica set di criteri di identità
- Elimina set di criteri di identità

Per impostazione predefinita, quando un amministratore utilizza una di queste attività, CA Identity Manager visualizza l'elenco di tutti i set di criteri di identità dei quali l'amministratore specifico è proprietario. A questo punto, l'amministratore può scegliere il set di criteri desiderato nell'elenco.

In un ambiente Identity Manager contenente più set di criteri di identità, è possibile personalizzare le attività Visualizza/Modifica/Elimina set di criteri di identità in modo da consentire agli amministratori di cercare un set di criteri specifico anziché visualizzarli tutti in un elenco.

Per personalizzare queste attività:

1. Nella console utente, selezionare Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.

Viene visualizzato la schermata Modifica attività di amministrazione.

2. Cercare e selezionare l'attività che si desidera personalizzare.
3. Nella scheda Ambito selezionare Tutti i set dei criteri di identità.

Se si seleziona questa opzione, CA Identity Manager utilizza la definizione della schermata Ricerca predefinita set di criteri di identità.

4. Fare clic su Invia.

Modalità di sincronizzazione di utenti e criteri di identità

Quando vengono utilizzati i criteri di identità, è importante comprendere in che modo i criteri vengono valutati e applicati agli utenti in CA Identity Manager. Senza una corretta comprensione del processo di sincronizzazione degli utenti, c'è il rischio di configurare set di criteri di identità che restituiscono risultati imprevisti.

La procedura seguente descrive la valutazione e l'applicazione dei criteri di identità in CA Identity Manager:

1. Il processo di sincronizzazione degli utenti viene avviato:
 - **Automaticamente:** è possibile configurare le attività di CA Identity Manager in modo che attivino automaticamente la sincronizzazione degli utenti.
 - **Manualmente:** utilizzare l'attività Sincronizza utente nella console utente per sincronizzare un utente.
2. CA Identity Manager determina il set di criteri di identità che si applicano ad un utente.
3. Il set di criteri viene quindi confrontato con l'elenco di criteri già applicati a tale utente.

Nota: l'elenco di criteri applicati ad un utente è archiviato nell'attributo %IDENTITY_POLICY% nel profilo utente. Per ulteriori informazioni sulla configurazione di questo attributo, consultare la *Guida alla configurazione*.

- Se un criterio di identità è presente nell'elenco di criteri applicabili e *non* è stato applicato precedentemente all'utente, tale criterio viene aggiunto a un elenco di assegnazione.
 - Se un criterio di identità si trova nell'elenco di criteri applicabili, è stato precedentemente applicato all'utente e l'impostazione Applicare una volta per il criterio è disattivata, tale criterio viene aggiunto a un elenco di riallocazione.
 - Se un criterio di identità non è presente nell'elenco di criteri applicabili, è stato applicato all'utente e l'utente non soddisfa più la condizione prevista, tale criterio viene aggiunto a un elenco di annullamento assegnazione.
4. Dopo la valutazione di tutti i criteri per un utente, questi vengono applicati nell'ordine seguente:
 - a. Criteri di identità dall'elenco di annullamento assegnazione
 - b. Criteri di identità dall'elenco di assegnazione
 - c. Criteri di identità dall'elenco di riassegnazione

5. Una volta applicati, i criteri di identità vengono rivalutati per controllare se è necessario applicare ulteriori modifiche in base alle modifiche già apportate nel primo processo di sincronizzazione (passaggi 2-4).

Tale operazione serve a garantire che le modifiche apportate applicando i criteri di identità non attivino altri criteri di identità.

6. La valutazione e l'applicazione dei criteri di identità continuano finché l'utente non viene sincronizzato in base a tutti i criteri applicabili oppure finché in CA Identity Manager non viene raggiunto il livello massimo di ricorrenza, definito nella console di gestione.

Ad esempio, con un criterio di identità il dipartimento di un utente potrebbe essere modificato quando all'utente viene assegnato un ruolo. Il nuovo dipartimento attiva un altro criterio di identità. Tuttavia, se il livello di ricorrenza è impostato a 1, la modifica successiva non viene apportata fino alla nuova sincronizzazione dell'utente.

Per ulteriori informazioni sull'impostazione del livello di ricorrenza, consultare la Guida in linea della console di gestione.

Configurazione della sincronizzazione automatica degli utenti

CA Identity Manager è in grado di sincronizzare automaticamente gli account utente con i criteri di identità in diversi punti durante il ciclo di vita di un'attività.

Un'attività di CA Identity Manager genera *eventi*, ovvero attività rilevabili che si verificano durante l'elaborazione dell'attività. Ad esempio, l'attività predefinita Crea utente genera gli eventi CreateUserEvent, AddUserToGroupEvent e AssignAccessRoleEvent. È possibile configurare CA Identity Manager in modo che gli utenti vengano sincronizzati al completamento di un'attività oppure al completamento di ogni evento.

Nota: nella sezione [Sincronizzazione degli utenti in base ai criteri di identità](#) (a pagina 472) sono riportate ulteriori informazioni sul processo di sincronizzazione degli utenti.

Per configurare un'attività in modo che attivi la sincronizzazione degli utenti

1. Accedere a CA Identity Manager con un account utente autorizzato a modificare le attività di amministrazione.
2. Fare clic su Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.

Viene visualizzato una schermata di ricerca.
3. Cercare e selezionare l'attività di amministrazione che attiverà la sincronizzazione degli utenti.

4. Selezionare una delle seguenti opzioni nel campo Sincronizzazione utente della scheda Profilo associata all'attività:
- **Disattivato:** l'attività non attiverà la sincronizzazione degli utenti.
 - **Al completamento dell'attività:** il processo di sincronizzazione degli utenti viene avviato al completamento di tutti gli eventi. Questa impostazione rappresenta l'opzione di sincronizzazione predefinita per le attività Crea utente, Modifica utente ed Elimina utente. L'impostazione predefinita per tutte le altre attività è Disattivato.

Nota: se si seleziona l'opzione Al completamento dell'attività per un'attività che include più eventi, gli utenti non vengono sincronizzati finché tutti gli eventi nell'attività non sono stati completati. Se uno o più di tali eventi richiedono l'approvazione del flusso di lavoro, tale processo potrebbe impiegare diversi giorni. Per evitare che venga atteso il completamento degli eventi per applicare i criteri di identità, selezionare l'opzione A ogni evento.
 - **A ogni evento:** il processo di sincronizzazione degli utenti viene avviato non appena viene completato ogni singolo evento di un'attività.

Per attività con un evento primario ed un evento secondario per lo stesso utente, l'impostazione del processo di sincronizzazione su A ogni evento potrebbe comportare un maggior numero di valutazioni dei criteri validi per un utente rispetto alla selezione dell'opzione Al completamento dell'attività.

Sincronizzazione manuale degli utenti

È possibile scegliere di eseguire una sincronizzazione manuale degli utenti in base ad un set di criteri di identità per garantire che i vari account utente dispongano dei privilegi adeguati o che siano conformi ad un determinato criterio.

È possibile sincronizzare manualmente un utente mediante l'attività Sincronizza utente disponibile nella console utente di CA Identity Manager.

Nota: per il corretto funzionamento di tale attività, l'opzione Sincronizzazione utente deve essere impostata su Disattivato, mentre l'opzione Sincronizzazione account deve essere impostata su Al completamento dell'attività o su A ogni evento. Per ottimizzare le prestazioni, scegliere l'opzione Al completamento dell'attività. Tali opzioni sono impostate nella scheda Profilo per l'attività Sincronizza utente.

L'attività Sincronizza utente contiene le schede seguenti:

- **Criteri attualmente corrispondenti:** in questa scheda viene visualizzato l'elenco dei criteri di identità che verranno applicati all'utente quando l'attività Sincronizza utente verrà inoltrata.

Nota: nella scheda Criteri attualmente corrispondenti vengono visualizzati solo i criteri di identità validi per l'utente al momento dell'accesso all'attività Sincronizza utente. Quando l'utente viene sincronizzato in base a tali criteri, è possibile che vengano apportate modifiche che attivano altri criteri di identità. Per impedire che vengano applicati i nuovi criteri prima che siano stati verificati, impostare il livello di ricorsione per i set di criteri di identità su 1 nella console di gestione di CA Identity Manager. Dopo aver inoltrato l'attività Sincronizza utente, accedervi nuovamente per rivedere i criteri.

- **Criteri già applicati:** in questa scheda viene visualizzato l'elenco dei criteri già applicati all'utente.
- **Riepilogo sincronizzazione:** in questa scheda vengono visualizzati tutti i criteri di identità validi per l'utente, nonché le azioni di modifica associate a tali criteri.

Per sincronizzare un account utente

1. Accedere ad Identity Manager come utente in grado di utilizzare l'attività Sincronizza utente. Per impostazione predefinita, gli utenti con il ruolo Gestore sistema possono utilizzare questa attività.
2. Selezionare Criteri, Sincronizza utente.
Viene aperta l'attività Sincronizza utente.
3. Selezionare la scheda Riepilogo sincronizzazione.
4. Rivedere i criteri e le azioni associate che verranno applicati all'utente, quindi fare clic su Inoltra.

Verifica della sincronizzazione degli utenti

Per verificare che le modifiche appropriate siano state apportate quando un utente viene sincronizzato in base ai criteri di identità, selezionare la scheda Criteri già applicati nell'attività Sincronizza utente.

1. Accedere a CA Identity Manager con un account utente autorizzato a utilizzare l'attività Sincronizza utente. Per impostazione predefinita, gli utenti con il ruolo Gestore sistema possono utilizzare questa attività.
2. Selezionare Criteri, Sincronizza utente.
Viene aperta l'attività Sincronizza utente.
3. Selezionare la scheda Criteri già applicati.
4. Rivedere i criteri e le azioni associate applicati da CA Identity Manager all'utente.

Set di criteri di identità in un ambiente Identity Manager

Nelle sezioni seguenti vengono descritte varie modalità di utilizzo dei criteri di identità:

- [Esempio: Inserimento automatico di valori negli attributi utente](#) (a pagina 477)
- [Esempio: Allocazione di risorse ed assegnazioni dei diritti](#) (a pagina 478)
- [Esempio: Applicazione della conformità](#) (a pagina 479)
- [Esempio: Applicazione dell'imposizione di mansioni](#) (a pagina 480)

Esempio: Inserimento automatico di valori negli attributi utente

È possibile utilizzare un set di criteri di identità per assegnare automaticamente i valori degli attributi utente in base al valore di un altro attributo o ad un'assegnazione di diritti utente diversa. Ad esempio, è possibile creare un set di criteri di identità che compili automaticamente l'indirizzo postale di un utente in base all'ufficio in cui lavora.

Per configurare un set di criteri di identità per gli indirizzi dei dipendenti, creare un criterio di identità con le impostazioni seguenti per l'ubicazione di ogni ufficio.

Impostazione	Valore
Condizione criteri	office = <ubicazione ufficio>
Azione su Applica criteri	set Street Address = <indirizzo> set City = <città> Set State/Province = <stato o provincia> Set Postal Code = <codice postale>

Nella figura seguente sono illustrati alcuni criteri di esempio nel set di criteri di identità Indirizzi dipendenti.

Criteri di identità

Set di criteri

	Nome criterio	Regola membri del criterio	Azione su Applica criteri
	Boston	in cui (Office = "Boston")	Imposta Address su 121 strada Imposta City su Boston Imposta State su MA Imposta Postal code su 02451
	NY	in cui (Office = "NY")	Imposta Address su 106 strada Imposta City su NY Imposta State su NY Imposta Postal code su 10017

Esempio: Allocazione di risorse ed assegnazione dei diritti

I criteri di identità consentono di assegnare automaticamente risorse, ad esempio account di dominio, oppure assegnare diritti specifici, ad esempio rendere un utente membro di un ruolo, quando gli utenti soddisfano le condizioni definite da un criterio specifico. Ad esempio, è possibile creare un set di criteri di identità per assegnare risorse e ruoli in base al titolo di un utente.

Per creare un set di criteri di identità per assegnare risorse e ruoli, creare un criterio di identità contenente le impostazioni seguenti per ogni titolo presente nell'organizzazione.

Impostazione	Valore
Condizione criteri	title = <titolo>

Impostazione	Valore
Azione su Applica criteri	Qualsiasi azione di assegnazione di risorse o diritti agli utenti che soddisfano le condizioni definite dal criterio, ad esempio: ■ rendi membro di <gruppo> ■ rendi membro del ruolo di amministrazione <ruolo di amministrazione> ■ rendi membro del ruolo di fornitura <ruolo di fornitura>
Azione su Rimuovi criteri	Qualsiasi azione finalizzata alla rimozione di risorse o diritti quando un utente non soddisfa più le condizioni definite dal criterio. Ad esempio, se in Identity Manager un utente è stato impostato come membro di un ruolo al momento dell'applicazione del criterio di identità, è possibile configurare Identity Manager in modo che tale ruolo venga revocato quando l'utente non soddisfa più le condizioni definite dal criterio stesso.

Nella figura seguente sono illustrati alcuni criteri di esempio nel set di criteri di identità Risorse dipendenti.

Criteri di identità

Set di criteri

	Nome criterio	Regola membri del criterio	Azione su Applica criteri	Azione su Rimuovi criteri
	Managers	in cui (Title = "Managers")	Rendi membro del ruolo di amministrazione UM Rendi membro del ruolo di provisioning UP	Rimuovi membro dal ruolo di amministrazione UM
	HR	in cui (Title = "HR")	Rendi membro del ruolo di amministrazione UM Aggiungi al gruppo UG Rendi membro del ruolo di provisioning UP	Rimuovi dal gruppo UG Rimuovi membro dal ruolo di amministrazione UM Rimuovi membro dal ruolo di provisioning UP

Esempio: Applicazione della conformità

È possibile configurare i criteri di identità per definire le condizioni che devono esistere o meno, nonché per eseguire determinate azioni in base alla valutazione di tali condizioni. Ad esempio, è possibile definire un criterio di compatibilità che imposti un limite di spesa pari a € 5.000 per i responsabili. Se un responsabile dispone di un limite di spesa pari a € 10.000, in CA Identity Manager è possibile reimpostare tale limite e registrare una violazione della conformità a fini di controllo.

Per creare un set di criteri di conformità per applicare i limiti di spesa, creare un criterio di identità contenente le impostazioni seguenti.

Impostazione	Valore
Applicare una volta	Non attivato
Conformità	Attivato
Condizione criteri	Qualsiasi condizione che definisca la conformità o una violazione della conformità, ad esempio: title=<titolo> AND Spending Limit > <limite di spesa>
Azione su Applica criteri	Azioni da eseguire in CA Identity Manager quando la condizione definita dal criterio è valida, ad esempio: ■ Messaggio di violazione compatibilità: Limite di spesa superato ■ Imposta limite di spesa su <valore>

Nella figura seguente è illustrato il criterio di conformità descritto nell'esempio precedente.

Criteri di identità

Set di criteri

	Nome criterio	Regola membri del criterio	Azione su Applica criteri
	Manager	in cui (Title = "Manager" e Spending Limit > "5000")	Messaggio di violazione conformità: limite spendendo superare i 5000

Esempio: Applicazione dell'imposizione di mansioni

I criteri di identità consentono la definizione di ruoli che si escludono reciprocamente e che non è possibile concedere simultaneamente allo stesso utente. Ad esempio, è possibile impedire ad un gestore di utenti che è in grado di concedere aumenti di essere anche un approvatore di stipendi.

Per creare un set di criteri di identità per applicare l'imposizione delle mansioni, creare un criterio di identità contenente le impostazioni seguenti.

Impostazione	Valore
Applicare una volta	Non attivato
Conformità	Attivato
Condizione criteri	Utilizzare l'opzione "in <vincolo intersezione amministrativa>" per definire un insieme di condizioni che violano un criterio aziendale. Se un utente soddisfa tutte le condizioni, in Identity Manager vengono eseguite le azioni incluse nel campo Azione su Applica criteri. Ad esempio, impostare la condizione del criterio nel modo seguente: intersezione (membri di <ruolo>) e che sono membri di <altro ruolo>)
Azione su Applica criteri	Azioni da eseguire in Identity Manager quando la condizione definita dal criterio è valida, ad esempio: ■ Messaggio di violazione compatibilità: Utente con ruoli che si escludono a vicenda ■ Rimuovi membro da <ruolo>

Nella figura seguente è illustrato il criterio di identità descritto nell'esempio precedente.

Criteri di identità

Set di criteri

	Nome criterio	Regola membri del criterio	Azione su Applica criteri
	Restrizione	intersezione (membri di (ruolo di amministrazione "Manager utente") e membri di (ruolo di amministrazione "Richiedente utente"))	Messaggio di violazione conformità: utente dispone dei diritti escludono a vicenda Rimuovi membro dal ruolo di amministrazione Richiedente utente

Criteri di identità preventivi

Un *criterio di identità preventivo* è un tipo di criterio di identità che impedisce che gli utenti ricevano privilegi che possono risultare in un conflitto di interessi o in una frode. Questi criteri soddisfano i requisiti SOD aziendali.

I criteri di identità preventivi, che vengono eseguiti prima dell'inoltro di un'attività, consentono all'amministratore di verificare la presenza di violazioni dei criteri prima di assegnare privilegi o modificare attributi del profilo. Se esiste una violazione, l'amministratore potrà cancellarla prima di inoltrare l'attività.

Ad esempio, una società può creare un criterio di identità preventivo che proibisce che gli utenti con il ruolo Manager utente dispongano anche del ruolo Responsabile dell'approvazione utente. Se un amministratore utilizza l'attività Modifica utente per assegnare a un Manager utente il ruolo di Responsabile dell'approvazione utente, in CA Identity Manager viene visualizzato un messaggio relativo alla violazione. L'amministratore può modificare le assegnazioni di ruolo per cancellare la violazione prima di inoltrare l'attività.

È possibile creare criteri di identità preventivi per le seguenti modifiche:

- **Appartenenza a ruolo**

Impedisce che gli utenti possano disporre di determinati ruoli nello stesso tempo.

Ad esempio, gli utenti non possono disporre contemporaneamente dei ruoli Manager utente e Responsabile dell'approvazione utente.

- **Amministratori di ruolo**

Impedisce che gli utenti possano essere amministratori di determinati ruoli se sono amministratori di altri ruoli.

Ad esempio, gli utenti non possono essere contemporaneamente amministratori dei ruoli Manager utente e Responsabile dell'approvazione utente.

- **Attributi utente**

Impedisce che gli utenti possano avere determinati attributi di profilo nello stesso tempo.

Ad esempio, gli utenti non possono avere il titolo di Contabile senior ed appartenere al dipartimento IT.

- **Attributi organizzazione**

Impedisce la creazione di profili utente in una determinata organizzazione.

Ad esempio, gli amministratori non possono creare profili di dipendenti nell'organizzazione Fornitori.

■ Attributi gruppo

Impedisce agli utenti di essere membri di determinati gruppi.

Ad esempio, gli utenti non possono essere membri del gruppo Team di progetto e del gruppo Contabilità.

Ulteriori informazioni:

[Azioni per le violazioni dei criteri di identità preventivi](#) (a pagina 483)

Azioni per le violazioni dei criteri di identità preventivi

Se ad una modifica aziendale si applica un criterio di identità preventivo, vengono eseguite azioni specifiche per risolvere la violazione.

Quando si specifica una di queste azioni all'interno di un criterio di identità, è necessario specificare un messaggio di descrizione della violazione. Il messaggio verrà registrato nel database di verifica. In base al tipo di azione, il messaggio può inoltre essere visualizzato agli utenti nella console utente e registrato in Visualizza attività inviate.

È possibile configurare le seguenti azioni per un criterio di identità preventivo:

Accetta

CA Identity Manager visualizza in Visualizza attività inviate un messaggio che descrive la violazione, ma consente l'inoltro dell'attività.

Rifiuta

CA Identity Manager visualizza un messaggio nella console utente ed impedisce l'inoltro dell'attività.

Avviso

CA Identity Manager visualizza un messaggio nella console utente ed in Visualizza attività inviate. Facoltativamente, questa azione può attivare un processo del flusso di lavoro che richiede l'approvazione da parte di un utente appropriato prima dell'effettiva esecuzione dell'attività.

Per attivare un processo del flusso di lavoro, si [associa il criterio di identità preventivo ad un processo del flusso di lavoro basato su criterio](#) (a pagina 489) nelle attività che possono provocare la violazione.

Se ad esempio la violazione si verifica quando un utente riceve determinati ruoli nello stesso tempo, configurare il processo del flusso di lavoro per tutte le attività che assegnano tali ruoli agli utenti.

Nota: quando si configura il processo del flusso di lavoro basato su criterio per l'attività, la regola di approvazione deve fare riferimento al nome del criterio di identità preventivo.

Funzionamento dei criteri di identità preventivi

L'esempio di processo seguente illustra il funzionamento dei criteri di identità preventivi:

1. Un amministratore dei criteri di identità crea un criterio di identità preventivo che proibisce che gli utenti che dispongono del titolo di Contabile senior appartengano al dipartimento IT.

Durante la definizione del criterio di identità, l'amministratore specifica che CA Identity Manager deve rifiutare qualsiasi modifica che comporti una violazione di questo criterio.

2. Un amministratore delle Risorse umane utilizza l'attività Crea utente per creare il profilo utente di un nuovo Contabile senior. L'amministratore delle Risorse umane seleziona correttamente il titolo dell'utente, ma per errore seleziona il dipartimento IT.
3. L'amministratore delle Risorse umane completa i campi rimanenti nell'attività Crea utente e fa clic su Inoltra.
4. CA Identity Manager rileva che l'attività comporta modifiche che sono definite in un criterio di identità e valuta le modifiche per rilevare eventuali violazioni.
5. Quando la violazione viene rilevata, l'inoltro dell'attività viene impedito e l'amministratore delle Risorse umane riceve un messaggio di avviso.
Il messaggio viene inoltre registrato nel database di verifica.
6. L'amministratore delle Risorse umane visualizza i dettagli sulla violazione nel messaggio e modifica il dipartimento dell'utente in Finanza, quindi inoltra nuovamente l'attività.
7. CA Identity Manager valuta la modifica proposta rispetto a tutti i criteri di identità applicabili, quindi consente l'inoltro dell'attività Crea utente.

Note importanti sui criteri di identità preventivi

Prima di implementare criteri di identità preventivi, considerare quanto segue:

- I criteri di identità preventivi prevengono solo le violazioni che verrebbero generate per effetto di modifiche proposte nell'attività corrente. Non impediscono le violazioni esistenti.

Ad esempio, una società crea un criterio di identità preventivo che proibisce che gli utenti dispongano contemporaneamente dei ruoli Manager utente e Responsabile dell'approvazione utente. Un amministratore assegna il ruolo di Manager gruppi ad un utente già titolare dei ruoli Manager utente e Responsabile dell'approvazione utente. CA Identity Manager consente l'esecuzione della nuova assegnazione, in quanto la modifica non è la causa diretta di una violazione del criterio.

- Se ad un set di modifiche proposte si applicano più criteri di identità preventivi, CA Identity Manager applica per primi i criteri con azioni di tipo Rifiuta.
- Non specificare gruppi dinamici nelle condizioni dei criteri di identità preventivi. Le condizioni dei criteri determinano il set di utenti ai quali si applica il criterio di identità preventivo.

Ad esempio, una società dispone di un gruppo dinamico che include tutti gli utenti il cui titolo è Manager. La società crea inoltre un criterio di identità preventivo che proibisce che i membri del gruppo Manager abbiano il ruolo Appaltatori.

Un amministratore modifica il titolo di un utente titolare del ruolo Appaltatori in Manager. Questa modifica renderà l'utente membro del gruppo Manager *dopo* il corretto inoltro dell'attività. Nel momento in cui il criterio viene valutato tuttavia, il titolo dell'utente non è Manager, dunque non vengono rilevate violazioni.

- Il filtro titolare di ruolo e il filtro query LDAP non sono supportati nelle condizioni per i criteri di identità preventivi.

Creazione di un criterio di identità preventivo

Prima di creare un criterio di identità preventivo, è necessario creare un set di criteri di identità, ovvero un raggruppamento logico di una serie di criteri di identità.

Nota: prima di iniziare, consultare la sezione [Note importanti sui criteri di identità preventivi](#) (a pagina 485).

Per creare un set di criteri di identità preventivi

1. Aprire Criteri, Crea set di criteri di identità nella console utente.
Creare un nuovo set di criteri di identità oppure utilizzarne uno esistente come modello.
2. [Definire il profilo per il set di criteri di identità](#) (a pagina 461) nella scheda Profilo.
3. [Creare una regola membri del set di criteri](#) (a pagina 462) nella scheda Criteri.
4. Creare un criterio di identità preventivo come descritto di seguito:
 - a. Fare clic su Aggiungi.
 - b. Immettere il nome da assegnare al criterio di identità.
Nota: le impostazioni Applicare una volta e Conformità non si applicano ai criteri di identità preventivi.
 - c. Identificare gli utenti ai quali applicare il criterio nella sezione Condizione criteri.
Nota: il filtro titolare di ruolo e il filtro query LDAP non sono supportati per i criteri di identità preventivi.
 - d. Nel campo Azione su Applica criteri, specificare le azioni eseguite da CA Identity Manager quando viene rilevata una violazione dei criteri:

Accetta

CA Identity Manager visualizza in Visualizza attività inviate un messaggio che descrive la violazione, ma consente l'inoltro dell'attività.

Rifiuta

CA Identity Manager visualizza un messaggio nella console utente ed impedisce l'inoltro dell'attività.

Avviso

CA Identity Manager visualizza un messaggio nella console utente ed in Visualizza attività inviate. Facoltativamente, questa azione può [attivare un processo del flusso di lavoro](#) (a pagina 488).

Quando si seleziona una di queste azioni, in CA Identity Manager viene visualizzata una casella di testo in cui è possibile specificare il messaggio da visualizzare quando si verifica una violazione.

- e. Specificare il messaggio nella console utente.

Nota: se si localizza la console utente, è possibile specificare nel campo del messaggio una chiave della risorsa invece che un testo. Per ulteriori informazioni sulle chiavi delle risorse, consultare la *User Console Design Guide*.

- f. Aggiungere ulteriori azioni se necessarie, quindi fare clic su OK.

5. [Specificare i titolari del set di criteri di identità](#) (a pagina 471).

Nota: prima di utilizzare il set di criteri di identità creato, verificare che i criteri di identità siano abilitati nella console di gestione. Per ulteriori informazioni, vedere la *Configuration Guide*.

Use Case: Impedire i conflitti di ruoli per gli utenti

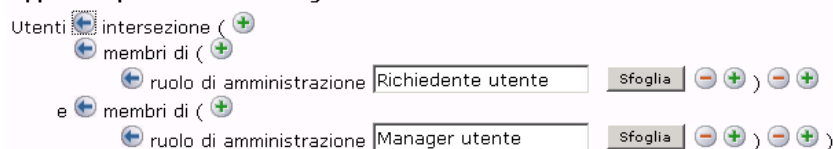
Forward, Inc. desidera impedire che i dipendenti dispongano contemporaneamente dei ruoli Manager utente e Responsabile dell'approvazione utente. I dipendenti titolari di entrambi i ruoli sono in grado di modificare attributi utente come lo stipendio e di approvarli, pertanto questa situazione non è appropriata.

Per impedire che si verifichi questo tipo di situazione, Forward, Inc. crea un criterio di identità preventivo applicato agli utenti con i ruoli Manager utente e Responsabile dell'approvazione utente. Se un amministratore tenta di assegnare tali ruoli ad un utente, l'inoltro dell'attività viene rifiutato e viene visualizzato un messaggio che descrive la violazione.

Per creare un criterio di identità preventivo a supporto di questo Use Case, procedere come segue:

- Creare un set di criteri di identità per il criterio da creare.
- Creare un criterio di identità preventivo con le seguenti impostazioni:
 - Condizione criteri:

Applicare questo criterio ai seguenti utenti:



- Azione su Applica criteri:
 - Rifiuta con messaggio: L'utente non può essere membro dei ruoli Manager utente e Responsabile dell'approvazione utente

Flusso di lavoro e criteri di identità preventivi

Quando un criterio di identità preventivo è configurato in modo da generare un avviso, è possibile definire un processo del flusso di lavoro basato su criterio del livello attività, che viene associato al criterio di identità, per le attività che potrebbero attivare una violazione. Se ad esempio un criterio di identità proibisce che i Contabili senior siano membri del dipartimento IT, è possibile definire un processo del flusso di lavoro basato su criterio del livello attività sulle attività Crea utente e Modifica utente.

Tutti gli elementi di lavoro generati per effetto del flusso di lavoro basato su criterio del livello attività devono essere approvati prima dell'esecuzione dell'attività. Nella console utente dei responsabili dell'approvazione viene visualizzato un elemento di lavoro. Quando il responsabile dell'approvazione fa clic su tale elemento di lavoro viene visualizzata un'attività di approvazione, che include il messaggio di avviso che descrive la violazione. Il responsabile dell'approvazione può scegliere di approvare o rifiutare l'attività, in base alla violazione.

I processi del flusso di lavoro basato su criterio vengono associati ai criteri di identità preventivi in base al nome del criterio.

Ulteriori informazioni:

[Flusso di lavoro basato su criterio](#) (a pagina 319)

Violazione di criteri di identità nelle attività di approvazione

Quando un criterio di identità preventivo è associato a un processo del flusso di lavoro per un'attività, in CA Identity Manager viene generato un elemento dell'elenco di lavoro per i responsabili dell'approvazione appropriati. I responsabili dell'approvazione utilizzano un'attività di approvazione per approvare o rifiutare la modifica che ha attivato la violazione dei criteri.

L'attività di approvazione predefinita contiene una sezione in cui sono elencate le violazioni dei criteri di identità. Se le modifiche proposte attivano più criteri di identità preventivi, è possibile che l'elenco contenga più violazioni.

Le violazioni possono presentare i seguenti stati:

- **Pending Evaluation (In attesa di valutazione)**

La valutazione delle regole di approvazione per l'attività non è ancora iniziata. Questo è lo stato iniziale.

- **In attesa di approvazione**

È stata individuata una corrispondenza per il criterio di identità definito nelle regole di approvazione ed è stato attivato il processo del flusso di lavoro associato.

- **Approvato**

Un responsabile dell'approvazione ha approvato le modifiche proposte. Le modifiche che hanno attivato le violazioni dei criteri di identità preventivi vengono applicate.

- **Rifiutato**

Un responsabile dell'approvazione ha rifiutato la modifica proposta. L'attività viene rifiutata.

- **Nessun flusso di lavoro configurato**

Per la violazione non è configurato alcun processo del flusso di lavoro. L'attività viene eseguita senza bisogno dell'approvazione.

Configurazione del flusso di lavoro per i criteri di identità preventivi

Il flusso di lavoro per i criteri di identità preventivi va configurato nelle attività di amministrazione che includono modifiche che potrebbero attivare una violazione dei criteri di identità.

Ad esempio, se il criterio di identità preventivo proibisce che gli utenti dispongano di determinati ruoli amministrativi allo stesso tempo, configurare le attività che assegnano ruoli amministrazione per il supporto del flusso di lavoro per i criteri di identità preventivi.

Nota: prima di configurare il flusso di lavoro, creare un criterio di identità preventivo con le seguenti impostazioni:

- Un nome di criterio univoco

Il nome del criterio deve essere univoco all'interno di tutti i set di criteri di identità, in quanto i processi del flusso di lavoro sono associati ai criteri di identità preventivi in base al nome.

Se esistono più criteri di identità preventivi con lo stesso nome, possono essere applicabili più processi del flusso di lavoro.

- Avviso nel campo Azione su Applica criteri

L'avviso è l'unica azione che può attivare un processo del flusso di lavoro.

Dopo aver configurato il criterio di identità preventivo, determinare le attività che possono attivare la violazione del criterio. Quindi, [creare un criterio di approvazione del flusso di lavoro](#) (a pagina 490) per tali attività.

Creazione di un criterio di approvazione del flusso di lavoro per i criteri di identità preventivi

È possibile configurare a livello di attività un processo del flusso di lavoro basato su criterio per un'attività amministrativa. Tale processo del flusso di lavoro includerà uno o più criteri di approvazione che possono associare un criterio di identità preventivo ad un flusso di lavoro. Il flusso di lavoro viene eseguito quando si verifica una violazione del criterio di identità preventivo associato.

Nota: per ulteriori informazioni sui processi del flusso di lavoro basati su criterio a livello di attività, vedere [Flusso di lavoro basato su criterio](#) (a pagina 319).

Per creare un criterio di approvazione del flusso di lavoro per i criteri di identità preventivi

1. Modificare l'attività di amministrazione che consente di apportare modifiche che potrebbero attivare la violazione di un criterio di identità preventivo.

Ad esempio, se si verifica la violazione di un criterio di identità in quanto un utente dispone dei ruoli Manager utente e Responsabile dell'approvazione utente, modificare l'attività di amministrazione che consente agli amministratori di assegnare ruoli, ad esempio Crea utente, Modifica utente e Modifica membri/amministratori del ruolo di amministrazione.
2. Fare clic sull'icona di modifica accanto al campo Processo del flusso di lavoro nella scheda Profilo dell'attività, per aggiungere un processo del flusso di lavoro.

Verrà visualizzata la schermata Configurazione del flusso di lavoro del livello attività.
3. Selezionare il flusso di lavoro basato su criterio, quindi fare clic su Aggiungi.
4. Nella sezione Regola di approvazione, selezionare l'oggetto Violazione criteri di identità.
5. Nel campo Criteri di identità, selezionare un filtro per specificare quali criteri di identità attivano il flusso di lavoro associato al criterio di approvazione.

Includere nel filtro il nome del criterio di identità, *non* il nome del set di criteri di identità.
6. Configurare i campi Valutazione regola, Ordine criterio e Descrizione criterio secondo le necessità.
7. Selezionare un processo del flusso di lavoro e fare clic su OK.

Quando si seleziona un processo del flusso di lavoro, in CA Identity Manager vengono visualizzati ulteriori campi.
8. Specificare le attività di approvazione e i responsabili dell'approvazione secondo le necessità.

Il processo del flusso di lavoro viene associato al criterio di identità preventivo.

Use Case: Approvazione di titoli

Forward, Inc utilizza un criterio aziendale che stabilisce che tutti i manager devono essere dipendenti a tempo pieno. Di recente tuttavia, la società ha assunto numerosi appaltatori per progetti speciali. Per consentire l'esecuzione efficiente dei progetti speciali, ad alcuni appaltatori verrà assegnato il titolo di Manager. Forward, Inc desidera che venga richiesta l'approvazione da parte del direttore del dipartimento Risorse umane prima di consentire agli amministratori di assegnare il titolo di Manager ad un appaltatore.

Per automatizzare il processo di approvazione in queste circostanze, Forward, Inc crea un criterio di identità preventivo denominato Titoli Manager per appaltatori, che rileva i casi in cui il titolo di utente è Manager e l'organizzazione dell'utente è Appaltatore. Forward, Inc configura inoltre un processo di approvazione basato su criterio per l'attività Modifica utente. Tale processo di approvazione viene attivato quando viene violato il criterio Titoli Manager per appaltatori.

Quando un amministratore modifica il titolo di un appaltatore in Manager, CA Identity Manager visualizza un messaggio di avviso e invia un elemento di lavoro al direttore del dipartimento Risorse umane per l'approvazione. Il titolo dell'appaltatore non viene modificato finché l'elemento di lavoro non viene approvato.

Per configurare il supporto per questo Use Case, è necessario completare le seguenti operazioni in CA Identity Manager:

- Creare un criterio di identità preventivo denominato Titoli Manager per appaltatori con le seguenti impostazioni:
 - Condizione criteri: Utenti dove (Titolo = "Manager" e Organizzazione = "Appaltatore")
 - Azione su Applica criteri: Avviso con messaggio "I Manager devono essere dipendenti a tempo pieno"
- Modificare l'attività Modifica utente in modo da includere un processo del flusso di lavoro con le seguenti impostazioni:
 - Processo del flusso di lavoro: Basato su criteri
 - Oggetto regola di approvazione: Violazione criteri di identità
 - Criteri di identità: dove (Nome = "Titolo Manager per appaltatori")
 - Processo del flusso di lavoro: SingleStepApproval

Combinazione di criteri di identità e criteri di identità preventivi

È possibile combinare criteri di identità e criteri di identità preventivi per soddisfare i requisiti SOD (Segregation of Duties). In questo caso, i criteri di identità elaborano le violazioni SOD esistenti e i criteri di identità preventivi impediscono le nuove violazioni.

Per supportare questo Use Case, è necessario configurare un set di criteri di identità con due tipi di azioni:

- Azioni che si verificano durante la sincronizzazione

Queste azioni determinano la modifica di attributi utente, membri di gruppi e ruoli, amministratori o titolari. Ad esempio, un'azione di questo tipo può rimuovere un utente da un ruolo se viene rilevata una violazione.

Queste azioni differiscono dalle azioni preventive per il fatto che non vengono applicate al momento dell'inoltro di un'attività, ma solo durante la [sincronizzazione utente](#) (a pagina 472).

- Azioni preventive

Queste azioni determinano il comportamento di CA Identity Manager quando si verifica una violazione dei criteri di identità preventivi *prima* dell'inoltro di un'attività. CA Identity Manager può consentire l'inoltro dell'attività, generare un avviso e attivare un processo del flusso di lavoro, oppure impedire l'inoltro dell'attività.

In tutti i casi, la violazione viene registrata nel database di verifica.

Si prenda ad esempio una società che desidera impedire che gli utenti dispongano contemporaneamente dei ruoli Amministratore delle Risorse umane e Approvatore stipendi. La società crea quindi un criterio di identità con due azioni di tipo Azione su Applica criteri:

- Rimuovere l'utente dal ruolo Approvatore stipendi

Questa azione ha luogo quando viene eseguita la sincronizzazione degli utenti con i criteri di identità.

In questo caso, la società ha configurato la sincronizzazione utente per l'attività Modifica utente. Se un amministratore modifica un utente, CA Identity Manager valuta tutti i criteri di identità applicabili ed applica le azioni. In questo esempio, CA Identity Manager rimuove gli utenti che hanno il ruolo Amministratore delle Risorse umane e il ruolo Approvatore stipendi dal ruolo Approvatore stipendi.

- Rifiutare l'attività

Questa azione preventiva impedisce agli amministratori di assegnare questi due ruoli ad un solo utente non consentendo l'inoltro dell'attività.

Nota: quando si configura un criterio di identità con entrambi questi tipi di azione, verificare che le azioni non siano in conflitto. Ad esempio, è possibile configurare un criterio di identità che impedisca agli utenti di disporre dei ruoli di Manager e Appaltatore. In questo criterio si specificano due azioni:

- Un avviso che attiva un processo del flusso di lavoro, che richiede un'approvazione prima dell'assegnazione dei ruoli, e
- Un'azione che rimuove un utente dal ruolo Manager

Un responsabile dell'approvazione approva l'assegnazione di ruolo per i ruoli Manager e Appaltatore, ma la seconda azione rimuove l'utente dal ruolo Manager quando viene eseguita la sincronizzazione utente.

Capitolo 15: Policy XPress

Questa sezione contiene i seguenti argomenti:

[Panoramica di Policy Xpress](#) (a pagina 495)

[Creazione di un criterio](#) (a pagina 496)

Panoramica di Policy Xpress

Policy Xpress consente di creare complesse logiche aziendali (criteri) in CA Identity Manager senza dover disporre di un codice personalizzato. Tuttavia, i concetti implicati nella creazione di criteri di Policy Xpress sono complessi e richiedono una considerazione e una pianificazione attente. Gli amministratori che utilizzano le schermate del portale di CA Identity Manager possono configurare un criterio in Policy Xpress per implementare anche la più sofisticata logica aziendale necessaria. Quando i criteri aziendali subiscono modifiche, un amministratore può cambiare i criteri mediante schermate di configurazione in CA Identity Manager senza richiedere allo sviluppatore di modificare il codice alla base o, cosa più importante, senza riavviare i servizi di CA Identity Manager (adottando le corrette procedure di gestione delle modifiche).

Nota: per ulteriori informazioni su Policy Xpress, consultare la pagina [Wiki di Policy Xpress](#).

Creazione di un criterio

Per creare un criterio in Policy Xpress, definire gli elementi di base del criterio seguenti.

Profilo

Consente di definire il tipo e la priorità del criterio, nonché di raggruppare criteri simili, per una maggiore semplicità di gestione.

Eventi

Consente di definire quando eseguire il criterio.

Nota: il parametro Eventi va impostato con attenzione. La logica aziendale deve essere eseguita in momenti specifici per evitare il danneggiamento dei dati e aumentare le prestazioni. Ad esempio, l'impostazione di un utente come attivo va eseguita al momento della creazione dell'utente. L'esecuzione di tale logica in qualsiasi momento può provocare la riattivazione di utenti che dovrebbero restare disabilitati. Un altro esempio può essere quello di assegnare all'utente un ruolo di fornitura che concede accesso a un determinato sistema. Questo ruolo va assegnato all'utente solo dopo l'assegnazione e l'approvazione di un ruolo diverso. Policy Xpress consente l'attivazione della logica aziendale durante l'elaborazione dell'evento e del gestore dell'attività di logica aziendale, in modo analogo alle schede personalizzate. Pertanto, a differenza dei criteri di identità, la logica può essere attivata in qualsiasi momento e non solo all'inizio di un'attività.

Dati (Elementi dati)

Consentono di specificare i dati utilizzati dal criterio. Per ogni tipo di logica aziendale è necessario specificare i dati da utilizzare. I dati possono essere utilizzati per prendere decisioni, oppure per costruire dati più complessi. In Policy Xpress sono disponibili numerosi componenti individuali per la raccolta dei dati. Tali componenti sono denominati *Elementi dati*. Un esempio di elemento dati è il valore di un attributo utente. Ad esempio, Policy Xpress può determinare il nome dell'utente e archiviarlo come elemento dati per l'utilizzo successivo.

Regole di ingresso

Consentono di specificare i requisiti da soddisfare prima dell'esecuzione. La definizione delle regole di ingresso consente di specificare il momento in cui Policy Xpress deve valutare i criteri. In questo modo è possibile semplificare i criteri stessi e migliorare le prestazioni. Un esempio di regola di ingresso è l'esecuzione di un criterio "Imposta nome completo" *solo* se il nome o il cognome sono stati modificati.

Regole azione

Consentono di definire l'azione da intraprendere in base alle informazioni raccolte. Ad esempio, Policy Xpress può assegnare un utente a ruoli diversi, oppure specificare valori account diversi in base al nome del dipartimento dell'utente.

Azioni

Consentono di specificare l'azione da eseguire. Al termine del processo, Policy Xpress esegue le azioni richieste dalla logica aziendale. In Policy Xpress, una regola di azione è associata a più azioni, in modo che quando la regola viene soddisfatta, le azioni vengono eseguite. Le azioni possono comprendere l'assegnazione di valori di attributo a un utente o un account, l'esecuzione di una riga di comando o di un comando SQL, oppure la generazione di un nuovo evento.

Profilo

La scheda Profilo di un criterio di Policy Xpress contiene campi che consentono di gestire i criteri e perfezionarne le funzionalità.

Nota: un criterio si applica solo all'ambiente in cui è stato creato. Se ad esempio si crea un criterio mentre si è connessi all'ambiente neteauto, il criterio viene eseguito solo per tale ambiente.

Per la creazione di un criterio è necessario inserire le informazioni di profilo seguenti:

Nome criterio

Consente di definire un nome descrittivo univoco per il criterio.

Tipo criterio

Consente di definire i [listener](#) (a pagina 499) che attivano il criterio. Ogni tipo di criterio è caratterizzato da una configurazione diversa.

Nota: non è possibile modificare questo campo dopo il salvataggio del criterio.

Categoria

Consente di definire un gruppo di criteri correlati. Questo campo consente di raggruppare i criteri per una maggiore semplicità di gestione.

Descrizione

Consente di specificare una descrizione del criterio.

Priorità

Se esistono più criteri da eseguire per un singolo evento, in questo campo è possibile specificare quando deve essere eseguito il criterio. I criteri vengono eseguiti in base alla priorità. Più basso è il valore, più alta è la priorità (la priorità 1 viene eseguita per prima, la priorità 10 per seconda, la priorità 50 per terza e così via).

L'impostazione della priorità è utile per i criteri che dipendono l'uno dall'altro, oppure per suddividere un criterio complesso in due criteri semplici che verranno eseguiti in sequenza.

Si supponga ad esempio che esistano tre criteri che vengono eseguiti se nel database è presente un valore specifico. Invece di lasciare che i tre criteri verifichino singolarmente il valore nel database, è possibile creare un quarto criterio da eseguire per primo, che verifica il valore. Se il nuovo criterio corrisponde al valore richiesto, Policy Xpress è quindi in grado di impostare una variabile. Gli altri tre criteri vengono eseguiti solo se viene impostata tale variabile, evitando accessi ridondanti al database.

Attivato

Consente di specificare se il criterio è attivo in CA Identity Manager. Deselezionare questa casella di controllo se si desidera disattivare un criterio senza eliminarlo.

Esegui una volta

Consente di specificare che il criterio deve essere eseguito una sola volta. Può essere necessario eseguire alcuni criteri ogni volta che vengono soddisfatte le condizioni specificate, mentre per altri è necessaria una sola esecuzione. Questo valore determina se le regole di azione che sono già state eseguite in passato vanno eseguite nuovamente.

Ad esempio, l'aggiunta di un ruolo SAP a un utente in base al dipartimento è un'azione che va eseguita solo la prima volta che viene rilevata la corrispondenza tra utente e dipartimento. Al contrario, un criterio che imposta il livello di stipendio dell'utente in base alla qualifica *non* andrebbe impostato per l'esecuzione singola, per assicurarsi che non vengano apportate modifiche non autorizzate.

Nota: l'opzione Esecuzione singola si applica a un oggetto e non a livello globale.

Listener

I criteri di Policy Xpress vengono attivati quando accade qualcosa nel sistema. Per implementare questa funzionalità, i listener integrati nel sistema notificano a Policy Xpress che si è verificato un evento e forniscono i relativi dettagli.

Sono disponibili i listener seguenti:

Evento

Resta in ascolto in attesa di qualsiasi evento nel sistema e di tutti gli stati associati all'evento (prima, approvato, rifiutato e così via). Questo listener segnala inoltre il nome dell'evento a Policy Xpress. Per il listener di eventi sono disponibili gli stati seguenti:

- Prima
- Rifiutato
- Approvato
- Dopo
- Non riuscito

UI

Resta in ascolto in attesa di diverse attività in esecuzione nel sistema durante lo stato sincronizzato, ossia quando è ancora aperta l'interfaccia utente per l'attività. Per il listener UI sono disponibili gli stati seguenti:

- Inizio - all'avvio dell'attività
- Imposta soggetto - quando viene individuato l'oggetto primario
- [Convalida la modifica](#) (a pagina 500) - quando viene modificato un attributo impostato con il flag Convalida la modifica
- Convalida all'invio - quando si fa clic sul pulsante di invio
- Invio - quando l'attività viene inviata

Flusso di lavoro

Resta in ascolto in attesa di processi del flusso di lavoro che hanno individuato responsabili dell'approvazione. Questo listener è utile per l'esecuzione di logica basata sui responsabili dell'approvazione, ad esempio l'invio di un messaggio di posta elettronica al responsabile dell'approvazione.

Attività inviata

Resta in ascolto in attesa di attività inviate non in esecuzione in background. È simile al listener di eventi, ma considera l'attività nel suo complesso, invece degli eventi dell'attività. Per il listener delle attività inviate sono disponibili gli stati seguenti:

- Inizio attività
- Attività completata
- Attività non riuscita

Sincronizzazione inversa

Resta in ascolto in attesa di notifiche nel sistema correlate alla funzionalità di esplorazione di CA Identity Manager.

Convalida dell'attributo sullo schermo

Oltre che dei trigger definiti (tipi di criterio), Policy Xpress può restare in ascolto della convalida degli attributi. Ciò consente di creare criteri che vengono eseguiti quando un attributo su schermo contrassegnato con il flag "Convalida la modifica" viene aggiornato.

È possibile utilizzare questa funzionalità per creare elenchi a discesa dipendenti. Se ad esempio sullo schermo sono presenti due elenchi a discesa, Policy Xpress va in esecuzione quando viene selezionato il primo elenco a discesa, quindi vengono impostati i valori per il secondo elenco a discesa in base all'opzione selezionata nel primo. È possibile eseguire l'aggiornamento di un numero illimitato di elenchi a discesa e altre schermate. La differenza rispetto all'opzione Dati casella di selezione è che questa funzionalità consente di popolare le opzioni degli elenchi a discesa utilizzando qualsiasi logica, invece che semplicemente importando un file XML di opzioni statiche.

Un altro possibile utilizzo è quello di popolare altri attributi in base al valore di un attributo. Ad esempio, quando un amministratore seleziona un dipartimento, Policy Xpress può popolare automaticamente altri attributi, quali manager del dipartimento, numero del dipartimento e codice HR del dipartimento. In questo modo si elimina la necessità di scrivere il codice personalizzato di un gestore attributo logico.

Per configurare la convalida con un criterio di Policy Xpress

1. Nella console utente, modificare lo schermo di profilo di un'attività e selezionare il campo di cui si desidera restare in ascolto.
2. Accedere alle proprietà del campo e selezionare Sì nell'elenco a discesa per Convalida la modifica.
3. In Policy Xpress, creare un criterio di tipo "[UI](#) (a pagina 499)".
4. Nella scheda Esegui per eventi, selezionare lo stato "Convalida la modifica" e l'attività modificata al passaggio 1.

Use Case: verifica dei nomi offensivi

Quando viene creato un nuovo utente, può essere utile verificare che il nome scelto non sia offensivo. La procedura seguente illustra come verificare che i nomi utente non siano offensivi utilizzando un criterio di Policy Xpress.

1. Verificare che i campi appropriati nello schermo di profilo dell'attività Crea utente siano impostati su Convalida la modifica = Sì.
2. In Policy Xpress, creare un criterio di tipo "UI".
3. Nella scheda Esegui per eventi selezionare lo stato "Convalida la modifica" e l'attività Crea utente.
4. Creare gli elementi dati seguenti per verificare il nome:
 - Ottenere l'attributo Nome (Attributi, Attributo utente, Ottieni)
 - Analizzare il nome in lettere minuscole (Generale, Analisi stringa, In minuscola)
 - Confrontare il nome con un elenco di parole offensive in una tabella di database (Origini di dati, Dati query SQL).
5. Creare elementi dati analoghi come nel passaggio 4 per verificare il cognome.
6. Creare una regola di azione come segue:
 - Condizione - il nome è diverso da "" (si verifica se la query restituisce il messaggio che il nome è offensivo)
 - Azione - messaggio visualizzato (Messaggi, On screen message (Messaggio su schermo)) che indica il nome offensivo.

Questa regola obbligherà l'utente a modificare il nome prima di ripetere l'invio dell'attività Crea utente.

7. Creare una regola di azione analoga come nel passaggio 6 per il cognome.

Eventi

A seconda del tipo di criterio selezionato nella scheda Profilo, è possibile configurare orari di attivazione per stabilire quando deve essere valutato il criterio. Ad esempio, un criterio di tipo Evento può essere impostato per la valutazione prima di un evento CreateUserEvent. Un criterio di tipo Attività può essere impostato per la valutazione al momento dell'impostazione del soggetto per l'evento DisableUserEvent.

Per configurare un orario di attivazione, selezionare i campi seguenti:

Stato

Consente di specificare l'intervallo di tempo o l'azione correlata all'evento che attiva il criterio. Ad esempio, è possibile impostare un criterio per l'esecuzione "Prima" che si verifichi un evento.

Nome evento

Consente di specificare l'evento che attiva il criterio, ad esempio CreateUserEvent.

Un criterio può disporre di più orari di attivazione. Ogni volta che nel sistema si verifica un orario di attivazione specificato (uno stato e un evento), Policy Xpress cerca tutti i criteri con tale orario di attivazione e li valuta in base all'ordine.

Nota: anche se un criterio corrisponde a un orario di attivazione che si verifica nel sistema, ciò non vuol dire che il criterio viene automaticamente eseguito. L'effettivo completamento del criterio viene determinato dai criteri relativi alle regole valutati successivamente nel processo.

Elementi dati

Gli elementi dati vengono utilizzati per la creazione dei dati dei criteri. Un criterio può contenere più elementi dati che rappresentano le informazioni utilizzate dal criterio.

Per la raccolta delle informazioni relative agli elementi dati, Policy Xpress utilizza plug-in flessibili. Ogni plug-in può eseguire una piccola attività dedicata. È tuttavia possibile utilizzare più plug-in per costruire criteri più complessi. Un esempio di plug-in elemento dati è un elemento attributo utente. Lo scopo dell'elemento è quello di raccogliere informazioni su un determinato attributo che fa parte del profilo dell'utente.

Gli elementi dati vengono calcolati nel momento in cui vengono chiamati, ovvero quando una regola sta utilizzando l'elemento dati, oppure quando un altro elemento che ha bisogno del calcolo sta utilizzando l'elemento dati come parametro. Ad esempio, un elemento dati query SQL può recuperare un valore da una tabella, ma per creare la query ha bisogno del dipartimento dell'utente. In questo caso, l'elemento dati dipartimento deve essere eseguito prima dell'elemento dati query SQL, quindi il [valore può essere utilizzato come parametro](#) (a pagina 505).

I campi seguenti consentono di definire un elemento dati:

Nome

Consente di definire un nome descrittivo per l'elemento dati. Alcuni elementi sono complessi (ad esempio quelli che comportano il recupero di variabili o di informazioni dal database). Per semplificare la gestione dell'elemento dati, è consigliabile selezionare un nome significativo.

Categoria

Contiene un raggruppamento di elementi dati. Questo campo consente di ordinare gli elementi dati e ne semplifica la selezione.

Tipo

Consente di specificare il tipo di elemento dati. Ogni tipo ha un utilizzo dedicato. Questo campo è basato sulla categoria selezionata.

Funzione

Consente di definire le possibili variazioni degli stessi dati. La maggior parte degli elementi dati supporta solo la funzione Ottieni.

Ad esempio, per l'elemento dati attributo utente sono disponibili le funzioni seguenti:

- Ottieni - restituisce i valori dell'attributo
- Presenta valori multipli - il valore restituito è "true" se il valore presenta valori multipli
- È un attributo logico - il valore restituito è "true" se il valore è logico

Descrizione della funzione

Contiene una descrizione prepopolata della funzione. Per ogni funzione selezionata è disponibile una descrizione diversa per facilitare la comprensione dell'utilizzo e dei valori previsti.

Parametri

Consente di definire i parametri passati all'elemento dati. Gli elementi dati sono dinamici, quindi possono comportarsi in modo diverso in base ai parametri. Un elemento dati attributo utente restituisce risultati diversi in base all'attributo selezionato. L'opzione relativa al tipo secondario consente inoltre di definire il numero di parametri, i relativi nomi e i valori opzionali eventualmente disponibili.

È possibile aggiungere ulteriori parametri, se necessario. L'esempio di query SQL accetta due parametri obbligatori, l'origine dati e la query stessa. Nella query è possibile utilizzare il segnaposto "?", che andrà sostituito con valori (in modo simile a un'istruzione preparata). L'aggiunta di ulteriori parametri consente di impostare tali valori.

Nota: nella visualizzazione degli elementi dati in Policy Xpress è presente una colonna denominata "In Uso". Un segno di spunta in questa colonna indica che l'elemento dati è utilizzato da una regola o un parametro di azione, o come parametro per altri elementi dati.

Utilizzo di valori dinamici in elementi dati o azioni

I valori dinamici sono il risultato di elementi dati calcolati e i relativi valori vengono decisi solo in fase di esecuzione. Tali valori possono quindi essere utilizzati come parametri per altri elementi dati (che vengono calcolati successivamente, in base alla priorità).

Per utilizzare un valore dinamico come parametro per un elemento dati

1. Nella scheda Dati criterio, individuare il parametro in cui si desidera impostare un valore dinamico.
2. Nel campo di testo vuoto, immettere un testo normale o selezionare il valore dinamico dall'elenco a discesa di destra.
3. Fare clic su OK.

Variabili

In Policy Xpress sono disponibili variabili che vengono impostate con azioni e salvate come elementi dati (categoria Variabili). Le variabili sono condivise tra tutti i criteri in esecuzione nello stesso momento, pertanto una variabile impostata può essere utilizzata da altri criteri di priorità inferiore.

Ad esempio, una variabile può contenere un valore calcolato una volta da un criterio e quindi condiviso tra altri criteri che non avranno bisogno di ricalcolare tale valore. Il criterio iniziale imposta un valore per la variabile e i criteri che vengono eseguiti successivamente leggono tale valore utilizzando un elemento dati che ha come parametro il nome della variabile.

Una variabile può inoltre fungere da trigger per altri criteri. In questo caso, i criteri vengono eseguiti solo se è stato eseguito il criterio ad essi precedente.

Regole di ingresso

Le regole di ingresso definiscono le condizioni per l'esecuzione di un criterio. Tali condizioni utilizzano i valori raccolti dagli elementi dati nel criterio.

Un criterio può contenere più regole di ingresso e una regola di ingresso può contenere più condizioni. È necessario che venga soddisfatta almeno una regola di ingresso, vale a dire che *tutte* le condizioni nella regola di ingresso devono essere soddisfatte perché il criterio passi alle regole di azione.

I campi seguenti consentono di definire una regola di ingresso:

Nome

Consente di specificare un nome descrittivo per la regola di ingresso.

Descrizione

Consente di specificare il significato della regola di ingresso.

Condizioni

Consente di specificare i criteri da soddisfare.

Nota: nelle regole di ingresso, tra le condizioni è sempre presente un operatore AND.

Ulteriori informazioni:

[Condizioni](#) (a pagina 506)

Condizioni

Le condizioni vengono utilizzate nelle regole di ingresso e di azione e comprendono i componenti seguenti:

- Dati criterio
- Operatore
- Valore

Si supponga ad esempio di voler creare una condizione che verifica se il dipartimento di un utente è stato modificato. Definire innanzitutto un elemento dati Dipartimento modificato, quindi, nella condizione, selezionare l'elemento dati Dipartimento modificato, impostare l'operatore Uguale a e impostare il valore su True.

Ulteriori informazioni:

[Regole di ingresso](#) (a pagina 505)

[Regole azione](#) (a pagina 506)

Regole azione

Le regole di azione sono analoghe alle regole di ingresso nella struttura, ma ne differiscono nelle funzionalità. Le regole di azione definiscono il momento in cui eseguire un'azione. Se ad esempio si desidera che un criterio esegua un'azione quando il dipartimento di un utente viene modificato in Vendite, creare una regola di azione che indica quando "Dipartimento = Vendite".

Inoltre, invece di dover soddisfare la corrispondenza con una regola di ingresso, è possibile soddisfare la corrispondenza con più regole di azione. La regola di azione con la priorità più alta (il valore più alto è 0) è l'unica che viene utilizzata.

Le regole di azione contengono inoltre una o più azioni, che sono suddivise in azioni di aggiunta e azioni di rimozione.

I campi seguenti consentono di definire una regola di azione:

Nome

Consente di specificare un nome descrittivo per la regola di azione. Il nome deve essere univoco.

Descrizione

Consente di specificare il significato della regola di azione.

Condizioni

Consente di specificare i criteri da soddisfare.

Priorità

Consente di specificare la regola di azione eseguita, nel caso in cui esista una corrispondenza per più regole di azione. Questo campo risulta utile per definire le azioni predefinite. Se ad esempio si dispone di più regole, ognuna per uno specifico nome di dipartimento, è possibile impostare un'azione predefinita aggiungendo un'ulteriore regola senza condizioni, ma con priorità più bassa (ad esempio 10 se tutte le altre hanno priorità 5). Se non esiste una corrispondenza per nessuna delle regole del dipartimento, viene utilizzata l'azione predefinita.

Aggiungi azioni

Consente di selezionare da un elenco l'azione da intraprendere quando la regola viene soddisfatta. Ad esempio, è possibile configurare una regola che indica che se il dipartimento dell'utente corrisponde a quello configurato nella condizione, è necessario aggiungere uno specifico gruppo di Active Directory. Le regole di azione si comportano in modo diverso, in base all'impostazione dell'opzione Esecuzione singola. Se il criterio è impostato per l'esecuzione singola, le azioni associate vengono eseguite la prima volta che viene rilevata una corrispondenza per la regola. L'azione non viene ripetuta quando vengono rilevate corrispondenze successive. Nell'esempio precedente, il gruppo di Active Directory viene aggiunto all'utente una sola volta. Se l'opzione Esecuzione singola non è impostata, le azioni vengono ripetute finché la regola continua ad essere soddisfatta. Questo campo è importante per l'applicazione di valori.

Rimuovi azioni

Consente di selezionare da un elenco l'azione da eseguire quando la regola non è più soddisfatta. Nell'esempio precedente, all'utente viene aggiunto un gruppo di Active Directory in base al dipartimento di appartenenza. Se il dipartimento viene modificato, l'azione consente di rimuovere il gruppo di Active Directory.

Ulteriori informazioni:

[Condizioni](#) (a pagina 506)

Azioni

Le azioni eseguono la logica aziendale dopo la conclusione di tutti i processi decisionali e funzionano in modo analogo agli elementi dati, tranne che nella parte finale. Le azioni infatti eseguono un'attività, invece di restituire un valore.

Nota: le azioni vengono eseguite nell'ordine in cui sono visualizzate nella console utente.

I campi seguenti consentono di definire un'azione:

Nome azione

Consente di definire lo scopo dell'azione.

Categoria

Contiene un raggruppamento di azioni. Questo campo consente di ordinare le azioni e ne semplifica la selezione.

Tipo e Funzione

Consentono di definire il tipo e la funzione dell'azione intrapresa.

Nota: per ulteriori informazioni su Tipo e Funzione, vedere Dati.

Descrizione della funzione

Contiene una descrizione prepopolata della funzione. Per ogni funzione selezionata è disponibile una descrizione diversa per facilitare la comprensione dell'utilizzo e dei valori previsti.

Parametri

Consente di definire i parametri passati all'azione.

Controllo di flusso

Per impostazione predefinita, i criteri vengono ordinati per priorità e quindi valutati uno alla volta. Sebbene questo flusso sia applicabile quasi sempre, se necessario è possibile modificarlo.

La funzionalità di modifica del flusso è rappresentata da un'azione che è possibile associare a qualsiasi regola di azione. Le funzioni di modifica del flusso sono disponibili nella categoria Sistema dell'azione.

Importante: modificare i flussi di processo con estrema cautela. L'utilizzo di queste azioni può risultare in un ciclo infinito. Se ad esempio si imposta "Ripeti criterio corrente" in una regola di azione senza impostare condizioni, la regola risulterà sempre vera e il criterio verrà riavviato di continuo, senza fine.

È possibile utilizzare le quattro funzioni di modifica del flusso seguenti:

Arresta elaborazione

Selezionando questa opzione, tutti i criteri successivi al criterio corrente vengono ignorati e Policy Xpress viene chiuso.

Nota: viene chiuso solo Policy Xpress. Se si desidera forzare anche l'arresto di CA Identity Manager, è possibile utilizzare il plug-in di azione di tipo Eccezione.

Riavvia tutti i criteri

Selezionando questa opzione, l'elaborazione dei criteri viene interrotta e riparte dall'inizio dell'elenco. Questa opzione risulta utile nei casi in cui l'azione di un criterio fa in modo che un altro criterio, che è stato avviato prima di questo e non è stato eseguito, soddisfi ora i criteri di ingresso. Tale criterio viene quindi rivalutato.

Ripeti criterio corrente

Selezionando questa opzione, il criterio selezionato viene eseguito nuovamente. Questa opzione risulta utile per l'iterazione. Ad esempio, per la creazione di un nome utente univoco è necessaria l'esecuzione ripetuta di un criterio finché non viene individuato un nome univoco.

Va a un criterio specifico

Per questa azione è necessario selezionare un criterio esistente. Se tale criterio è in esecuzione nello stesso momento del criterio corrente (può avvenire in un momento precedente o successivo), Policy Xpress passa al criterio selezionato. Se il nuovo criterio è di priorità inferiore, tutti i criteri tra il criterio corrente e il criterio selezionato vengono ignorati. Se il nuovo criterio è di priorità superiore, il processo va indietro.

Nota: poiché con questa azione è possibile che alcuni criteri vengano ignorati, è opportuno utilizzarla con cautela.

Impostazione di oggetti associati agli account

Quando si crea un'azione di aggiunta per impostare un oggetto associato ad un account, ad esempio Membro di, per rappresentare l'oggetto viene utilizzato un formato di relazione specifico. In CA Identity Manager possono rappresentare l'oggetto i due tipi di formato seguenti:

- Per rappresentare relazioni semplici tra l'oggetto e l'account, ad esempio gruppi Active Directory:
`NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- Per rappresentare relazioni di associazione tra l'oggetto e l'account, ad esempio ruoli SAP:
`{"validFromDate":"2009\12\01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,Endpoint=sap_endpoint,Namespace=SAPR3,Domain=im,Server=Server","validToDate":"2009\12\31"}`

Una relazione di associazione è diversa da una relazione semplice per il fatto che l'associazione tra l'oggetto e l'account contiene dati aggiuntivi. Nell'esempio precedente, i parametri `validFromDate` e `validToDate` contengono solo dati relativi all'associazione tra l'account ed il ruolo SAP. I dati `validFromDate` e `validToDate` non esistono nell'account o nell'oggetto ruolo.

Per distinguere il formato per la relazione, creare un elemento dati che ottenga il valore dell'oggetto. Il valore restituito è il formato da utilizzare nell'azione di aggiunta per impostare l'oggetto.

Esempio: gruppi Active Directory

1. Creare un criterio di Policy Xpress con le impostazioni seguenti:
 - Tipo di criterio: Evento
 - Eventi: Dopo – Modifica utente
2. Nella regola di azione, configurare l'azione di aggiunta seguente:
 - Categoria: Attributi
 - Tipo: Imposta dati account
 - Funzione: Imposta
 - Tipo endpoint: Active Directory
 - Endpoint: *nome_endpoint*
 - Nome account: *account*
 - Attributo: Membro di (appartenenza al gruppo)
 - Valore:
`NativeGroup=Administrators,Container=Builtin,Endpoint=nome_endpoint,Namespace=ActiveDirectory,Domain=im,Server=Server`

Avanzate

Policy Xpress consente di apportare molte variazioni alla configurazione e può interagire con componenti esterni. Questa flessibilità può provocare errori non necessariamente legati a problemi del programma, ad esempio la configurazione errata di un'origine dati, la restituzione di un valore mancante da un elemento dati dinamico, oppure la mancata risposta di un endpoint.

Quando si verifica un errore, in genere il sistema interrompe il calcolo dei criteri per l'operazione corrente. È tuttavia possibile modificare la risposta predefinita agli errori, in base alla categoria dell'errore. Se ad esempio è presente un criterio non critico, è possibile definire che in caso di errore l'elaborazione continui.

Le risposte predefinite agli errori possono essere modificate nella scheda Avanzate.

Nota: si consiglia di non modificare le impostazioni predefinite di risposta agli errori, tuttavia, nei casi di utilizzo avanzati è possibile modificare tali impostazioni per criterio. Se ad esempio è presente un criterio non critico, è possibile specificare che l'elaborazione continui anche se il criterio non è riuscito.

Nella scheda è possibile configurare le categorie di errore seguenti:

- Convalida - si verifica quando a un plug-in vengono fornite informazioni errate. Questo tipo di errore viene segnalato prima che venga tentata l'azione.
- Ambiente - è provocato da problemi nell'ambiente, ad esempio il mancato funzionamento di un server di database per il plug-in SQL.
- Allowed (Consentito) - un errore non critico. Il comportamento predefinito per questo tipo di errore prevede il proseguimento dell'elaborazione della richiesta, come ad esempio quando l'invio di un messaggio di posta elettronica fallisce.

Per ognuno degli errori precedenti è possibile impostare le opzioni seguenti:

- Evento non riuscito - l'azione corrente viene interrotta. Si tratta dell'impostazione predefinita per la maggior parte dei tipi di errore.
- Criterio non riuscito - il criterio corrente e tutte le azioni ad esso associate vengono interrotti. L'elaborazione del resto dei criteri continua.
- Ignora - gli errori vengono registrati senza interrompere le azioni o i criteri.

Capitolo 16: Applicazione mobile CA Identity Manager

L'applicazione mobile CA Identity Manager sfrutta l'infrastruttura di CA Identity Manager esistente per consentire agli utenti di completare le attività seguenti su una periferica mobile, come ad esempio uno smartphone o un tablet:

- Ripristinare una password dimenticata
- Modificare una password
- Rispondere alle richieste di approvazione mediante accettazione o rifiuto. Utilizzare la console utente per prenotare o rilasciare una richiesta.
- Visualizzazione delle informazioni utente

Questa funzionalità consente agli utenti di visualizzare le informazioni sugli altri utenti dell'organizzazione. Ad esempio, i responsabili dell'approvazione degli elementi di lavoro possono visualizzare le informazioni di base relative a un manager di un utente, quali nome e indirizzo, prima della decisione di approvazione. Se sono necessarie ulteriori informazioni, il responsabile dell'approvazione può selezionare un collegamento per visualizzare il profilo completo.

Questa sezione contiene i seguenti argomenti:

[L'architettura dell'applicazione mobile di CA Identity Manager](#) (a pagina 514)

[Funzionamento del processo di implementazione](#) (a pagina 517)

[Funzionamento della configurazione dell'applicazione](#) (a pagina 518)

[Funzionamento della registrazione utenti](#) (a pagina 519)

[Configurazione di CA Identity Manager per il supporto dell'applicazione mobile](#) (a pagina 519)

[Configurazione di un'applicazione mobile](#) (a pagina 529)

[Configurare delle proprietà aggiuntive](#) (a pagina 532)

[Download dell'applicazione mobile](#) (a pagina 534)

[Risoluzione dei problemi delle applicazioni mobili](#) (a pagina 535)

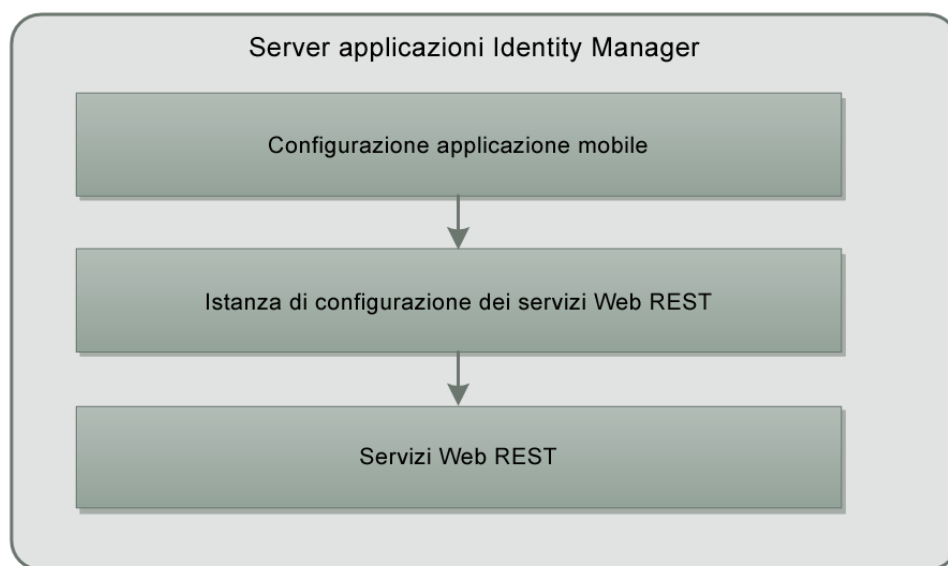
L'architettura dell'applicazione mobile di CA Identity Manager

L'architettura dell'applicazione mobile di CA Identity Manager è progettata per fornire un insieme di funzionalità di CA Identity Manager per diversi dispositivi mobili, come smartphone e tablet. Le funzionalità selezionate per l'applicazione mobile si basano su esigenze di business critiche e per le interazioni utente appropriate per dispositivi di piccole dimensioni.

L'architettura si basa sull'utilizzo di un componente di configurazione specifico per l'applicazione e per i servizi Web RESTful per le funzionalità server di CA Identity Manager. Il Server CA Identity Manager supporta la funzionalità di gestione di configurazione di una determinata applicazione mobile dell'ambiente e di configurazione dei servizi Web REST utilizzati dell'applicazione.

Nota: i servizi Web REST sono specifici dell'applicazione mobile di CA Identity Manager e pertanto non costituiscono API pubblici, a differenza dei TEWS (Task Execution Web Service) basati su SOAP.

I servizi Web REST supportano più configurazioni per l'ambiente CA Identity Manager. Ogni configurazione è solitamente associata a un determinato client REST, come ad esempio l'applicazione mobile. L'architettura di livello elevato e la relazione tra la configurazione dell'applicazione mobile e quella dei servizi Web viene riportata di seguito:



La configurazione di servizi Web REST richiede la selezione di un set specifico di opzioni per il funzionamento dell'applicazione mobile. Prima di creare la configurazione dell'applicazione mobile, è necessario definire una configurazione del servizio Web mediante l'attività di configurazione del servizio Web. Tale attività è disponibile anche dalle Attività di amministrazione.

Dettagli di configurazione del servizio Web delle applicazioni mobili

Una configurazione del servizio Web REST è composta dai seguenti elementi:

- Un profilo che definisce un nome di configurazione univoco, l'identificatore corrispondente e il flag abilitato
- Una configurazione di protezione che definisce l'uso di SSL, della crittografia di payload e della chiave di crittografia.
- L'insieme dei tipi di oggetto gestiti, le operazioni e gli attributi supportati per ciascun tipo mediante REST.
- Operazioni self-service supportate, come ad esempio la password di ripristino e l'insieme degli attributi self-service dell'utente consentiti.
- La policy di appartenenza in base a cui gli utenti sono autorizzati a richiamare le operazioni REST configurate.

La tabella sottostante riporta i dettagli di configurazione dei servizi Web e le impostazioni richieste per l'applicazione mobile.

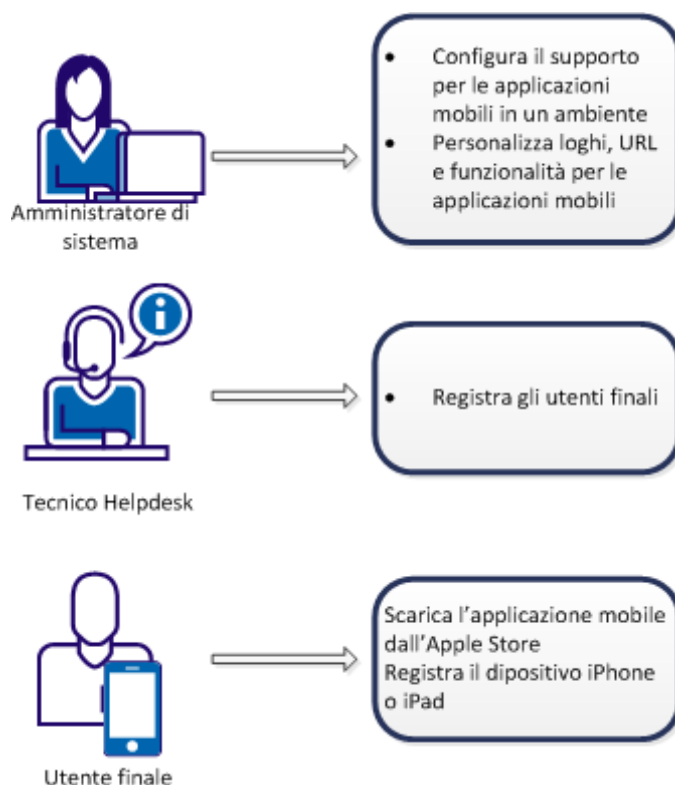
Sezione di configurazione	Elemento	Descrizione	Impostazione dell'applicazione mobile
Profilo	nome	Il nome della configurazione.	Selezione della distribuzione
	identificatore	L'ID univoco che deve essere impostato da un determinato client nell'intestazione http dell'ID di configurazione per ogni richiesta del server CA Identity Manager.	Selezione della distribuzione. Il servizio di configurazione dell'applicazione mobile restituisce l'identificatore che dovrà essere utilizzato per tutte le richieste REST successive.
	Abilitato	Abilita/disattiva la configurazione	True
Protezione	Richiedi comunicazione protetta.	https richiesto o non richiesto	Selezione della distribuzione. Valore scaricato dal Servizio di configurazione dell'applicazione mobile.

	Abilita crittografia	L'opzione viene utilizzata per crittografare i payload non SSL. Richiede una libreria di crittografia sul lato client, la conoscenza della chiave di crittografia e un supporto di crittografia/decrittografia esplicito sul lato client	Non utilizzato. Non selezionare la casella.
	Segreto di configurazione	Il segreto condiviso richiesto come parte del client REST per il modello di attendibilità del server.	È necessario specificare il valore. Le distribuzioni generano il segreto durante la definizione dell'istanza di configurazione.
Tipi di oggetto	Tipo di oggetto	I tipi di oggetto impostati come risorse REST.	Il tipo di oggetto Utente
	Metodi e attributi	I metodi di risorsa (CRUD) supportati per un tipo di oggetto selezionato e il set di attributi consentiti per tali metodi.	Il tipo di oggetto Utente con diritti di visualizzazione per i seguenti attributi, in base a quanto riportato nella distribuzione specifica dello schema utente. ■ Telefono ufficio ■ Reparto ■ E-mail ■ Nome ■ Cognome ■ Manager ■ Ufficio ■ Title
Auto-amministrazione	Regola membri	Regola che indica quali utenti possono eseguire le attività di auto-amministrazione.	La regola deve corrispondere alla regola di appartenenza della configurazione dell'applicazione mobile. Il set di attributi per la modifica deve rimanere vuoto.

	Abilita reimpostazione password	Consente agli utenti di reimpostare la propria password.	Abilita
	Attributi	L'insieme di attributi che l'utente può gestire	Elenco vuoto
Membri	Membri	Definisce le regole per l'autorizzazione del richiamo delle operazioni REST definite per la configurazione	Una regola di appartenenza corrispondente all'insieme di utenti dell'applicazione mobile

Funzionamento del processo di implementazione

La configurazione delle applicazioni mobili viene eseguita da tre tipi di utenti. Il grafico seguente illustra i tipi di utente e le attività che eseguono.



Per abilitare un utente finale all'utilizzo dell'applicazione mobile con CA Identity Manager, si verificano le attività seguenti:

1. Un amministratore di sistema configura il supporto dell'applicazione mobile in un ambiente.

La configurazione comprende le attività seguenti:

- Configurazione dell'attivazione e reimpostazione degli attributi dei codici
- Aggiunta di attività, di criteri Policy Xpress e di un modello di messaggio di posta elettronica per la registrazione degli utenti mobili.
- Creazione di una definizione di servizi Web.
- Modifica del messaggio di posta elettronica di registrazione.

L'amministratore di sistema configura anche la personalizzazione, gli URL e le funzionalità a cui gli utenti mobili possono accedere.

2. Un amministratore, come ad esempio un tecnico dell'Helpdesk, registra gli utenti finali applicabili nella console utente.

Il processo di registrazione attiva un codice di attivazione per ciascun utente finale e invia automaticamente un messaggio di posta elettronica con le istruzioni sul codice e di registrazione all'utente finale.

3. L'utente finale esegue il download dell'applicazione mobile dall'Apple Store e registra una periferica, come ad esempio uno smartphone o un tablet seguendo le istruzioni e utilizzando il codice ricevuto nel messaggio di posta elettronica.

L'utente finale può quindi utilizzare l'applicazione mobile per accedere alle funzionalità di CA Identity Manager.

Nota: Se durante la creazione dell'utente viene selezionata l'opzione La password deve essere cambiata, gli utenti dell'applicazione mobile non possono completare l'attivazione.

Funzionamento della configurazione dell'applicazione

L'applicazione mobile recupera la configurazione delle API di configurazione del server CA Identity Manager. Se l'applicazione mobile viene installata e non è stata scaricata la configurazione corrispondente, verrà richiesta l'immissione del nome utente e della password. Tali credenziali verranno richieste per il download della configurazione definita dal collegamento fornito nel messaggio di posta elettronica di registrazione.

In seguito al download iniziale della configurazione, per ogni avvio dell'applicazione verrà eseguito il controllo dell'ultima versione disponibile sul server CA Identity Manager. L'API di verifica della versione di configurazione viene utilizzata per verificare la disponibilità della versione più recente.

Funzionamento della registrazione utenti

Per ciascun accesso all'applicazione mobile, è necessario richiedere l'accesso da CA Identity Manager. Se l'accesso viene consentito, l'utente riceverà il codice di attivazione corrispondente. La policy di appartenenza per la configurazione dell'applicazione mobile e la policy di appartenenza corrispondente per i servizi Web dovrà soddisfare i criteri definiti per gli utenti mobili che richiedono l'accesso. È necessario definire un valore minimo di %ACTCODE% per il valore "Registered", oppure un valore superiore a 0.

Se l'accesso per un utente mobile viene rimosso, il server CA Identity Manager ripristinerà gli attributi di attivazione impedendo l'accesso all'utente per l'applicazione mobile.

Configurazione di CA Identity Manager per il supporto dell'applicazione mobile

L'applicazione mobile comunica con CA Identity Manager (utilizzando i servizi Web REST) per la gestione delle password e delle approvazioni. Per abilitare questa comunicazione, un amministratore di sistema completa i passaggi seguenti:

1. [Configurazione degli attributi obbligatori](#) (a pagina 520).
2. [Importazione delle attività di amministrazione](#) (a pagina 523)
3. [Creazione di un servizio Web](#) (a pagina 525).
4. [Modifica del messaggio di posta elettronica di registrazione](#) (a pagina 527).
5. È inoltre possibile configurare il supporto di SiteMinder per l'applicazione mobile.

Configurazione degli attributi obbligatori

L'archivio utenti di CA Identity Manager deve includere i seguenti attributi noti per abilitare la registrazione e l'accesso degli utenti mediante l'applicazione mobile:

- **%ACTCODE%:** identifica l'attributo che archivia un numero di attivazione generato casualmente. Dopo che l'utente è stato registrato, questo attributo contiene la parola Registered.
- **%ACTCODEVAL%:** identifica l'attributo che archivia il codice di attivazione impostato dal client durante la registrazione. CA Identity Manager confronta questo valore con il valore %ACTCODE%.
- **%CURRENT_AUTH_QUESTIONS%:** identifica l'attributo che archivia temporalmente i valori della domanda di verifica. Il valore viene cancellato in seguito alla corretta risposta da parte dell'utente.
- **%MOBILE_PIN%:** identifica l'attributo che archivia il numero di identificazione personale o il valore di stringa, i quali forniscono la password alfanumerica condivisa tra un utente e un sistema utilizzabile per l'autenticazione dell'utente nel sistema.
- **%PWRESETCODE%:** identifica l'attributo che archivia un codice crittografato, il quale fornisce l'autenticazione con fattore singolo durante la reimpostazione della password.

Questi attributi noti vengono mappati sugli attributi disponibili dell'archivio utenti nel file di configurazione della directory (directory.xml). Se non c'è nessun attributo disponibile, estendere lo schema dell'archivio utenti. Per ulteriori informazioni sull'estensione dello schema, consultare la documentazione relativa al proprio archivio utenti.

Includere le seguenti classificazioni di dati nelle descrizioni degli attributi:

<DataClassification name="sensitive"/>

Sostituisce il valore del codice di reimpostazione con caratteri jolly in schermate di attività, record di verifica e registri di sistema.

Importante. Non includere la classificazione di dati sensibili nella definizione dell'attributo %ACTCODE%. Se viene incluso l'attributo sensibile, l'applicazione mobile non funzionerà correttamente.

<DataClassification name=" AttributeLevelEncrypt "/>

Crittografa e decrittografa il valore del codice di reimpostazione così come viene scritto e letto dall'archivio utenti mediante la chiave di crittografia definita.

<DataClassification name=" ignore_on_copy "/>

Consente a CA Identity Manager di ignorare un attributo quando un amministratore crea una copia di un oggetto nella console utente.

Nota: consultare la fine del presente argomento per ottenere esempi degli attributi noti.

Procedere come descritto di seguito:

1. Accedere alla console di gestione.
2. Selezionare Directory, quindi fare clic sulla directory che contiene gli utenti mobili.
3. Esportare la directory.
4. Aggiungere o modificare una descrizione di attributo in modo da includere l'attributo noto %ACTCODE%.

È possibile eseguire il mapping di qualsiasi attributo disponibile sull'attributo noto %ACTCODE%.

5. Ripetere il passaggio 4 per definire l'attributo noto %ACTCODEVAL%. Includere le classificazioni di dati seguenti:

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

6. Aggiungere una descrizione per l'attributo noto %CURRENT_AUTH_QUESTIONS%. Includere le seguenti classificazioni di dati:

```
<DataClassification name="ignore_on_copy"/>
```

7. Aggiungere una descrizione di attributo per l'attributo noto %MOBILE_PIN%. Includere le classificazioni di dati seguenti:

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

8. Aggiungere una descrizione di attributo per l'attributo noto %PWRESETCODE%. Includere le classificazioni di dati seguenti:

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

9. Salvare il file directory.xml.

10. Caricare il file directory.xml salvato facendo clic su Aggiorna nella pagina delle proprietà di directory nella console di gestione.

Esempi

Nota: è possibile eseguire il mapping di qualsiasi attributo disponibile sugli attributi noti.

%ACTCODE%

```
<ImManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
```

```
wellknown="%ACTCODE%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%ACTCODEVAL%

```
ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%ACTCODEVAL%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%CURRENT_AUTH_QUESTIONS%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
```

```
valuetype="String"
required="false"
multivalued="false"
wellknown="%MOBILE_PIN%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%PWRESETCODE%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%PWRESETCODE%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

Importazione delle attività di amministrazione

Prima che gli utenti mobili possano accedere a CA Identity Manager, gli amministratori li registrano nella console utente. Il processo di registrazione genera un codice di attivazione e invia un messaggio di posta elettronica all'utente mobile.

Per supportare queste attività, importare un file di definizione di ruolo che aggiunge la funzionalità seguente all'ambiente:

- Attività di configurazione mobile
- Registrazione dell'utente per l'applicazione mobile e rimozione dell'utente dalle attività dell'applicazione mobile
- Criteri di Policy Xpress che generano codici di attivazione e annullamento della registrazione del client mobile da un account utente.
- Un modello di messaggio di posta elettronica per inviare il messaggio di posta elettronica agli utenti mobili

Procedere come descritto di seguito:

1. Accedere alla console di gestione.
2. Selezionare Environments (Ambienti), quindi fare clic sull'ambiente che supporta l'applicazione mobile.
3. Selezionare Role and Task Settings (Impostazioni ruolo e attività), quindi fare clic su Importa nella schermata successiva.
4. Selezionare MobileApp-RoleDefinitions, quindi fare clic su Fine.
5. Riavviare l'ambiente.
6. Aggiungere le attività seguenti al ruolo Manager di Sistema:
 - Creare la configurazione mobile
 - Modificare la configurazione mobile
 - Visualizzare la configurazione mobile
 - Eliminare la configurazione mobile
 - Registrare l'utente per l'applicazione mobile
 - Rimuovere l'utente dall'applicazione mobile

Le nuove attività si trovano nelle categorie Utente e Sistema.

Creazione di una configurazione dei servizi Web

L'applicazione mobile utilizza i servizi Web REST per comunicare con CA Identity Manager. Per supportare l'applicazione mobile, un amministratore di sistema crea una definizione del servizio Web nella console utente.

Nota: se nella configurazione dei servizi Web è abilitata la crittografia, le chiamate REST non funzionano.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con privilegi di amministratore di sistema.
2. Creare una definizione del servizio Web nel modo seguente:
 - a. Accedere a Sistema, Servizi Web, Crea configurazione dei servizi Web.
 - b. Nella scheda Profilo, completare i seguenti campi:
 - Nome: *qualsiasi nome*. Ad esempio RestMobile.
 - ID: *ID univoco*. Il valore predefinito è RestMobile.

Il valore del campo ID deve corrispondere al valore di **restid** nella configurazione dell'applicazione mobile.

Considerare di modificare il valore dell'ID e del restid per aumentare la protezione.
 - Enable Attribute (Abilita attributo): selezionare questa casella di controllo.

c. Nella scheda Protezione, completare le seguenti azioni:

- Stabilire se è necessario selezionare l'opzione Richiedi comunicazione protetta.

Nota: tenere in considerazione la crittografia del traffico http di tutte le applicazioni mobili. È possibile configurare il traffico in due modalità:

- Mediante un server proxy: in questo scenario di utilizzo, il server di CA Identity Manager sarà protetto da un firewall. È possibile decidere di non proteggere la comunicazione dal server proxy al server di CA Identity Manager. Si consiglia tuttavia di verificare che la comunicazione http tra l'applicazione mobile e il server proxy sia protetta. Per questo scenario di utilizzo, **NON** selezionare Richiedi comunicazione protetta.

Nota: se viene eseguita l'integrazione di CA Identity Manager e SiteMinder, selezionare l'opzione Richiedi comunicazione protetta per applicare la comunicazione SSL alle chiamate di servizio Web.

- Direttamente sul server di CA Identity Manager: in questo scenario di utilizzo, il client mobile stabilisce la comunicazione direttamente con il server di CA Identity Manager. Si consiglia di crittografare questo tipo di comunicazione. Per impostare il requisito, selezionare l'opzione Richiedi comunicazione protetta.
- Verificare che l'opzione Abilita crittografia non sia selezionata.

Not: se la crittografia è abilitata, i dettagli utente non vengono visualizzati nell'applicazione mobile.

d. Nella scheda Tipi di oggetto, andare a UTENTE, selezionare UTENTE, quindi fare clic sul pulsante Modifica.

e. Selezionare soltanto Consenti accesso in visualizzazione.

Rimuovere le altre autorizzazioni di accesso deselectando le opzioni Consenti accesso per la modifica, Consenti accesso per la creazione e Consenti accesso per l'eliminazione.

f. Nella scheda Amministrazione automatica, completare i passaggi seguenti:

- Selezionare il pulsante Aggiungi posizionato sotto Regola membri per creare un ruolo membri e specificare Tutto.

Nota: È possibile creare soltanto una regola membri.

- Abilitare la reimpostazione della password per supportare la funzionalità Modifica password nell'applicazione mobile.

g. Nella scheda Membro, costruire una regola membri con i criteri seguenti:

- Codice di attivazione = Registrato, o
- Codice di attivazione >0

h. Inviare e salvare il servizio Web.

Modifica del messaggio di posta elettronica di registrazione

Modificare il messaggio di posta elettronica di registrazione predefinito per includere l'URL dell'oggetto di configurazione mobile.

Procedere come descritto di seguito:

1. Nella console utente, selezionare Sistema, Posta Elettronica, Modifica messaggio di posta elettronica.
2. Cercare e selezionare l'utente registrato per la posta elettronica dell'applicazione mobile.
3. Nella scheda Contenuto, fare clic sul pulsante Toggle HTML Source (Attiva/Disattiva origine HTML).
4. Specificare l'URL dell'oggetto di configurazione mobile nella voce href per mobileregsvdm come segue:

```
<a  
href="mobileregsvdm://{Attribute:%ACTCODE%}&https://FQN/iam/im/ws  
/Alias/mobile/ConfigName">
```

FQN

Specificare il nome o l'indirizzo IP del server CA Identity Manager.

Alias

Specificare il nome dell'ambiente.

ConfigName

Specificare il nome dell'oggetto di configurazione.

5. Fare clic su Inoltra.

Configurazione di SiteMinder per il supporto dell'applicazione mobile

I servizi Web utilizzati dall'applicazione mobile supportano l'autenticazione nativa mediante le credenziali nome utente/password fornite dall'applicazione mobile mediante l'intestazione HTTP AUTHORIZATION o l'autenticazione SiteMinder. In base a quanto riportato precedentemente, la configurazione dei servizi Web definisce il criterio di autorizzazione per ciascuna richiesta di metodo e di risorse REST.

URL del servizio Web REST di IM

I servizi REST di IM si basano sui seguenti URL di base:

`http[s]://[FQN]/iam/im/ws/[Alias]`

- FQN – Il nome completo e la porta del punto di accesso al server CA Identity Manager
- Alias – L'alias pubblico dell'ambiente di CA Identity Manager per la connessione.

URL di configurazione dell'applicazione mobile

La configurazione dell'applicazione mobile contiene un URL specifico che consente il recupero di informazioni di configurazione bootstrap richieste per il download della configurazione dell'applicazione mobile. L'URL per la configurazione è il seguente:

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]`

ConfigName: il nome della configurazione dell'applicazione mobile dell'ambiente di CA Identity Manager per un determinato set di utenti dell'applicazione mobile. Il nome della configurazione viene reso noto all'applicazione mediante un collegamento all'URL di configurazione nel messaggio di posta elettronica di registrazione inviato in seguito all'approvazione della richiesta dell'utente per l'accesso all'applicazione mobile.

API REST non autenticate

API di configurazione

Le seguenti API di configurazione non richiedono l'autenticazione.

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/image`

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/ver`

Ripristino API della password

`https://[FQN]/iam/im/ws/[Alias]/myself/resetpasswordWithResetCodeAndToken`

Nota: l'API `resetPasswordWithResetCodeAndToken` contiene token di protezione forniti nelle intestazioni `http` dell'applicazione mobile. Il server di CA Identity Manager verifica la presenza e la validità di questi token.

Durante l'integrazione di SiteMinder per la protezione dell'accesso CA Identity Manager, è possibile definire gli URL con un realm non protetto o protetto da uno schema di autenticazione anonima.

API REST autenticate

I seguenti URL vengono utilizzati dall'applicazione mobile e richiedono l'autenticazione e l'utilizzo delle policy di configurazione del servizio Web per l'autorizzazione.

Configurazione

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/conf`

Utente self-service

`http[s]://[FQN]/iam/im/ws/[Alias]/myself`

Elenco di lavoro

`http[s]://[FQN]/iam/im/ws/[Alias]/worklist`

Utente

`http[s]://[FQN]/iam/im/ws/[Alias]/mo/User`

Configurazione di un'applicazione mobile

Gli amministratori di sistema configurano l'applicazione mobile di CA Identity Manager nella console utente.

Un ambiente può includere più configurazioni di applicazione mobili. La creazione di più configurazioni permette di supportare varie personalizzazioni o funzionalità per diversi tipi di utenti mobili. Ad esempio, è possibile creare una configurazione per modifiche della password di dipendente e un'altra per l'approvazione degli elementi di lavoro da parte dei responsabili.

Gli amministratori possono configurare le proprietà di configurazione seguenti per l'applicazione mobile:

- Personalizzazione

Specificare il logo dell'azienda nell'applicazione mobile.

- Funzionalità

Attivare la funzionalità seguente:

- Supporto per password dimenticata
- Supporto per la modifica della password
- Coda di approvazione del flusso di lavoro
- Visualizzazione collegamento al Manager

- Informazioni di supporto
- Mapping attributo

Eseguire il mapping degli attributi nell'archivio utenti sugli attributi esposti nell'applicazione mobile.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente autorizzato all'uso delle attività di configurazione mobile.
2. Fare clic su Attività, Sistema, Configurazione mobile, Crea configurazione mobile.
3. Accettare l'opzione predefinita, Crea un nuovo oggetto di tipo Configurazione mobile.
4. Nella scheda Generale, compilare i campi obbligatori. È possibile specificare un'immagine per l'applicazione mobile.

URL di base

Verificare l'URL di base dell'ambiente corrente. L'URL di base viene inserito automaticamente quando si crea una configurazione mobile.

CA Identity Manager utilizza l'URL di base per recuperare il nome, la porta e il protocollo del server utilizzati dall'applicazione mobile per generare l'URL per le chiamate REST.

Configurazione

Individuare una configurazione o immettere un nome di configurazione univoco.

Versione

Aumentare il numero di versione ogni volta che si modifica e si salva una configurazione.

Nell'applicazione mobile il numero di versione viene utilizzato per determinare quando scaricare una nuova versione della configurazione. Quando l'applicazione mobile viene avviata, il numero di versione dal server viene confrontato con la versione della configurazione caricata. Se è disponibile una nuova versione, l'applicazione mobile aggiorna la configurazione.

Nota: non aumentare il numero di versione quando si modifica il file inizialmente.

Immagine di personalizzazione

Specificare l'URL completo di un'immagine PNG, con una dimensione suggerita di 222 per 222 pixel. L'immagine viene visualizzata nella schermata iniziale, nella schermata di gestione della password e nella parte superiore della schermata dell'applicazione mobile.

5. Nella scheda Funzionalità, selezionare le funzionalità per l'applicazione mobile.

Comportamento di ripristino della password

Selezionare il metodo da utilizzare per il comportamento, il quale è determinato al momento della configurazione degli attributi obbligatori:

- Predefinito
- Richiesta di verifica PIN
- Richiesta di verifica Domande e Risposte

Nota: Se si seleziona Richiesta di verifica Domande e Risposte, è necessario accedere a Attività, Environment Administrator (Amministratore ambiente) e selezionare Configurazione domande e risposte. Assicurarsi di selezionare la casella Attiva, immettere il numero di domande di autenticazione (da 1 a 5) e fare clic su Invia. Per applicare le impostazioni di configurazione, è necessario fare clic sul pulsante Invia anche se non si apportano modifiche alle impostazioni predefinite.

6. Nella scheda Supporto, specificare le informazioni di supporto per gli utenti mobili.
7. Nella scheda Mapping attributo, eseguire il mapping degli attributi dell'applicazione mobile sugli attributi nell'archivio utenti di CA Identity Manager. È possibile eseguire il mapping degli attributi su attributi fisici o attributi noti.
8. Nella scheda Proprietà aggiuntive, specificare coppie di valore per le proprietà aggiuntive ai fini del supporto di nuovi campi o funzionalità nell'applicazione mobile.

Utilizzare il formato seguente:

Key1=value1

Key2=value2

Key3=value3

Nota: CA Technologies fornirà le istruzioni quando gli amministratori dovranno aggiungere altre proprietà. In questa release, non è necessario specificare proprietà aggiuntive.

9. Nella scheda Membri, specificare le regole che determinano l'insieme di utenti in grado di visualizzare questa configurazione sull'applicazione mobile.
10. Fare clic su Inoltra.

Configurare delle proprietà aggiuntive

Dopo aver configurato l'applicazione mobile, sarà inoltre possibile specificare coppie di valore della chiave di proprietà specifiche per il supporto delle nuove funzionalità dell'applicazione mobile. L'operazione viene eseguita utilizzando la scheda Proprietà aggiuntive.

Utilizzare il formato seguente:

- demoMode="Disable/Enable"
- maxPinRetries=<qualsiasi valore numerico positivo>
- multiAccount="Disable/Enable"
- managerTraversal="Disable/Enable"
- startupWithBrandLogo="true/false"

Nota: CA Technologies fornirà le istruzioni quando gli amministratori dovranno aggiungere altre proprietà.

Tuttavia, queste funzionalità sono abilitate per impostazione predefinita con le configurazioni mobili:

- DemoMode: consente la visualizzazione di una versione dimostrativa dell'applicazione mobile. Questa opzione è disponibile nella sezione Impostazioni dell'applicazione mobile.
- maxPinRetries: consente all'amministratore di configurare il numero massimo di tentativi di immissione del PIN non riusciti per gli utenti mobili. Il numero predefinito di tentativi non riusciti è 5.
- MultiAccount: consente di aggiungere più account mediante l'aggiunta di più utenti registrati per l'applicazione mobile mediante i codici di attivazione.
- ManagerTraversal: mostra i dettagli del manager del responsabile dell'approvazione e del richiedente per i dettagli dell'elemento di lavoro.
- startupWithBrandLogo: consente all'utente di specificare il logo dell'account personalizzato (l'immagine di personalizzazione dell'account) che verrà visualizzato invece del logo predefinito di CA. Se questo valore di chiave è impostato su true ma il campo del logo contiene un URL vuoto o non valido, la schermata di avvio non verrà caricata. Il logo CA verrà sempre visualizzato con il primo avvio dell'applicazione dopo l'installazione. Questa proprietà aggiuntiva appartiene ai dati dell'account. Non è disponibile nessun dato dell'account al primo avvio.

Nota: le modifiche apportate verranno visualizzate correttamente all'avvio successivo e dopo aver stabilito la comunicazione con il server CA Identity Manager.

Per disattivare le funzionalità per il client mobile, è necessario aggiungere la seguente coppia del valore chiave nella scheda Proprietà aggiuntive della configurazione mobile di CA Identity Manager.

- Attivazione o disattivazione della funzionalità per la modalità demo
Impostare DemoMode su "Enable" o "Disable"
 - demoMode="Disable/Enable"
- Attivazione o disattivazione della funzionalità maxPinRetries
Impostare maxPinRetries su un valore numerico positivo
 - maxPinRetries=<qualsiasi valore numerico positivo> Il numero predefinito di tentativi non riusciti è 5.
- Attivazione o disattivazione della funzionalità multi-account
Impostare MultiAccount su "Enable" o "Disable"
 - multiAccount="Disable/Enable"
- Attivazione o disattivazione della funzionalità ManagerTraversal
Impostare ManagerTraversal su "Enable" o "Disable"
 - managerTraversal="Disable/Enable"
- Attivazione o disattivazione della funzionalità startupWithBrandLogo
Impostare startupWithBrandLogo su "true" o "false"
 - startupWithBrandLogo="true/false"

Procedere come descritto di seguito:

1. Accedere alla console utente di CA Identity Manager come amministratore.
2. Fare clic su Attività, Sistema, Configurazione mobile, Crea configurazione mobile.
3. Nella scheda Proprietà aggiuntive, specificare le coppie di valore per le proprietà aggiuntive ai fini del supporto di nuovi campi o funzionalità nell'applicazione mobile.
 - demoMode="Disable/Enable"
 - maxPinRetries=<qualsiasi valore numerico positivo> Il numero predefinito di tentativi non riusciti è 5.
 - multiAccount="Disable/Enable"
 - managerTraversal="Disable/Enable"
 - startupWithBrandLogo="true/false"

Download dell'applicazione mobile

Una volta configurata l'applicazione mobile, gli utenti finali possono scaricarla da Apple Store. Per individuare l'applicazione mobile nell'Apple Store, cercare CA Identity Manager.

L'utente finale può quindi registrare il proprio dispositivo, ad esempio uno smartphone o un tablet, seguendo le istruzioni e il codice ricevuti via posta elettronica.

Risoluzione dei problemi delle applicazioni mobili

Richiesta al team di supporto di un file di registro

Se un utente ha un problema con l'applicazione mobile, i tecnici del supporto possono richiedere un file di registro per facilitare la procedura di risoluzione dei problemi.

L'utente mobile abilita il debug attraverso il proprio iPhone o iPad. Una volta abilitato il debug, l'utente mobile può utilizzare l'applicazione mobile per inviare il registro a un indirizzo di posta elettronica del supporto.

Per abilitare la generazione di un registro nell'applicazione mobile, l'utente mobile completa i passaggi seguenti.

1. Nel telefono o iPad, accedere a Impostazioni, Identity Manager, Debug.
2. La selezione mediante pressione è abilitata.
3. Riavviare l'applicazione ed eseguire le azioni che si desidera che vengano visualizzate nel registro.
4. Nella scheda Impostazioni dell'applicazione mobile di CA Identity Manager, premere Email Log (Registro posta elettronica).

L'applicazione mobile crea un messaggio di posta elettronica con il file di registro allegato. Il messaggio di posta elettronica viene inviato all'indirizzo di posta elettronica configurato per l'assistenza nella console utente.

La domanda/risposta di ripristino del comportamento della password produce un errore con l'utilizzo delle impostazioni di configurazione della domanda e della risposta predefinite nell'amministratore di ambiente delle attività Identity Manager.

Sintomo

Dopo aver selezionato le QnA come comportamento di reimpostazione della password con le impostazioni di configurazione della domanda e della risposta predefinite, la reimpostazione della password non riesce e viene visualizzato il seguente messaggio di errore:

"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0,0,0,0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file"

Soluzione:

Eseguire i passaggi seguenti per garantire il funzionamento della reimpostazione della password con le QnA impostate sul comportamento di reimpostazione della password:

Procedere come descritto di seguito:

1. Accedere a CA Identity Manager come SuperAdmin.
2. Accedere a Attività, Environment Administrator (Amministratore di ambiente), quindi selezionare Configurazione domande e risposte.
3. Fare clic sul pulsante Inoltra.

Nota: anche i valori predefiniti delle opzioni Attiva e Numero di domande di autenticazione vengono applicati dopo aver eseguito l'operazione.

Capitolo 17: CA User Activity Reporting

Questa sezione contiene i seguenti argomenti:

[Funzionalità di CA Enterprise Log Manager](#) (a pagina 537)

[Integrare i rapporti o le query aggiuntive di CA Enterprise Log Manager con CA Identity Manager](#) (a pagina 548)

Funzionalità di CA Enterprise Log Manager

Quando CA Enterprise Log Manager si integra con CA Identity Manager, si ottiene la seguente funzionalità:

- L'agente CA Enterprise Log Manager raccoglie le informazioni di controllo di CA Identity Manager e le invia a CA Enterprise Log Manager per la conversione in Grammatica evento comune (CEG, Common Event Grammar) di CA.
- La Console utente di CA Identity Manager può recuperare facilmente i rapporti di CA Enterprise Log Manager e/o le query con informazioni di contesto di CA Identity Manager utilizzate per filtrare le informazioni restituite.
- CA Identity Manager viene fornito con un numero di rapporti predefiniti e con un'infrastruttura predisposta per l'aggiunta di rapporti e/o di query di CA Enterprise Log Manager a un'attività esistente o nuova.
- L'agente CA Enterprise Log Manager viene installato sul computer su cui è installato CA Identity Manager [Database di controllo]
- CA Identity Manager Connector viene configurato sull'agente CA Enterprise Log Manager
- Viene creata la registrazione del prodotto CA Enterprise Log Manager per l'ambiente di Identity Manager
- Per la registrazione del prodotto viene creato un filtro di accesso ai dati di CA Enterprise Log Manager facoltativo

Componenti di CA Enterprise Log Manager

Quando CA Identity Manager si integra con CA Enterprise Log Manager, i componenti seguenti vengono aggiunti all'architettura di CA Identity Manager:

- La scheda di visualizzazione di CA Enterprise Log Manager consente di incorporare gli oggetti di CA Enterprise Log Manager in qualsiasi attività nuova o esistente.
Nota: è necessaria una connessione server di CA Enterprise Log Manager configurata.
- Definizioni di ruolo che è possibile importare

Limiti di integrazione

Di seguito vengono elencati i limiti noti dell'integrazione del framework con il server CA Enterprise Log Manager:

- L'esecuzione dell'operazione di recupero di elenchi di query e rapporti per la configurazione delle attività può risultare lenta.
- Le API di CA Enterprise Log Manager riconoscono solo i fusi orari con nomi Java predefiniti.
- L'operazione EQUAL effettua la distinzione tra maiuscole e minuscole se utilizzata in un filtro composto.
- La versione minima del server CA Enterprise Log Manager è CA ELM (45.10) con i seguenti aggiornamenti di sottoscrizione applicati in ordine di visualizzazione:
 1. Patch sottoscrizione SP-1
 2. Patch contenuto M5
 3. Aggiornamento Open API
- È supportata una sola connessione al server CA Enterprise Log Manager alla volta.

Integrazione di CA Enterprise Log Manager con CA Identity Manager

Prima di visualizzare e gestire i rapporti e le query di CA Enterprise Log Manager, è necessario che l'amministratore effettui le operazioni seguenti:

1. Installare l'agente CA Enterprise Log Manager.
2. Creare un nuovo connettore.
3. Abilitare il controllo in CA Identity Manager.
4. Configurare il server CA Enterprise Log Manager.

Prerequisiti di installazione dell'agente CA Enterprise Log Manager

Prima di installare l'agente CA Enterprise Log Manager, è necessario procedere come segue:

- Assicurarsi che il computer server CA Enterprise Log Manager sia raggiungibile dal computer su cui è in esecuzione CA Identity Manager o che ospita il database di controllo di CA Identity Manager.
- Assicurarsi che il computer agente sia raggiungibile dal computer server.
- Configurare l'origine dati sul computer agente. Per ulteriori informazioni, fare clic [qui](#) (a pagina 539).
- Verificare che sia in uso la versione 9.0.28 o superiore di Adobe Flash Player. È possibile scaricare Adobe Flash Player dal seguente URL:
<http://www.adobe.com/go/getflash>
- Scaricare i file binari agente. Per ulteriori informazioni, fare clic [qui](#) (a pagina 540).
- Ottenere la chiave di autenticazione agente. Per ulteriori informazioni, fare clic [qui](#) (a pagina 540).
- Rendere il nome/indirizzo IP del server prontamente accessibile.
- Rendere le informazioni di account prontamente accessibili, ma senza compromettere la sicurezza. Questo è l'account di identità con il quale l'agente viene eseguito come servizio (Windows).
- Se un connettore esiste già, esportare le informazioni predefinite sul connettore e tenerle a disposizione.
- Assicurarsi che il computer disponga di 4 GB RAM.

Configurare l'origine dati sul computer agente.

Seguire questa procedura per configurare l'origine dati sul computer agente.

Per configurare l'origine dati

1. Accedere al Pannello di controllo, Strumenti di amministrazione, Origini di dati (ODBC)
2. Nella scheda DSN di sistema, aggiungere quanto segue:
origini dati (ODBC) imsauditevent12 che fa riferimento al database di controllo.
3. Fare clic su Applica e quindi su OK.
L'origine dati viene configurata.

Download dei file binari dell'agente

Seguire questa procedura per scaricare i file binari dell'agente.

Per scaricare i file binari agente

1. Accedere al server CA Enterprise Log Manager mediante l'URL seguente:
`https://<host>:5250/spin/calm/CALMSpindle.csp`
2. Accedere a Amministrazione, Raccolta log, Gestione agenti, Download file binari agente, <OS> <version>
3. Salvare in File.

Ottenere la chiave di autenticazione agente

Utilizzare questa procedura per ottenere la chiave di autenticazione agente.

Per ottenere la chiave di autenticazione agente

1. Dal server CA Enterprise Log Manager, accedere ad Amministrazione, Raccolta log, Gestione agenti, Chiave di autenticazione agente.
2. Rendere la chiave prontamente accessibile, ma senza compromettere la sicurezza.

Installazione dell'agente CA Enterprise Log Manager

L'agente CA Enterprise Log Manager è responsabile della raccolta eventi e di inviare le informazioni al server CA Enterprise Log Manager. Installare l'agente su un server di database o computer di endpoint CA Identity Manager per abilitare la registrazione.

Nota: l'agente CA Enterprise Log Manager viene supportato su Windows e Linux.

Per installare l'agente CA Enterprise Log Manager

1. Sul server di database, eseguire l'installazione di `ca-elmagent-<versione>.exe` e specificare quanto segue:

Nome server/indirizzo IP di CA Enterprise Log Manager e codice di autenticazione.

Le informazioni di account dell'agente server saranno utilizzate per eseguire l'agente come servizio/demon.
2. Specificare il file dell'elenco di connettori predefinito, se disponibile.
3. Accedere al server CA Enterprise Log Manager mediante l'URL seguente:
`https://<host> :5250/spin/calm/CALMSpindle.csp`
4. Accedere ad Amministrazione, Raccolta log, Gestione agenti, Gruppo agenti predefinito
5. Selezionare il computer agente e avviare la visualizzazione Stato e comando.

Lo stato dovrebbe essere in esecuzione.

Importazione delle definizioni di ruolo

Prima di poter configurare la connessione Enterprise Log Manager nella console utente, è necessario importare le definizioni di ruolo di CA Enterprise.

Per importare le definizioni di ruolo:

1. Accedere alla console di gestione mediante l'URL seguente.
`http://host:port/iam/immanage`
2. Accedere a Environment (Ambiente), Role and Task Settings (Impostazioni ruolo e attività), fare clic sul pulsante Import (Importa) e selezionare Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml.
3. Fare clic su Salva e chiudi.
4. Nella scheda Sistema della console utente, fare clic su Configura la connessione Enterprise Log Manager, compilare le informazioni richieste e fare clic su Invia.

Creare un nuovo connettore

Seguire questa procedura per creare un nuovo connettore.

Per creare un nuovo connettore:

1. Accedere al server CA Enterprise Log Manager mediante l'URL seguente:
`https://<host>:5250/spin/calm/CALMSpindle.csp`
2. Accedere ad Amministrazione, Raccolta log, Gestione agenti, Gruppo agenti predefinito
3. Selezionare il computer agente.
4. Passare alla visualizzazione Connettori.
5. Fare clic sul pulsante Create a new Connector (Crea un nuovo connettore) e immettere le informazioni seguenti:

Dettagli connettore

Se si desidera, selezionare il tipo di integrazione CA IdentityManager e modificare il nome del connettore.

Configurazione connettore

Stringa di connessione

- `Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>`
- `Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>`

Nome utente: <Auditing DB User>

Password: <Auditing DB User Password>

6. Applicare al connettore di CA Identity Manager le seguenti modifiche apportate alla configurazione della connessione perché possa essere utilizzato con 12.6.5.
 - **SourceName:** il nome dell'origine dei dati sul computer agente - `imsauditevent12`
 - **AnchorSQL:** selezionare `max(id)` da `imsauditevent12`
 - **AnchorField:** `IMS_EVENTID`
 - **Evento SQL:**

```
select imsauditevent12.id as IMS_EVENTid ,imsauditevent12.audit_time as  
IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME  
,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn  
as ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID  
,imsauditevent12.event_description as EVENTINFO  
,imsauditevent12.event_state as EVENTSTATE  
,imsauditevent12.tasksession_oid as TASKOID
```

```
,imsaudittasksession12.task_name as TASKNAME
,imsauditeventobject12.object_type as OBJECTTYPE ,
imsauditeventobject12.object_name as
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as ATTRNAME
,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRNEWVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE from
imsaudittasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsaudittasksession12.id and
imsauditevent12.tasksession_oid = imsaudittasksession12.tasksession_oid
and
imsauditeventobject12.parent_event_id = imsauditevent12.id and
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id
ORDER BY
imsauditevent12.id ASC;
```

7. Salvare e chiudere.

Per verificare che il connettore funzioni correttamente

1. Accedere ad Amministrazione, Raccolta log, Gestione agenti, Gruppo agenti predefinito
2. Selezionare il computer agente.
3. Passare alla visualizzazione Connettori e fare clic sul pulsante di avvio della visualizzazione Stato e comando.

Lo stato dovrebbe essere in esecuzione.

Abilitare il controllo in CA Identity Manager

Per abilitare il controllo in CA Identity Manager

1. Aprire la console di gestione
`http://host:port//iam/immanage`
2. Accedere ad Environments (Ambienti), <Environment>, Advanced Setting (Impostazione avanzata), Auditing (Controllo).
3. Esportare le impostazioni esistenti e salvare il file.
4. Modificare il file salvato nel modo seguente e salvare le modifiche:
 - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
 - Aggiungere il profilo di controllo per i criteri delle password sotto l'ultimo profilo di controllo già definito:
`<AuditProfile objecttype="FWPASSWORDPOLICY"
auditlevel="BOTHCHANGED"/>`
5. Reimportare il file nella console di gestione ed effettuare una delle operazioni seguenti per attivare l'aggregazione delle informazioni di controllo:
 - Attività eseguite su un oggetto gestito dall'utente
 - Attività eseguite su un oggetto gestito dal gruppo
 - Attività eseguite su un oggetto gestito da criteri di password
6. Accedere al server CA Enterprise Log Manager mediante l'URL seguente:
`https://<host> : 5250/spin/calm/CALMSpindle.csp`
7. Per verificare i rapporti esistenti, accedere a Query e rapporti, Query, CA Identity Manager
Nota: è necessario che il server Enterprise Log Manager sia già configurato.
8. A seconda delle attività eseguite, aprire i rapporti predefiniti seguenti per verificare che gli eventi stiano arrivando:
 - L'attività Tutti gli eventi di sistema per Utente richiama CA Identity Manager - Tutti gli eventi di sistema filtrato per ID utente
 - L'attività Gestione account per Host richiama Gestione account per Host così com'è
 - L'attività Creazioni account per Account richiama Creazioni account per Account così com'è
 - L'attività Eliminazioni account per Account richiama Eliminazioni account per account così com'è
 - L'attività Blocchi account per Account richiama Blocchi account per account così com'è

- L'attività Attività di processo di certificazione per Host richiama CA Identity Manager - Attività di processo di certificazione per Host così com'è
- L'attività Attività di modifica criterio di password richiama CA Identity Manager - Attività di modifica criterio di password così com'è

Configurazione del server CA Enterprise Log Manager

Prima di configurare il server CA Enterprise Log Manager per la gestione, assicurarsi di quanto segue:

- È necessario disporre di credenziali EiamAdmin
- È necessario disporre di Adobe Flash Player versione 9.0.28 o superiore.

Una volta che il server CA Enterprise Log Manager è stato configurato, la funzionalità seguente diventa disponibile:

- Un singolo server CA Enterprise Log Manager o una gerarchia federata consumano più ambienti che producono eventi di controllo.
- È possibile implementare l'autorizzazione dei dati per sistemi remoti mediante il filtro di accesso ai dati di CA Enterprise Log Manager.

Per configurare il server CA Enterprise Log Manager

1. Accedere alla pagina di registrazione prodotto del server CA Enterprise Log Manager con credenziali di amministratore di CA Enterprise Log Manager mediante l'URL seguente:

`https://host:port/spin/calmap/products.csp`

2. Registrare il proprio ambiente di CA Identity Manager facendo clic sul pulsante Registra e fornendo il nome di certificato e la password.

Nota: ciascun ambiente deve avere dettagli di registrazione separati (nome certificato/password).

3. Accedere ad Amministrazione, Gestione utenti e accessi, New Data Access Filter (Nuovo filtro di accesso ai dati) e fornire un nome per il filtro da creare.
4. Proseguire con il passaggio successivo.
5. Lasciare l'opzione Tutte le Identità nell'impostazione Identità selezionate e proseguire con il passaggio successivo.
6. Creare un filtro di accesso facendo clic sul pulsante Nuovo filtro evento.

Configurare il filtro di accesso ai dati limitando il certificato creato al nome del computer/ambiente solo per i registri raccolti da CA Identity Manager. È possibile limitare il certificato anche per l'accesso alle informazioni di endpoint nativi solo per gli endpoint gestiti.

7. Salvare e chiudere.
8. Aprire Criteri di accesso facendo clic sul pulsante Open Access Policies (Apri criteri di accesso).
9. Selezionare Obligation Policies (Criteri di obbligo) e fare clic sull'unico criterio disponibile.
10. Rimuovere l'opzione Tutte le identità e aggiungere il nome del certificato.
11. Salvare il criterio.

12. Accedere alla console utente di Identity Manager e configurare la connessione di Enterprise Log Manager.

Configurazione della connessione Enterprise Log Manager

Utilizzare la schermata Configura la connessione Enterprise Log Manager per gestire le attività di connessione CA Enterprise Log Manager aggiunte di recente.

Di seguito sono descritti i campi presenti in questa schermata:

Nome connessione

Nome univoco utilizzato per il singolo oggetto gestito connessione CA ELM.

Il campo è di sola lettura.

Descrizione

Descrizione della connessione CA ELM.

Nome host

Nome host o indirizzo IP del server CA Enterprise Log Manager.

Campo obbligatorio.

Porta #

Porta di connessione del server CA Enterprise Log Manager.

Impostazione predefinita: 52520

Campo obbligatorio.

Certificato SSL firmato dall'Autorità di certificazione

Se selezionata, questa opzione consente di specificare il controllo rigido di un certificato SSL durante la connessione a CA Enterprise Log Manager.

Se si dispone di un certificato SSL autofirmato, ad esempio un certificato installato per impostazione predefinita in CA Enterprise Log Manager, non selezionare questa casella di controllo in quanto non esiste un percorso attendibile dell'autorità di certificazione.

Nome certificato

Nome del certificato CA Enterprise Log Manager da utilizzare per l'autenticazione.

Campo obbligatorio.

Certificate password (Password certificato)

Password di CA Enterprise Log Manager.

Campo obbligatorio.

Attributo

Non supportato. La versione viene recuperata durante il tentativo di salvare le informazioni di connessione come prova.

Eliminazione della connessione Enterprise Log Manager

Selezionare una connessione nell'elenco, quindi fare clic su Elimina. L'attività connessione CA Enterprise Log Manager viene eliminata.

Integrare i rapporti o le query aggiuntive di CA Enterprise Log Manager con CA Identity Manager

È possibile integrare i rapporti e le query aggiuntive di CA Enterprise Log Manager con CA Identity Manager mediante la scheda di visualizzazione Enterprise Log Manager. È possibile combinare i nuovi rapporti e le query con attività esistenti (comprese le procedure guidate) e nuove e, se necessario, si possono includere anche i dati federati di CA Enterprise Log Manager. Mediante la scheda di visualizzazione Enterprise Log Manager, è inoltre possibile applicare filtri alle informazioni recuperate. Questi filtri possono utilizzare:

- Valori costanti
- Attributi di oggetto gestiti
 - Ad esempio, fisici - ::MyPhysicalAttribute::
logici - ::|MyLogicalAttribute|::
- Qualsiasi campo come descritto da Grammatica evento comune (CEG) di CA Enterprise Log Manager
 - dest_username
 - dest_objectname
 - dest_uid
 - source_username
 - source_objectname
 - source_uid
 - ...

Configurazione della scheda di visualizzazione Enterprise Log Manager

Configurare la scheda di visualizzazione CA Enterprise Log Manager da visualizzare con qualsiasi o tutti i campi seguenti:

Nome

Nome assegnato alla scheda.

Tag

Identificatore della scheda univoco all'interno dell'attività. Questo deve iniziare con una lettera o un carattere di sottolineatura e contenere solo lettere, numeri o caratteri di sottolineatura. Il tag viene utilizzato principalmente per impostare valori dati tramite documenti XML o parametri HTTP.

Nascondi scheda

Impedisce la visualizzazione della scheda nell'attività. Questa opzione è utile per applicazioni che richiedono che la scheda sia nascosta mantenendo però l'accesso agli attributi presenti in essa.

Query Enterprise Log Manager

Consente di specificare che le query CA Enterprise Log Manager devono essere visualizzate.

Nota: è possibile specificare query Enterprise Log Manager oppure rapporto Enterprise Log Manager, ma non entrambe le opzioni.

Rapporto Enterprise Log Manager

Consente di specificare che i rapporti CA Enterprise Log Manager devono essere visualizzati.

Nota: è possibile specificare query Enterprise Log Manager oppure rapporto Enterprise Log Manager, ma non entrambe le opzioni.

ID Enterprise Log Manager

Consente di specificare l'ID per la query o il rapporto.

Includi dati federati

Include o esclude i dati federati di CA Enterprise Log Manager nei risultati. Questo campo è selezionato per impostazione predefinita.

Mostra prompt

Consente di specificare solo le query di prompt di CA Enterprise Log Manager. Questo campo è selezionato per impostazione predefinita.

Filtro

Consente di specificare le condizioni avanzate basate su SQL utilizzate per restringere i risultati restituiti dalle query o dai rapporti restituiti da CA Enterprise Log Manager. È possibile includere valori costanti e dinamici. Di seguito viene riportata un'espressione di esempio:

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username EQUAL ::logical.attribute.Y:: ))
```

Le operazioni supportate includono:

- uguale a (EQUAL)
- diverso da (NEQ)
- minore di (LESS)
- maggiore di (GREATER)
- minore di o uguale a (LEQ)
- maggiore di o uguale a (GREATEREQ)
- simile a (LIKE)
- non simile a (NOTLIKE)
- nel set (INSET)
- non nel set (NOTINSET)

Le congiunzioni supportate includono:

- AND
- OR

Le parentesi sono obbligatorie. Se il valore nella parte sinistra nell'espressione condizionale non ha l'indicatore "::" da entrambi i lati, il valore viene considerato una costante e viene inviato a CA Enterprise Log Manager così com'è.

Tabella Parameter/Value

Specificano i campi e i valori da utilizzare per l'ambito.

Vengono selezionate solo le query o i rapporti che corrispondono ai tag e alla logica dei tag dell'ambito.

Parametro

Consente di specificare i valori per i parametri di inizio, fine e limite. Sono supportati i parametri seguenti:

- Granularità (solo per tendenze)
- Ora di avvio
- Ora fine;
- Il primo gruppo di eventi è datato dopo (solo per gruppi di query)
- L'ultimo gruppo di eventi è datato dopo (solo per gruppi di query)

- L'ultimo gruppo di eventi è datato prima (solo per gruppi di query)
- Numero minimo di eventi per il gruppo (solo per gruppi di query)
- Numero massimo di eventi per il gruppo (solo per gruppi di query)

Capitolo 18: Ruoli di accesso

I ruoli di accesso rappresentano un ulteriore modo per concedere diritti in CA Identity Manager o in un'altra applicazione. Ad esempio, è possibile utilizzare i ruoli di accesso per completare le seguenti operazioni:

- Fornire l'accesso indiretto a un attributo utente
- Creare espressioni complesse
- Impostare un attributo in un profilo utente, utilizzato da un'altra applicazione per determinare i diritti

I ruoli di accesso sono analoghi ai criteri di identità, in quanto applicano un insieme di modifiche aziendali a un utente o a un gruppo di utenti. Tuttavia, quando si utilizza un ruolo di accesso per applicare modifiche aziendali, è possibile visualizzare a quali utenti si applicano le modifiche visualizzando i membri del ruolo di accesso.

Nella maggior parte dei casi, i ruoli di accesso non vengono associati alle attività.

Nota: quando CA Identity Manager si integra con CA SiteMinder, i ruoli di accesso possono anche fornire accesso ad applicazioni protette da CA SiteMinder. In questo caso, i ruoli di accesso comprendono attività di accesso. Per ulteriori informazioni, consultare il capitolo relativo all'integrazione con SiteMinder nella *Guida alla configurazione*.

Questa sezione contiene i seguenti argomenti:

[Gestione dei diritti mediante i ruoli di accesso](#) (a pagina 554)

[Esempio: Modifica indiretta dell'attributo di profilo](#) (a pagina 554)

[Creazione di un ruolo di accesso](#) (a pagina 555)

Gestione dei diritti mediante i ruoli di accesso

È possibile utilizzare ruoli di accesso per gestire i diritti. A tal fine, specificare le azioni di modifica da eseguire quando un utente viene aggiunto o rimosso come membro o amministratore di un ruolo.

Per utilizzare i ruoli di accesso, completare le operazioni seguenti:

1. Un amministratore crea un ruolo di accesso.
2. Nella scheda Membri, l'amministratore specifica se aggiungere o rimuovere azioni. In tal modo vengono determinate le azioni eseguite da CA Identity Manager quando il ruolo di accesso viene assegnato a un utente.
3. L'amministratore specifica i criteri di titolarità e amministrazione in base alle proprie esigenze, quindi inoltra l'attività per creare il ruolo di accesso.
4. Gli amministratori del ruolo di accesso assegnano il ruolo di accesso agli utenti.
5. CA Identity Manager completa le azioni di aggiunta specificate nel ruolo.

Esempio: Modifica indiretta dell'attributo di profilo

È possibile utilizzare i ruoli di accesso per apportare modifiche indirette a un attributo del profilo di un utente. Ad esempio, un'azienda potrebbe non desiderare che tutti gli utenti siano in grado di modificare direttamente il titolo di un altro utente. In tal caso, l'azienda può creare un ruolo di accesso per consentire la modifica del titolo. L'amministratore assegna tale ruolo agli utenti desiderati.

Per la modifica indiretta di un attributo, impostare le azioni di modifica per il ruolo di accesso. Quando un amministratore assegna il ruolo, l'azione di modifica consente di apportare una o più modifiche a un attributo del profilo dell'utente.

Per utilizzare un ruolo di accesso per la modifica indiretta di un attributo, procedere come segue:

1. Creare un ruolo di accesso.
2. Nella scheda Membri, selezionare la casella di controllo Gli amministratori possono aggiungere e rimuovere i membri di questo ruolo e fare clic sull'icona a freccia.
CA Identity Manager visualizza i campi Aggiungi azione e Rimuovi azione.
3. Selezionare un'azione della casella di riepilogo corrispondente.
CA Identity Manager mostra i campi aggiuntivi in base all'opzione selezionata.
4. Configurare le azioni di aggiunta o rimozione in base alle proprie necessità.
5. Selezionare la scheda Amministratore per specificare gli amministratori che possono aggiungere membri al ruolo di accesso in corso di creazione.

6. Selezionare la scheda Titolari per specificare gli amministratori che possono modificare la definizione del ruolo di accesso.
7. Fare clic su Invia per completare la creazione del ruolo di accesso.
8. Assegnare il ruolo di accesso agli utenti desiderati.

Creazione di un ruolo di accesso

La creazione di un ruolo di accesso si articola nei seguenti passaggi:

- [Inizio della procedura di creazione del ruolo di accesso](#) (a pagina 555)
- [Definizione del profilo di un ruolo di accesso](#) (a pagina 555)
- [Definizione dei criteri membri per un ruolo di accesso](#) (a pagina 556)
- [Definizione dei criteri di amministrazione per un ruolo di accesso](#) (a pagina 556)
- [Definizione delle regole proprietari per un ruolo di accesso](#) (a pagina 557)

Inizio della procedura di creazione del ruolo di accesso

1. Accedere ad Identity Manager utilizzando un account con un ruolo associato ad attività finalizzate alla creazione di ruoli di accesso.
2. Fare clic su Ruoli di accesso, Crea ruolo di accesso.
Scegliere le opzioni desiderate per creare un nuovo ruolo oppure una copia di un ruolo esistente. Se si seleziona Copia, cercare il ruolo desiderato.
3. Continuare con la sezione Definizione del profilo di un ruolo di accesso.

Definizione del profilo di un ruolo di accesso

Per definire il profilo di un ruolo di accesso

1. Immettere un nome ed una descrizione, quindi aggiungere eventuali attributi personalizzati definiti per il ruolo.
Nota: nella scheda Profilo è possibile definire attributi personalizzati con i quali specificare informazioni aggiuntive sui ruoli di accesso. Tali informazioni aggiuntive sono utili per facilitare le ricerche di ruoli in ambienti che presentano un numero elevato di ruoli.
2. Selezionare Attivato per rendere disponibile il ruolo subito dopo la creazione.
3. Continuare con la sezione [Definizione dei criteri membri per un ruolo di accesso](#) (a pagina 556).

Definizione dei criteri membri per un ruolo di accesso

Nella scheda Membri:

1. Fare clic su **Aggiungi** per definire i criteri membri.
2. (Facoltativo) Nella pagina **Criterio membri** definire una regola membri per identificare gli utenti in grado di utilizzare questo ruolo.

In questo modo, il ruolo verrà automaticamente assegnato agli utenti che soddisfano il criterio membri specificato.
3. Verificare che il criterio membri sia visualizzato nella scheda **Membri**.

Per modificare un criterio, fare clic sulla freccia sulla sinistra. Per rimuoverlo, fare clic sul segno meno.
4. Nella scheda **Membri** selezionare la casella di controllo **Gli amministratori possono aggiungere e rimuovere i membri di questo ruolo**.

Dopo aver abilitato questa funzionalità, definire l'azione di aggiunta e l'azione di rimozione. Queste azioni definiscono l'operazione eseguita quando un utente viene aggiunto o rimosso come membro del ruolo.
5. Continuare con la sezione [Definizione dei criteri di amministrazione per un ruolo di accesso](#) (a pagina 556).

Definizione dei criteri di amministrazione per un ruolo di accesso

Nella scheda Amministratori:

1. Per rendere disponibile l'opzione **Gestione amministratori**, selezionare la casella di controllo **Gli amministratori possono aggiungere o rimuovere gli amministratori di questo ruolo**.

Dopo aver abilitato questa funzionalità, definire le azioni eseguite quando un utente viene aggiunto o rimosso come amministratore del ruolo.
2. Nella scheda **Amministratori** aggiungere i criteri di amministrazione contenenti le regole relative ad amministrazione ed ambito, nonché i privilegi di amministratore. Ogni criterio deve disporre di almeno un privilegio (**Gestisci membri** o **Gestione amministratori**).

È possibile aggiungere più criteri di amministrazione con regole e privilegi diversi per gli amministratori che soddisfano la regola.
3. Per modificare un criterio, fare clic sulla freccia disponibile a sinistra. Per rimuovere il criterio, fare clic sull'icona raffigurante il segno meno.
4. Continuare con la sezione [Definizione delle regole proprietari per un ruolo di accesso](#) (a pagina 557).

Definizione delle regole proprietari per un ruolo di accesso

Nella scheda Proprietari:

1. Definire le regole proprietari che determinano gli utenti che possono modificare il ruolo.
2. Fare clic su Inoltra.

Viene visualizzato un messaggio indicante che l'attività è stata inoltrata. Prima di poter utilizzare il ruolo definito, potrebbe essere necessario attendere alcuni minuti.

Capitolo 19: Attività di sistema

Questa sezione contiene i seguenti argomenti:

[Attività di sistema predefinite](#) (a pagina 559)
[Aggiunta di utenti mediante il file alimentatore](#) (a pagina 560)
[Scheda Dettagli record dell'Utilità di caricamento](#) (a pagina 565)
[Scheda Mappatura azioni dell'Utilità di caricamento](#) (a pagina 565)
[Scheda Dettagli di notifica dell'utilità di caricamento](#) (a pagina 566)
[Conferma delle modifiche all'attività dell'Utilità di caricamento in blocco](#) (a pagina 567)
[Configurazione delle notifiche di posta elettronica per le attività in blocco](#) (a pagina 568)
[Pianificazione di un'attività dell'Utilità di caricamento in blocco](#) (a pagina 568)
[Modifica del file analizzatore per l'Utilità di caricamento in blocco](#) (a pagina 569)
[Supporto dei servizi Web per l'Utilità di caricamento in blocco](#) (a pagina 569)
[Gestione connessione JDBC](#) (a pagina 570)
[Gestori attributi logici](#) (a pagina 570)
[Dati casella di selezione](#) (a pagina 574)
[Schermata di attività Configura attributi di correlazione](#) (a pagina 574)
[Schermata attività Configurare il flusso di lavoro basato sul criterio globale per Eventi](#) (a pagina 575)
[Stato delle attività in CA Identity Manager](#) (a pagina 576)
[Pulitura delle attività inoltrate](#) (a pagina 593)
[Eliminazione di attività ricorrenti](#) (a pagina 598)
[Configurazione della connessione Enterprise Log Manager](#) (a pagina 599)
[Eliminazione della connessione Enterprise Log Manager](#) (a pagina 600)
[Gestione delle chiavi segrete](#) (a pagina 600)

Attività di sistema predefinite

CA Identity Manager comprende le attività seguenti, che facilitano la gestione di un ambiente CA Identity Manager da parte degli amministratori:

- **Attività Visualizza attività inoltrate**
Consente agli amministratori di visualizzare lo stato delle attività nell'ambiente. Rimuove anche le attività obsolete dalle schermate Visualizza attività inoltrate.
- **Attività Bulk Loader**
Consente di caricare file alimentatore utilizzati per manipolare un gran numero di oggetti gestiti in contemporanea.

- **Attività in blocco**
Esegue un'attività su un oggetto, ad esempio un utente, in base agli attributi dell'oggetto, come dipartimento, città, data di fine ecc. È possibile eseguire l'attività periodicamente, ad esempio ogni sabato.
È inoltre possibile utilizzare questa attività per apportare modifiche utente a livello di blocco.
- **Attività Dati casella di selezione**
Consente agli amministratori di caricare file utilizzati per popolare le opzioni in campi quali le caselle di selezione nelle attività di amministrazione.
- **Attività Gestore attributo logico**
Consente agli amministratori di gestire gli attributi logici, utilizzati per visualizzare gli attributi dell'archivio utente (detti attributi fisici) in un formato semplice da usare negli schermi delle attività.
- **Attività di gestione connessione JDBC**
Consente di configurare i dettagli di connessione al server di database in CA Identity Manager.
- **Attività di posta elettronica**
Gestisce i criteri di notifica di posta elettronica.

Aggiunta di utenti mediante il file alimentatore

La scheda Utilità di caricamento in blocco consente di caricare i file alimentatore utilizzati per la gestione simultanea di un numero elevato di oggetti. Ad esempio, la creazione di 1000 utenti nel sistema può essere eseguita in modo manuale oppure utilizzando il caricamento in blocco. Inoltre, è possibile mappare l'attività Bulk Loader su un processo del flusso di lavoro.

Il client dell'Utilità di caricamento in blocco corrisponde a un'utilità della riga di comando disponibile per l'elaborazione batch. Si raccomanda di utilizzare il client dell'Utilità di caricamento in blocco per gli ambienti cluster (ai fini del bilanciamento del carico). Il client dell'Utilità di caricamento in blocco è disponibile sul supporto dei componenti di provisioning.



Procedere come descritto di seguito:

1. [Consultare le considerazioni sull'Utilità di caricamento in blocco](#) (a pagina 561).
2. [Creare un file alimentatore CSV o XLS](#) (a pagina 563) e caricarlo.
3. [Configurare i dettagli dei record dell'Utilità di caricamento](#) (a pagina 565).
Questa scheda consente di specificare i campi Azione e Identificatore del file alimentatore.
4. [Specificare il mapping delle azioni dell'Utilità di caricamento](#) (a pagina 565).
Questa scheda consente di selezionare l'oggetto primario e di specificare le attività da eseguire per l'azione su un oggetto.
5. [Specificare i dettagli di notifica dell'Utilità di caricamento](#) (a pagina 566).
Questa scheda consente di selezionare gli utenti per certificare le modifiche dell'attività dell'Utilità di caricamento in blocco.
6. [Confermare e modificare l'avanzamento delle modifiche dell'attività dell'Utilità di caricamento in blocco](#) (a pagina 567).

Considerazioni sull'Utilità di caricamento in blocco

La scheda Utilità di caricamento in blocco consente di caricare i file alimentatore utilizzati per la gestione simultanea di un numero elevato di oggetti. Tenere in considerazione le operazioni seguenti durante l'utilizzo dell'Utilità di caricamento in blocco:

- Pianificare il caricamento in blocco di grandi dimensioni durante i periodi di bassa attività ad esempio, durante le ore notturne. I caricamenti in blocco di grandi dimensioni possono alterare le prestazioni. In alcuni casi, se il caricamento in blocco include un numero elevato di attività secondarie, il completamento delle attività inviate dagli utenti potrebbe essere eseguito solo una volta finalizzato il caricamento in blocco.
- Se il server diventa non disponibile durante un'attività a esecuzione prolungata, quale il caricamento di un gran numero di oggetti, è possibile riavviare l'attività nella scheda Visualizza attività inoltrate. Una volta riavviata, l'attività riprende dall'ultimo record eseguito correttamente.
- Se si utilizza LDAP come archivio utenti con Solaris, l'utilità di caricamento in blocco potrebbe bloccarsi durante l'importazione. Per risolvere questo problema, consultare la sezione relativa alla configurazione della connessione LDAP della *Guida alla configurazione* e applicare le impostazioni indicate.

- Se si utilizza l'Utilità di caricamento in blocco per importare un numero elevato di utenti, potrebbero verificarsi eccezioni di memoria esaurita. Per risolvere questo problema, modificare i seguenti parametri delle dimensioni heap di memoria:
 - -Xmx
 - -XX:maxPermSize

Nota: per ulteriori informazioni sulla modifica dei parametri di memoria, consultare la documentazione del server applicazioni in uso.
- L'utilizzo dell'Utilità di caricamento in blocco per numerosi oggetti gestiti, ad esempio per creare un numero elevato di utenti, può influire sulle prestazioni. Per migliorare le prestazioni, considerare i seguenti suggerimenti:
 - Se si utilizza la console utente per il caricamento in blocco, dividere un file CSV di grandi dimensioni in più file di dimensioni minori. Ad esempio, l'esecuzione di dieci operazioni di caricamento in blocco di 10.000 utenti è più veloce di un unico caricamento in blocco di 100.000 utenti.

Nota: un file CSV con più di 10.000 voci può causare problemi nel sistema.
 - Limitare il numero di attività dell'utente che esegue il caricamento in blocco. Ad esempio, è possibile ottenere migliori prestazioni quando l'amministratore che ha avviato il caricamento in blocco ha poche attività. Quando l'amministratore ha molte attività, in CA Identity Manager è necessario eseguire verifiche più estese sulle autorizzazioni, il che può influire sulle prestazioni.
 - Limitare il numero di criteri di Policy Xpress, associate alle modifiche in blocco, che implicano il provisioning. Inoltre, considerare la creazione di criteri semplici di Policy Xpress, che non influiscono sulle prestazioni così come i criteri complessi durante un'operazione di caricamento in blocco.
 - Verificare di avere a disposizione sufficienti risorse di sistema.

Limitazione della convalida dei dati per migliorare prestazioni di caricamento in blocco

Un'attività di amministrazione generalmente include più schede. Per impostazione predefinita, le operazioni in blocco convalidano i dati in ciascuna scheda di un'attività.

La convalida può influire sulle prestazioni delle operazioni in blocco. Per migliorare le prestazioni, è possibile disabilitare la convalida dei dati per le schede di attività, se la convalida non è necessaria.

Procedere come descritto di seguito:

1. Accedere alla console utente come utente con privilegi per modificare le attività di amministrazione.
2. Selezionare Attività, Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
3. Cercare e selezionare l'attività che si applica nell'operazione in blocco.

4. Selezionare Schede, quindi selezionare la scheda da modificare.
5. Selezionare Non convalidare nell'operazione in blocco, quindi fare clic su OK.
6. Ripetere i passaggi 4 e 5 per ciascuna scheda che non richiede la convalida dei dati.
7. Fare clic su Inoltra.

La convalida dei dati viene disabilitata per le schede modificate.

Limitazione della logica aziendale personalizzata

L'inclusione della logica aziendale personalizzata, tra cui gestori attività di logica aziendale e listener di evento, nelle attività utilizzate in operazioni in blocco può influire sulle prestazioni.

Per migliorare le prestazioni, disabilitare la logica aziendale personalizzata nelle operazioni di caricamento in blocco.

Procedere come descritto di seguito:

1. Aprire la console di gestione.
2. Selezionare l'ambiente adatto che include il listener di evento o il gestore attività di logica aziendale.
3. Selezionare Impostazioni avanzate, Gestori attività di logica aziendale (se applicabile).
4. Impostare il valore della proprietà UseInBulkOperation su false, quindi fare clic su Salva.
5. Ripetere il passaggio 4 per i listener di evento.
6. Una volta completate le modifiche per i gestori attività di logica aziendale e i listener di evento, riavviare l'ambiente.

Creazione di un file alimentatore

I file dell'Utilità di caricamento in blocco consentono di automatizzare le azioni ripetute eseguite su un numero elevato di oggetti gestiti. Quando un file alimentatore viene caricato, il sistema analizza ed esegue la lettura de file alimentatore.

Il file alimentatore deve presentare l'estensione CSV o XLS e le proprietà riportate di seguito.

- Il file deve contenere un'intestazione che specifica gli attributi fisici e logici o i nomi degli attributi noti di un oggetto gestito.
- La riga di intestazione deve includere una colonna che indichi l'azione da eseguire sui record.

- Ogni riga del file alimentatore è detta record. I record contengono i valori di ognuno degli attributi specificati dalla riga di intestazione. Le opzioni seguenti rappresentano valori accettabili per un attributo:
 - Valore: l'attributo viene impostato sul valore specificato.
 - Valore;Valore;Valore: l'attributo viene impostato sull'attributo con più valori specificato.
 - " " (vuoto): l'attributo non viene modificato.
 - NULL: l'attributo viene eliminato. Per impostazione predefinita la sequenza di eliminazione viene impostata su NULL, ma può essere modificata nella schermata Ricerca caricamento file dell'Utilità di caricamento in blocco.

Nota: per utilizzare un marcatore hash (#) nel file alimentatore, racchiuderlo tra virgolette doppie, ad esempio utente#1 va specificato come "utente#1".

Importante. Il file alimentatore deve essere salvato con codifica UTF-8.

Esempio di file alimentatore per creare utenti

Con questo esempio di file alimentatore è possibile creare utenti con determinati attributi obbligatori.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

Nel codice riportato sopra, il file alimentatore ha le proprietà seguenti:

Intestazione

La prima riga del codice è la riga di intestazione. La riga di intestazione presenta gli attributi fisici o gli attributi noti dell'oggetto gestito Utente.

Azione

La colonna action identifica l'attività da eseguire per ciascun record. Ad esempio, il file precedente specifica l'esecuzione di un'azione "crea" per il Nome John.

Esempio di file alimentatore per abilitare gli utenti

Questo esempio di file alimentatore modifica il valore dell'attributo logico |enabled|. Si specifica l'attributo logico nell'intestazione e il valore (in questo caso, true o false) in ciascuna voce utente nel file.

```
action,%USER_ID%,|enable|
MODIFY,user1,false
MODIFY,user2,true
```

Scheda Dettagli record dell'Utilità di caricamento

Nella scheda Dettagli record dell'Utilità di caricamento viene visualizzata una breve anteprima dei record disponibili nel file alimentatore. Nella tabella di anteprima sono visualizzati un massimo di 5 record. La tabella di anteprima consente agli utenti di accertarsi di star caricando il file corretto. Inoltre, questa scheda consente di identificare l'azione che si desidera eseguire sugli oggetti gestiti specificati nel file alimentatore. È necessario completare i campi seguenti:

Quale campo rappresenta l'azione da eseguire sull'oggetto?

Consente di identificare i campi del file alimentatore che indicano l'azione da eseguire sugli oggetti gestiti. Ad esempio, è possibile utilizzare un file alimentatore con un campo "azione" che assume i valori Crea, Modifica ed Elimina. È necessario eseguire il mapping di ognuna di queste azioni su un'attività di amministrazione in [Mappatura azioni dell'Utilità di caricamento](#) (a pagina 565).

Quale campo verrà usato per identificare l'oggetto in modo univoco?

Consente di identificare il campo del file alimentatore che può identificare in modo univoco l'oggetto primario.

Nota: se il file alimentatore presenta un'intestazione non valida, i relativi record non verranno visualizzati nella scheda Dettagli record dell'Utilità di caricamento. In caso di intestazioni non valide, selezionare un altro file alimentatore. Se il file alimentatore contiene alcuni record non validi, lo stato dettagliato del caricamento sarà presente in Visualizza attività inoltrate nella scheda Sistema.

Scheda Mappatura azioni dell'Utilità di caricamento

La scheda Mappatura azioni dell'Utilità di caricamento consente di selezionare un oggetto primario su cui verranno eseguite le azioni specificate nel file alimentatore. Per l'oggetto primario selezionato è inoltre necessario mappare le azioni dal file alimentatore alle attività di amministrazione.

Qual è l'oggetto primario?

Consente di identificare l'oggetto primario che verrà modificato in CA Identity Manager con il file alimentatore. È possibile selezionare qualunque oggetto primario tra i seguenti:

- Utente
- Gruppi
- Organizzazione

Selezionare un'attività da eseguire per l'azione

Consente di identificare le attività di amministrazione da eseguire per ogni azione specificata nel file alimentatore, ad esempio attività di eliminazione e modifica.

Nota: sarà necessario mappare tutte le azioni contenute nel file alimentatore su un'attività di amministrazione. Le attività di amministrazione visualizzate in questo campo, inoltre, dipendono dall'oggetto primario selezionato. Se ad esempio si seleziona "Utente" come oggetto primario, verranno visualizzate solo le attività di amministrazione correlate a "Utente".

Selezionare un'attività per l'oggetto non esistente dell'azione

Consente di identificare le attività di amministrazione alternative da eseguire per un'azione specificata nel file alimentatore, nell'eventualità che l'oggetto gestito non esista ancora in CA Identity Manager, ad esempio l'attività di creazione.

Scheda Dettagli di notifica dell'utilità di caricamento

Importante. Per impostazione predefinita, questa scheda non è inclusa nella procedura guidata dell'Utilità di caricamento in blocco. È necessario aggiungerla manualmente modificando l'attività dell'Utilità di caricamento in blocco e aggiungere la scheda Dettagli di notifica dell'utilità di caricamento. Inoltre, questa scheda richiede l'abilitazione del flusso di lavoro nell'ambiente.

La scheda Dettagli di notifica dell'utilità di caricamento consente di selezionare i manager di certificazione per l'attività dell'Utilità di caricamento in blocco. Al termine di un'attività dell'Utilità di caricamento in blocco, CA Identity Manager genera una notifica sull'Utilità di caricamento in blocco per tutti i manager di certificazione configurati per l'attività. Questa notifica viene visualizzata nella scheda Pagina principale in Notifiche dell'Utilità di caricamento in blocco. Facendo clic sulla notifica vengono visualizzati i dettagli per le attività avviate dall'operazione di caricamento in blocco. I manager di certificazione possono quindi esaminare e confermare le modifiche elencate nelle notifiche.

Nota: per specificare un elenco di manager della certificazione, utilizzare uno dei resolver partecipanti nell'elenco a discesa. Per ulteriori informazioni sui resolver partecipanti, consultare la sezione relativa al flusso di lavoro di questa guida.

Conferma delle modifiche all'attività dell'Utilità di caricamento in blocco

Le notifiche dell'Utilità di caricamento in blocco contengono le informazioni relative a tutte le modifiche avviate dall'attività dell'Utilità. I manager di certificazione possono rivedere e confermare le modifiche avviate da un'attività dell'Utilità di caricamento in blocco.

Per rivedere e confermare le modifiche delle attività dell'Utilità di caricamento in blocco

1. Accedere alla console utente come utente elencato come gestore di certificazione per un'attività dell'Utilità di caricamento in blocco.
2. Raggiungere la Pagina principale, Visualizza notifiche dell'Utilità di caricamento in blocco.
3. Selezionare le Notifiche dell'Utilità di caricamento in blocco che si desidera rivedere.

Viene visualizzata la schermata Gestisci notifiche dell'Utilità di caricamento in blocco e un elenco di tutte le modifiche avviate dalle attività dell'Utilità di caricamento in blocco.

Da questa schermata è possibile eseguire le seguenti operazioni:

- Per rivedere i dettagli di un'attività specifica per un oggetto di creazione o modifica, fare clic sul collegamento nella colonna Descrizione.
 - Se sono presenti violazioni di conformità, o se si desidera rimuovere un ruolo aggiunto a un utente, è possibile modificare l'utente direttamente dalla schermata di notifica facendo clic sull'icona Modifica accanto all'ID utente.
 - Per rivedere i ruoli aggiunti a un utente, fare clic sul collegamento ipertestuale nella colonna Assegnazioni ruoli richiesti associata con l'ID utente.
4. Dopo aver esaminato tutte le modifiche per un oggetto specifico, selezionare la casella di controllo Conferma per tale oggetto.
 5. Una volta terminato il rilevamento delle modifiche, fare clic su Conferma per rimuovere tutte le notifiche di modifica selezionate dall'elenco.

Nota: è possibile selezionare Conferma tutto per confermare tutte le modifiche in una notifica dell'Utilità di caricamento in blocco. Questa operazione consente di eliminare le Notifiche dell'Utilità di caricamento in blocco dalla scheda Pagina principale. Inoltre, è possibile selezionare la casella di controllo nella parte superiore della colonna Conferma per selezionare tutte le notifiche di modifica nella schermata, e confermare le modifiche schermata per schermata.

Quando tutte le modifiche utente associate a un'attività dell'Utilità di caricamento in blocco sono state confermate, le Notifiche dell'Utilità di caricamento in blocco non vengono più visualizzate nella scheda Pagina principale.

Configurazione delle notifiche di posta elettronica per le attività in blocco

In alcuni ambienti, le notifiche di posta elettronica delle operazioni in blocco sono configurate per impostazione predefinita. Per verificare che le notifiche di posta elettronica delle operazioni in blocco siano configurate nel sistema in uso, accedere a Sistema, Posta elettronica, Visualizza messaggi di posta elettronica e cercare il termine "bulk".

Se le notifiche di posta elettronica non sono configurate nell'ambiente in uso, configurare il messaggio di posta elettronica che viene inviato al completamento di un'operazione in blocco.

Procedere come descritto di seguito:

1. Nella console utente Fare clic su Sistema, Posta elettronica, Crea messaggio di posta elettronica.
2. Completare i seguenti campi obbligatori nella scheda Profilo:
3. Nella scheda Invia messaggi con stato, completare le operazioni seguenti:
 - a. Selezionare Completamento attività nel primo campo.
 - b. Selezionare Utilità di caricamento in blocco nel secondo campo.
4. Completare le schede Destinatari e Contenuto e fare clic su Invia.

Le notifiche di posta elettronica vengono configurate per le attività dell'Utilità di caricamento in blocco.

Pianificazione di un'attività dell'Utilità di caricamento in blocco

È possibile pianificare attività dell'Utilità di caricamento in blocco nel sistema. Per pianificare l'attività dell'Utilità di caricamento in blocco, [aggiungere una scheda di pianificazione](#) (a pagina 63) all'attività.

Modifica del file analizzatore per l'Utilità di caricamento in blocco

Per modificare l'analizzatore utilizzato per l'analisi dei file alimentatori, configurare l'attività di amministrazione corrispondente.

Modifica dell'attività di amministrazione dell'Utilità di caricamento in blocco

1. Accedere a Ruoli e attività, Attività di amministrazione, Gestisci attività di amministrazione.
2. Cercare l'attività dell'Utilità di caricamento in blocco.
3. Selezionare l'attività dell'Utilità di caricamento in blocco e fare clic su Seleziona.
4. Selezionare la scheda Cerca per l'attività dell'Utilità di caricamento in blocco.
5. Fare clic su Sfoglia per individuare gli schermi di ricerca.
Verrà visualizzato l'elenco degli schermi di ricerca disponibili.
6. Selezionare una schermata di profilo di ricerca e fare clic su Modifica.
Verranno visualizzati i dettagli della schermata di ricerca.
7. (Facoltativo) Modificare il Nome analizzatore pienamente qualificato.

Il Nome analizzatore pienamente qualificato deve corrispondere al nome del file analizzatore.

Nota: per ulteriori informazioni sulla creazione di un analizzatore personalizzato CSV, consultare la documentazione Java relativa alla classe FeederParser. Se si utilizza JBoss come server applicazioni e si crea un analizzatore personalizzato, il file dell'analizzatore personalizzato deve essere contenuto all'interno della directory `iam_im.ear/user_console_war/WEB-INF/classes`.

8. Fare clic su OK.

Supporto dei servizi Web per l'Utilità di caricamento in blocco

L'Utilità di caricamento in blocco contiene un'API dei servizi Web che può essere richiamata mediante l'interfaccia TEWS (Task Execution Web Service) di CA Identity Manager. TEWS consente alle applicazioni client di inoltrare attività remote per l'esecuzione in CA Identity Manager. Questa interfaccia implementa gli standard aperti WSDL e SOAP per fornire l'accesso remoto a CA Identity Manager.

CA Identity Manager include esempi di client Java che descrivono la chiamata dell'Utilità di caricamento in blocco come servizio Web. Gli esempi Java si trovano nel file sorgente indicato di seguito:

`admin_tools\samples\WebService\Axis\optional\ObjectsFeeder.java`

I dati di esempio e la documentazione necessaria per la chiamata dell'Utilità di caricamento in blocco come servizio Web sono disponibili nella directory seguente:

`admin_tools\samples\Feeder\`

Nota: per ulteriori informazioni, consultare la guida *Programming Guide for Java*.

Gestione connessione JDBC

Le informazioni per i rapporti di CA Identity Manager possono provenire da varie origini e ogni rapporto deve essere associato a un'origine dati specifica, a seconda delle informazioni da includere.

Per impostare diverse origini dati per i rapporti (ad esempio un database di controllo o un database di persistenza delle attività), creare un oggetto di connessione gestita in CA Identity Manager. Dopo aver creato la connessione è possibile associare un rapporto con un oggetto connessione gestita specifico modificando l'attività del rapporto e impostando l'oggetto di connessione per il rapporto nella scheda di ricerca dell'attività del rapporto.

Creazione di una connessione JDBC

Procedere come segue per fornire dettagli di connessione in CA Identity Manager.

Creazione di una connessione JDBC

1. Fare clic su Sistema, Gestione connessione JDBC, Crea connessione JDBC.
2. Creare un nuovo oggetto connessione oppure selezionare un oggetto connessione basato su una specifica origine dati JNDI.
3. Compilare tutti i campi necessari e fare clic su Inoltra.

Verrà creata una nuova connessione JDBC.

Gestori attributi logici

Gli attributi logici di CA Identity Manager consentono di visualizzare gli attributi dell'archivio utenti (detti attributi fisici) in un formato semplice da usare nelle schermate delle attività. Gli amministratori di CA Identity Manager utilizzano le schermate delle attività per eseguire funzioni in CA Identity Manager. Gli attributi logici non esistono in un archivio utenti. In genere, rappresentano uno o più attributi fisici per semplificarne la presentazione. Ad esempio, l'attributo logico data può rappresentare gli attributi fisici mese, giorno e anno.

Gli attributi logici vengono elaborati dai relativi gestori, oggetti Java scritti mediante l'API dell'attributo logico. (Consultare la *Guida alla programmazione per Java*.) Ad esempio, quando viene visualizzato lo schermo di un'attività, un gestore attributo logico può convertire i dati degli attributi fisici in dati dell'attributo logico, visualizzati nello schermo dell'attività. È possibile utilizzare gli attributi logici predefiniti e i relativi gestori forniti con CA Identity Manager oppure crearne di nuovi mediante l'API dell'attributo logico.

Nota: per ulteriori informazioni sugli attributi logici, consultare la *Guida alla programmazione per Java*.

Nella console utente, la categoria Ambiente contiene attività per la gestione dei gestori attributi logici. L'elenco comprende i gestori predefiniti forniti con CA Identity Manager ed eventuali gestori personalizzati definiti presso la sede dell'utente.

Dalla categoria di attività Ambiente, è possibile effettuare le operazioni seguenti:

- Creazione di un nuovo gestore attributo logico con CA Identity Manager
- Copia di un gestore
- Eliminazione di un gestore
- Modifica della configurazione di un gestore esistente

Nota: per cambiare l'ordine di esecuzione dei gestori attributi logici, utilizzare la console di gestione.

Creazione di un gestore attributo logico

Come creare un gestore attributo logico

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nella schermata Crea gestore attributo logico, selezionare Crea gestore attributo logico standard e fare clic su OK.
3. Nella schermata Crea gestore attributo logico, configurare le impostazioni del gestore attributo logico.
Per una descrizione di ogni campo, fare clic sul collegamento ? in questa schermata.
4. Fare clic su Inoltra.
Il gestore viene aggiunto all'elenco di gestori nella schermata Gestori attributi logici.

Nota: non è necessario riavviare il server di applicazione dopo aver configurato i gestori attributi logici mediante la Console utente.

Copia di un gestore attributo logico

Come copiare un gestore attributo logico

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nello schermata Crea gestore attributo logico, selezionare Crea una copia di una definizione del gestore attributo logico e fare clic su Cerca.
3. Selezionare un gestore attributo logico, ad esempio ConfirmPasswordHandler, e fare clic su OK.
4. Nella schermata Crea gestore attributo logico, configurare le impostazioni del gestore attributo logico.
Per una descrizione di ogni campo, fare clic sul collegamento ? in questa schermata.
5. Fare clic su Inoltra.

Il gestore viene aggiunto all'elenco di gestori nella schermata Gestori attributi logici.

Nota: non è necessario riavviare il server di applicazione dopo aver configurato i gestori attributi logici mediante la Console utente.

Creazione di un gestore attributo logico ForgottenPasswordHandler

Il gestore attributo logico ForgottenPasswordHandler utilizza attributi logici separati per:

- configurazione
- domande e risposte di runtime.

Come creare un gestore attributo logico ForgottenPasswordHandler

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nella schermata Crea gestore attributo logico, selezionare Crea gestore attributo logico standard e fare clic su Cerca.
3. Selezionare ForgottenPasswordHandler e fare clic su OK.
4. Nella schermata Crea gestore attributo logico: ForgottenPasswordHandler, configurare le impostazioni del gestore attributo logico.
Per una descrizione di ogni campo, fare clic sul collegamento ? in questa schermata.
5. Fare clic su Inoltra.

Il gestore viene aggiunto all'elenco di gestori nella schermata Gestori attributi logici.

Nota: non è necessario riavviare il server di applicazione dopo aver configurato i gestori attributi logici mediante la Console utente.

Eliminazione di un gestore attributo logico

Come eliminare un gestore attributo logico

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nella schermata Elimina gestore attributo logico, selezionare la casella di controllo a sinistra di ciascun attributo logico da eliminare.
3. Fare clic su Seleziona.
In CA Identity Manager viene visualizzato un messaggio di conferma.
4. Fare clic su Sì per confermare l'eliminazione.

Modifica di un gestore attributo logico

Come modificare un gestore attributo logico

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nella schermata Modifica gestore attributo logico, selezionare il gestore da modificare e fare clic su Seleziona.
3. Selezionare un gestore attributo logico, ad esempio ConfirmPasswordHandler, e fare clic su OK.
4. Nella schermata Modifica gestore attributo logico, configurare le impostazioni del gestore attributo logico.
Per una descrizione di ogni campo, fare clic sul collegamento ? in questa schermata.
5. Fare clic su Inoltra.

Nota: non è necessario riavviare il server di applicazione dopo aver configurato i gestori attributi logici mediante la Console utente.

Visualizzazione di un gestore attributo logico

Come visualizzare un gestore attributo logico

1. Accedere a Sistema, Attributi logici, Crea gestore attributo logico.
2. Nella schermata Visualizza gestore attributo logico, selezionare il gestore da visualizzare e fare clic su Seleziona.
3. Visualizzare le proprietà del gestore attributo logico e fare clic su Chiudi.

Dati casella di selezione

È possibile popolare le opzioni disponibili nei seguenti campi:

- Casella di controllo selezione multipla
- Casella a discesa
- Casella combinata a discesa
- Selezione multipla
- Selettore opzione
- Casella combinata selettore opzione
- Selezione singola pulsante di opzione
- Selezione singola

Queste opzioni sono archiviate nei file XML di selezione dei dati delle caselle. Ad esempio, è possibile utilizzare i file XML Dati casella di selezione per popolare le opzioni di una casella a discesa Città o Stato su una scheda Profilo per l'attività Crea utente.

È inoltre possibile utilizzare questo tipo di file XML per configurare una dipendenza tra due campi in un'attività di amministrazione. Ad esempio, le opzioni disponibili nel campo Città possono dipendere dall'opzione scelta dall'utente nel campo Stato.

Nota: per ulteriori informazioni sui dati della casella di selezione, consultare la *User Console Design Guide*.

Schermata di attività Configura attributi di correlazione

Questo argomento si applica solo a CA CloudMinder.

Usare la schermata di attività Configura attributi di correlazione per configurare le regole di correlazione per l'ambiente.

CA Identity Manager è in grado di leggere i parametri di configurazione memorizzati e di sincronizzare periodicamente la versione della memoria con la versione di database del DSA comune. Poiché gli attributi di correlazione sono specifici per titolare, il server di provisioning legge gli attributi di correlazione dal DSA del titolare corrispondente durante un'operazione Esplora e Correla. Le regole di correlazione aggiornate hanno effetto immediato senza dover aspettare il tempo di aggiornamento parametri.

Schermata attività Configurare il flusso di lavoro basato sul criterio globale per Eventi

L'attività Configurare il flusso di lavoro basato sul criterio globale per Eventi consente agli amministratori di configurare il flusso di lavoro basato o non basato su criterio per tutti gli eventi dell'ambiente corrente. Facendo clic sull'attività viene visualizzato il mapping predefinito degli eventi alle definizioni dei processi del flusso di lavoro. È possibile modificare tutti i mapping degli eventi e aggiungere nuovi mapping per gli eventi non configurati.

Configurare il flusso di lavoro basato sul criterio globale per Eventi

Processi di flusso associati a eventi in questo ambiente.

Nome evento	Processo del flusso di lavoro
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
CertifyRoleEvent	CertifyRoleApproveProcess
CreateGroupEvent	CreateGroupApproveProcess
CreateOrganizationEvent	CreateOrganizationApproveProcess
CreateUserEvent	CreateUserApproveProcess
DeleteGroupEvent	DeleteGroupApproveProcess
DeleteOrganizationEvent	DeleteOrganizationApproveProcess
DeleteUserEvent	DeleteUserApproveProcess
ModifyOrganizationEvent	ModifyOrganizationApproveProcess
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
SelfRegisterUserEvent	SelfRegistrationApproveProcess

Aggiungi nuovi mapping

Evento:

Di seguito sono descritti i campi presenti in questa schermata:

Processi di flusso associati a eventi in questo ambiente.

Consente di specificare i processi del flusso di lavoro associati ai criteri di approvazione.

Aggiungi nuovi mapping

Consente di specificare un criterio di approvazione da mappare a un processo del flusso di lavoro.

Pulsante Aggiungi

Consente di aggiungere il nuovo mapping.

Aggiungendo o modificando un mapping viene visualizzata la schermata di mapping del flusso di lavoro, in cui è possibile selezionare i mapping dei processi e i criteri di approvazione. Il comportamento è analogo a quello della configurazione del flusso di lavoro del livello evento. Facendo clic sul pulsante Aggiungi nella pagina Workflow Mappings (Mapping del flusso di lavoro) viene visualizzata un'altra pagina in cui è possibile configurare un criterio di approvazione.

Ulteriori informazioni

[Configurazione di un flusso di lavoro basato su criterio per gli eventi](#) (a pagina 331)

[Modalità di configurazione di un criterio di approvazione](#) (a pagina 334)

Stato delle attività in CA Identity Manager

Gli amministratori possono tenere traccia dello stato delle attività di CA Identity Manager inoltrate per l'elaborazione. CA Identity Manager offre i seguenti metodi per visualizzare lo stato delle attività:

■ Scheda Visualizza attività inoltrate

Questa scheda consente di cercare e visualizzare le attività di CA Identity Manager inoltrate per l'elaborazione.

Gli amministratori possono visualizzare i dettagli delle attività ad alto livello o a livelli più approfonditi.

La scheda Visualizza attività inoltrate è inclusa in due attività predefinite:

- Visualizza attività personali inoltrate

Consente agli amministratori di ricercare e visualizzare informazioni relative alle attività da loro inoltrate per l'elaborazione.

- Visualizza attività inoltrate

Consente agli amministratori di ricercare e visualizzare informazioni relative alle attività inoltrate per l'elaborazione da altri amministratori.

■ Scheda Cronologia utente

Questa scheda, che può essere aggiunta alle attività relative agli utenti, come Visualizza utente o Modifica utente, consente agli amministratori di visualizzare le informazioni riportate di seguito per un utente selezionato:

- Attività eseguite sull'utente.
- Attività eseguite dall'utente.
- Approvazioni del flusso di lavoro eseguite dall'utente

■ Rapporti

I rapporti di CA Identity Manager consentono di rilevare lo stato attuale di un ambiente CA Identity Manager. È possibile utilizzare tali informazioni per garantire conformità con criteri aziendali interni o con normative esterne.

In Rapporti vengono fornite ulteriori informazioni sull'impostazione e l'utilizzo dei rapporti.

■ Registri

Visualizzano le informazioni relative a tutti i componenti di un'installazione di CA Identity Manager e forniscono dettagli su tutte le operazioni in CA Identity Manager.

Per ulteriori informazioni sui registri di CA Identity Manager, consultare la *Guida alla configurazione*.

Determinazione dello stato delle attività con CA Identity Manager

Un'*attività* è una funzione amministrativa eseguibile da un utente in CA Identity Manager. Le attività includono *eventi*, azioni eseguite da CA Identity Manager per completare l'attività. Un'attività può includere più eventi. Ad esempio, l'attività Crea utente può includere eventi che comportano la creazione del profilo dell'utente, la sua aggiunta a un gruppo e l'assegnazione di ruoli.

Attività ed eventi di CA Identity Manager possono essere associati a un processo del flusso di lavoro che determina in che modo vengono eseguite le azioni richieste in CA Identity Manager e altre logiche aziendali personalizzate. Le attività possono essere anche associate con altre attività, dette attività nidificate. In questo caso, in CA Identity Manager le attività nidificate vengono elaborate con l'attività originale.

Lo stato di un'attività dipende dallo stato degli eventi ad essa associati, dei processi del flusso di lavoro, delle attività nidificate e della logica aziendale personalizzata.

Visualizzazione delle attività inoltrate

CA Identity Manager include la funzionalità Visualizza attività inoltrate che fornisce informazioni sulle attività nell'ambiente CA Identity Manager. Questa funzionalità consente di cercare e visualizzare informazioni generali sulle azioni eseguite da CA Identity Manager. Le schermate dei dettagli forniscono ulteriori informazioni su ciascuna attività ed evento.

A seconda dello stato dell'attività, è possibile utilizzare l'opzione Visualizza attività inoltrate per annullare o inoltrare nuovamente l'attività.

La funzionalità Visualizza attività inoltrate consente di tenere traccia dell'elaborazione di un'attività dall'inizio alla fine. Ad esempio, se un'attività di CA Identity Manager include l'assegnazione di un ruolo di provisioning e tale assegnazione attiva la creazione di account in altri sistemi, la scheda Visualizza attività inoltrate visualizza tutti i dettagli dell'attività originale e quelli relativi alle operazioni di creazione degli account.

La funzionalità Visualizza attività inoltrate include dettagli sulle operazioni eseguite nel sistema. Tali operazioni possono essere il risultato di un evento di CA Identity Manager, ad esempio EnableUserEvent. Le notifiche inviate dal server di provisioning sono raggruppate sotto questo evento. L'opzione Visualizza attività inoltrate mostra un messaggio che indica che le notifiche sono In corso fino a quando non viene inviata la notifica di conclusione. Lo stato del messaggio visualizzato verrà quindi modificato in Completato.

Per impostazione predefinita, CA Identity Manager include in due attività la scheda Visualizza attività inoltrate:

- Visualizzazione delle attività inoltrate
- Visualizza attività personali inoltrate

Ricerca di attività inoltrate

Eseguire le operazioni seguenti per cercare le attività inoltrate.

Per eseguire la ricerca di attività inoltrate:

1. Fare clic su Sistema, Visualizza attività inoltrate.
Viene visualizzata la pagina Visualizza attività inoltrate.
2. Specificare i criteri di ricerca, immettere il numero di righe da visualizzare e fare clic su Cerca.

Vengono visualizzate le pagine che soddisfano i criteri di ricerca specificati.

Nota: per ulteriori informazioni sulla procedura da utilizzare per specificare gli attributi nei criteri di ricerca, consultare la sezione [Attributi di ricerca per la visualizzazione di attività inoltrate](#) (a pagina 579).

Attributi di ricerca per la visualizzazione di attività inoltrate

Per consultare le attività inoltrate per l'elaborazione è possibile utilizzare la funzione di ricerca in Visualizza attività inoltrate. La ricerca di attività può basarsi sui criteri seguenti:

Iniziato da

Identifica come criterio di ricerca il nome dell'utente che ha iniziato l'attività. Le ricerche saranno basate sul nome utente. Per essere certi di immettere un nome utente valido, utilizzare il pulsante Convalida.

Attività di approvazione eseguite da

Identifica come criterio di ricerca il nome del revisore dell'attività. Le ricerche saranno basate sul nome utente. Per essere certi di immettere un nome utente valido, utilizzare il pulsante Convalida.

Nota: se viene selezionato il criterio Attività di approvazione eseguite da per filtrare le attività, viene attivato per impostazione predefinita anche il criterio Mostra attività di approvazione.

Nome attività

Identifica come criterio di ricerca il nome dell'attività. È possibile definire meglio la ricerca specificando condizioni quali "uguale a", "contiene", "inizia con" o "finisce con" il valore del campo Posizione nome attività. Ad esempio, è possibile specificare il criterio di ricerca "nome attività è uguale a Crea utente" selezionando la condizione uguale a e immettendo Crea utente nel campo di testo.

Stato attività

Identifica come criterio di ricerca lo stato dell'attività. Per selezionare lo stato dell'attività, attivare Dove è presente lo stato dell'attività uguale a e selezionare la condizione. Per limitare ulteriormente la ricerca, è possibile utilizzare le condizioni seguenti:

- Completato
- In corso
- Non riuscito
- Rifiutato
- Parzialmente completato
- Operazione interrotta
- Pianificato

Nota: per ulteriori informazioni, vedere [Descrizione dello stato dell'attività](#) (a pagina 581).

Priorità di attività

Identifica come criterio di ricerca la priorità dell'attività. Per selezionare la priorità dell'attività, attivare Dove è presente la priorità dell'attività uguale a e selezionando la condizione. Per limitare ulteriormente la ricerca, è possibile utilizzare le condizioni seguenti:

Bassa

Specifica la ricerca di attività con priorità bassa.

Media

Specifica la ricerca di attività con priorità media.

Alta

Specifica la ricerca di attività con priorità alta.

Eseguito su

Identifica attività eseguite sull'istanza selezionata dell'oggetto. Se non viene selezionata un'istanza dell'oggetto, vengono visualizzate le attività eseguite su tutte le istanze dell'oggetto in questione.

Nota: questo campo viene visualizzato solo quando il campo Configurazione eseguita il è popolato nella schermata Configura attività inoltrate. Mediante questa schermata è possibile configurare la scheda Attività inoltrate. Per ulteriori informazioni, consultare la Guida in linea relativa a tale schermata.

Intervallo data

Identifica le date che delimitano l'intervallo in cui ricercare attività inoltrate. È necessario specificare le date Da e A.

Mostra attività non inoltrate

Identifica le attività con stato Verificato. Identifica le attività che hanno iniziato altre attività o quelle che non sono state inoltrate. Tutte queste attività saranno verificate e visualizzate se si seleziona questa scheda.

Mostra attività di approvazione

Identifica le attività che devono essere approvate come parte di un flusso di lavoro.

Cerca l'archivio delle attività inoltrate

Identifica le attività inoltrate che sono state archiviate.

Ulteriori informazioni:

[Descrizione dello stato delle attività](#) (a pagina 581)

Descrizione dello stato delle attività

Un'attività inoltrata può avere uno o più stati tra quelli descritti di seguito. In base allo stato dell'attività, sono possibili azioni quali l'annullamento o la ripetizione dell'inoltro.

Nota: per annullare o ripetere l'inoltro di un'attività, è necessario configurare Visualizza attività inoltrate per visualizzare i pulsanti di annullamento e nuovo inoltro a seconda dello stato delle attività. Per ulteriori informazioni sull'annullamento o il nuovo inoltro delle attività, vedere [Personalizzazione della scheda Visualizza attività inoltrate](#) (a pagina 584).

In corso

Visualizzato al verificarsi delle situazioni seguenti:

- Il flusso di lavoro è iniziato ma non ancora completato.
- Le attività iniziate prima delle attività correnti sono in corso.
- Le attività nidificate sono iniziate ma non ancora completate.
- L'evento primario è iniziato ma non ancora completato.
- Gli eventi secondari sono iniziati ma non ancora completati.

È possibile annullare un'attività in questo stato.

Nota: l'annullamento di un'attività annulla tutte le attività nidificate non completate e gli eventi dell'attività corrente.

Annullato

Visualizzato quando si annulla qualsiasi attività o evento in corso.

Rifiutato

Visualizzato quando in CA Identity Manager viene rifiutato un evento o un'attività che fa parte di un processo del flusso di lavoro. È possibile inoltrare di nuovo un'attività rifiutata.

Nota: quando l'attività viene inoltrata di nuovo, in CA Identity Manager viene ripetuto l'inoltro di tutte le attività nidificate e degli eventi non riusciti o rifiutati.

Parzialmente completato

Visualizzato in caso di annullamento di parte degli eventi o delle attività nidificate. È possibile inoltrare di nuovo un evento o un'attività nidificata parzialmente completati.

Completato

Visualizzato quando un'attività è completata. Un'attività è completata quando le attività nidificate e gli eventi nidificati dell'attività corrente sono stati completati.

Non riuscito

Visualizzato quando un'attività, un'attività nidificata o un evento nidificato nell'attività corrente non è valido. Questo stato viene visualizzato quando l'attività non riesce. È possibile inoltrare di nuovo un'attività non riuscita.

Pianificato

Visualizzato quando l'attività è pianificata per l'esecuzione in una data successiva. È possibile annullare un'attività in questo stato.

Verificato

Visualizzato quando l'attività corrente è verificata.

Visualizza dettagli attività

In CA Identity Manager vengono forniti dettagli sull'attività, quali lo stato di un'attività inoltrata, delle attività nidificate e degli eventi associati a un'attività.

Come visualizzare i dettagli di un'attività inoltrata

1. Fare clic sulla freccia rivolta verso destra accanto all'attività selezionata nella scheda Visualizza attività inoltrate.

Verranno visualizzati i dettagli dell'attività.

Nota: eventi e attività nidificate, se presenti, vengono visualizzati nella pagina Dettagli dell'attività. È possibile visualizzare i dettagli per ogni attività ed evento.

2. Fare clic su Chiudi.

La scheda Dettagli dell'attività viene chiusa e in CA Identity Manager viene visualizzata la scheda Visualizza attività inoltrate con l'elenco delle attività.

Visualizzazione dei dettagli degli eventi

In CA Identity Manager vengono forniti dettagli sugli eventi, quali lo stato di un evento inoltrato, gli attributi e le eventuali ulteriori informazioni sugli eventi.

Come visualizzare i dettagli di un evento inoltrato

1. Fare clic sulla freccia rivolta verso destra accanto a un evento nella pagina Visualizza dettagli attività.

Verranno visualizzati i dettagli dell'evento.

2. Fare clic su Chiudi.

La pagina Dettagli evento viene chiusa.

Descrizione dello stato degli eventi

Gli eventi in CA Identity Manager possono presentare uno degli stati descritti di seguito. A seconda dello stato dell'evento, è possibile annullarlo o ripeterne l'inoltro per l'esecuzione.

Nota: per consentire agli amministratori di annullare o ripetere l'inoltro di un evento, è necessario configurare Visualizza attività inoltrate per visualizzare i pulsanti di annullamento e nuovo inoltro degli eventi. Durante la configurazione dell'attività, è possibile specificare quali amministratori possono annullare e inoltrare di nuovo gli eventi. Per ulteriori informazioni sull'annullamento o il nuovo inoltro degli eventi, vedere [Personalizzazione della scheda Visualizza attività inoltrate](#) (a pagina 584).

In corso

Visualizzato al verificarsi delle situazioni seguenti:

- Il flusso di lavoro o gli eventi preliminari sono iniziati, in corso o approvati.
- L'evento è in esecuzione in CA Identity Manager.
- Gli eventi successivi sono in esecuzione in CA Identity Manager.

Gli eventi con questo stato possono essere annullati.

Rifiutato

Questo stato viene visualizzato quando un evento del flusso di lavoro viene rifiutato. È possibile inoltrare di nuovo un evento rifiutato.

Annullato

Questo stato viene visualizzato quando un evento in corso viene annullato. È possibile inoltrare di nuovo un evento annullato.

Completato

Questo stato viene visualizzato quando un evento viene completato.

Non riuscito

Questo stato viene visualizzato quando viene rilevata un'eccezione durante l'esecuzione di un evento. È possibile inoltrare di nuovo un evento annullato.

Nota: non è possibile inoltrare di nuovo un evento secondario fino a che l'evento primario non raggiunge lo stato Completato.

Pianificato

Questo stato viene visualizzato quando l'esecuzione dell'evento è pianificata in una data successiva. Gli eventi con questo stato possono essere annullati.

Verificato

Questo stato viene visualizzato quando l'evento corrente è stato verificato.

Personalizzazione della scheda Visualizza attività inoltrate

È possibile personalizzare la scheda Visualizza attività inoltrate come segue:

- Specificare un altro nome attività e tag.
- Cambiare le proprietà di visualizzazione predefinite. Dopo l'installazione, gli utenti visualizzano una schermata di ricerca in cui è possibile immettere criteri che determinano le attività mostrate nella scheda. È possibile configurare la scheda per visualizzare automaticamente le attività inoltrate per il giorno corrente, evitando agli utenti di dover immettere criteri di ricerca.
- Determinare se gli eventi di controllo vengono visualizzati nella pagina Dettagli dell'attività.
- Aggiungere un'ulteriore colonna alla visualizzazione delle attività.
- Specificare i criteri per l'annullamento o il nuovo inoltro di attività ed eventi.

Nota: alcuni dettagli relativi ad attività ed eventi potrebbero comprendere dati quali stipendi o password che non andrebbero visualizzati senza crittografia nella scheda Visualizza attività inoltrate. Per nascondere tali attributi è necessario specificare parametri di classificazione dei dati quando si definiscono gli attributi nel file `directory.xml`. Per ulteriori informazioni sul file `directory.xml`, si rimanda alla *Configuration Guide*.

È possibile configurare la scheda Visualizza attività inoltrate modificando la scheda Attività di amministrazione corrispondente.

Come configurare la scheda Visualizza attività inoltrate

1. Fare clic su Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
Verrà visualizzata la pagina Selezionare attività di amministrazione.
2. Selezionare Nome o Categoria nel campo Ricerca attività di amministrazione dove, immettere la stringa da ricercare e fare clic su Cerca.
In CA Identity Manager vengono visualizzate le attività di amministrazione che soddisfano i criteri di ricerca.
3. Selezionare Visualizza attività inoltrate e fare clic su Seleziona.
In CA Identity Manager vengono visualizzati i dettagli relativi all'attività di amministrazione Visualizza attività inoltrate.
4. Fare clic sulla scheda Schede.
Verranno visualizzate le schede utilizzate per la scheda Visualizza attività inoltrate.

5. Fare clic sulla freccia rivolta verso destra per modificare la scheda Attività inoltrate. Verranno visualizzati i dettagli della scheda.
6. Modificare secondo necessità i campi per personalizzare la scheda Visualizza attività inoltrate. Vedere [Impostazioni di configurazione per la scheda Visualizza attività inoltrate](#) (a pagina 585).

Impostazioni di configurazione per la scheda Visualizza attività inoltrate

Utilizzare i campi seguenti per modificare l'aspetto e le funzionalità della scheda Visualizza attività inoltrate.

Nome

Definisce il nome dell'attività.

Tag

Definisce un identificatore univoco per l'attività. Viene utilizzato in URL, servizi Web o file delle proprietà. Deve essere composto di lettere, numeri e caratteri di sottolineatura e iniziare con una lettera o un carattere di sottolineatura.

Nascondi scheda

Identifica la scheda come visibile agli utenti ma non eseguibile. Selezionando questa opzione, in CA Identity Manager gli utenti ricevono un errore.

Visualizza elenchi attività in carico

Visualizza le attività inoltrate per il giorno corrente.

Nota: se è stata attivata questa opzione, agli utenti che selezionano Visualizza attività inoltrate verranno presentate direttamente le attività inoltrate nello stesso giorno.

Mostra eventi di verifica

Specifica se gli eventi verificati sono inclusi tra le attività nella pagina Visualizza attività inoltrate.

Permetti colonne personalizzate

Indica che è possibile aggiungere una colonna personalizzata alla tabella delle attività visualizzabile dalle schede Visualizza attività inoltrate e Cronologia utente. Ad esempio, è possibile aggiungere una colonna "ID utente" alla tabella delle attività visualizzata nella scheda Cronologia utente.

Intestazione colonna personalizzata

Indica il nome visualizzato per la colonna personalizzata.

Attributo colonna personalizzata

Indica l'attributo che verrà utilizzato per popolare la colonna personalizzata nella tabella delle attività. Ad esempio, se vengono ricercate attività svolte su dipendenti di un'organizzazione, è possibile aggiungere una colonna in cui visualizzare l'organizzazione di ciascun dipendente.

Annulla attività e eventi

Identifica i criteri per l'annullamento di attività o eventi. È possibile impostare l'ambito di questo campo selezionando una delle opzioni seguenti:

Il creatore dell'attività deve essere l'utente corrente

Specifica che l'utente può annullare o inoltrare nuovamente attività o eventi creati da lui.

Il creatore dell'attività deve essere nell'ambito

Specifica che è possibile annullare o inoltrare di nuovo attività iniziate da altri utenti che corrispondono ai criteri di ambito per il ruolo di amministrazione che consente di accedere alla scheda.

Ad esempio, è stato ricevuto il ruolo Gestore utente, che include Visualizza attività inoltrate, poiché sono soddisfatti i criteri in una regola di appartenenza che include l'ambito su tutti gli utenti nell'organizzazione Dipendente. È possibile annullare o inoltrare di nuovo attività inoltrate da tutti gli utenti nell'organizzazione Dipendente.

Nessuna restrizione

Specifica che qualsiasi utente può annullare o inoltrare di nuovo un'attività o un evento.

Non permesso

Specifica che non è consentito l'annullamento o il nuovo inoltro di un'attività o un evento.

Inoltra nuovamente attività e eventi

Identifica i criteri per inoltrare nuovamente un'attività o un evento. È possibile impostare l'ambito di questo campo selezionando una delle opzioni seguenti:

Il creatore dell'attività deve essere l'utente corrente

Specifica che l'utente può annullare o inoltrare nuovamente attività o eventi creati da lui.

Il creatore dell'attività deve essere nell'ambito

Specifica che è possibile annullare o inoltrare di nuovo attività iniziate da altri utenti che corrispondono ai criteri di ambito per il ruolo di amministrazione che consente di accedere alla scheda.

Ad esempio, è stato ricevuto il ruolo Gestore utente, che include Visualizza attività inoltrate, poiché sono soddisfatti i criteri in una regola di appartenenza che include l'ambito su tutti gli utenti nell'organizzazione Dipendente. È possibile annullare o inoltrare di nuovo attività inoltrate da tutti gli utenti nell'organizzazione Dipendente.

Nessuna restrizione

Specifica che qualsiasi utente può annullare o inoltrare di nuovo un'attività o un evento.

Non permesso

Specifica che non è consentito l'annullamento o il nuovo inoltro di un'attività o un evento.

Scheda Cronologia utente

La scheda Cronologia utente consente di visualizzare le attività correlate a un utente. È possibile visualizzare anche i dettagli di attività mostrati in questa scheda nella scheda Visualizza attività inoltrate.

Nota: Non è possibile aggiungere questa scheda alle attività di creazione, ad esempio Crea utente.

È possibile utilizzare questa scheda per visualizzare la cronologia delle attività seguenti:

- **Attività eseguite sull'utente.**

Visualizza tutte le attività eseguite sull'utente selezionato.

- **Attività eseguite dall'utente.**

Visualizza tutte le attività eseguite dall'utente selezionato.

- **Approvazioni del flusso di lavoro eseguite dall'utente**

Visualizza tutte le attività approvate dall'utente durante un flusso di lavoro.

Nota: Il tipo di attività che è possibile visualizzare in questa scheda dipende dalla configurazione della scheda. Per ulteriori informazioni, consultare la sezione [Personalizzazione della scheda Cronologia utente](#) (a pagina 589).

Attributi di ricerca per la visualizzazione della cronologia utente

Per consultare le attività inoltrate per l'elaborazione è possibile utilizzare la funzione di ricerca in Visualizza attività inoltrate. La ricerca di attività può basarsi sui criteri seguenti:

Nome attività

Identifica come criterio di ricerca il nome dell'attività. È possibile limitare la ricerca specificando condizioni quali uguale a, inizia con o finisce con il valore del campo Dove è presente il nome dell'attività. Ad esempio, è possibile specificare il criterio di ricerca "nome attività è uguale a Crea utente" selezionando la condizione uguale a e immettendo Crea utente nel campo di testo.

Stato attività

Identifica come criterio di ricerca lo stato dell'attività. Per selezionare lo stato dell'attività, attivare Dove è presente lo stato dell'attività uguale a e selezionare la condizione. Per limitare ulteriormente la ricerca, è possibile utilizzare le condizioni seguenti:

- Completato
- In corso
- Non riuscito
- Rifiutato
- Parzialmente completato
- Annullato
- Pianificato

Nota: per ulteriori informazioni, vedere [Descrizione dello stato dell'attività](#) (a pagina 581).

Priorità di attività

Identifica come criterio di ricerca la priorità dell'attività. Per selezionare la priorità dell'attività, attivare Dove è presente la priorità dell'attività uguale a e selezionando la condizione. Per limitare ulteriormente la ricerca, è possibile utilizzare le condizioni seguenti:

Bassa

Specifica la ricerca di attività con priorità bassa.

Media

Specifica la ricerca di attività con priorità media.

Alta

Specifica la ricerca di attività con priorità alta.

Intervallo data

Identifica le date che delimitano l'intervallo in cui ricercare attività inoltrate. È necessario specificare le date Da e A.

Personalizzazione della scheda Cronologia utente

Gli amministratori possono personalizzare la scheda Cronologia utente come segue:

- Specificare un altro nome attività e tag.
- Cambiare le proprietà di visualizzazione predefinite. Per impostazione predefinita, gli utenti possono immettere criteri che determinano quali attività sono visualizzate nella scheda. Gli amministratori possono configurare la scheda per visualizzare automaticamente le attività per un giorno corrente, evitando agli utenti di dover immettere criteri di ricerca.

- Determinare se gli eventi di controllo vengono visualizzati nella pagina Dettagli dell'attività.
- Aggiungere una colonna alla visualizzazione delle attività.
- Specificare i criteri per l'annullamento o il nuovo inoltro di attività ed eventi.

Procedere come descritto di seguito:

1. Accedere a Ruoli e attività, Attività di amministrazione, Gestisci attività di amministrazione.
Verrà visualizzata la pagina Selezionare attività di amministrazione.
2. Selezionare Nome o Categoria nel campo Ricerca attività di amministrazione dove, immettere la stringa da ricercare e fare clic su Cerca.
In CA Identity Manager vengono visualizzate le attività di amministrazione che soddisfano i criteri di ricerca.
3. Selezionare l'attività che include la scheda Cronologia utente e fare clic su Seleziona.
In CA Identity Manager vengono visualizzati i dettagli relativi all'attività di amministrazione.
4. Fare clic sulla scheda Schede.
5. Fare clic sull'icona Modifica accanto alla scheda Cronologia utente.
Verranno visualizzati i dettagli della scheda.
6. Modificare i campi per personalizzare la scheda Cronologia utente.

Impostazioni di configurazione per la scheda Cronologia utente

Utilizzare i campi seguenti per modificare l'aspetto e le funzionalità della scheda Cronologia utente.

Nome

Definisce il nome dell'attività.

Tag

Definisce un identificatore univoco per l'attività. Viene utilizzato in URL, servizi Web o file delle proprietà. Deve essere composto di lettere, numeri e caratteri di sottolineatura e iniziare con una lettera o un carattere di sottolineatura.

Nascondi scheda

Identifica la scheda come visibile agli utenti ma non eseguibile. Selezionando questa opzione, in CA Identity Manager gli utenti ricevono un errore.

Visualizza elenchi attività in carico

Visualizza le attività inoltrate per il giorno corrente.

Nota: se è stata attivata questa opzione, agli utenti che selezionano Visualizza attività inoltrate verranno presentate direttamente le attività inoltrate nello stesso giorno.

Mostra eventi di verifica

Specifica se gli eventi verificati sono inclusi tra le attività nella pagina Visualizza attività inoltrate.

Permetti colonne personalizzate

Indica che è possibile aggiungere una colonna personalizzata alla tabella delle attività visualizzabile dalle schede Visualizza attività inoltrate e Cronologia utente. Ad esempio, è possibile aggiungere una colonna "ID utente" alla tabella delle attività visualizzata nella scheda Cronologia utente.

Intestazione colonna personalizzata

Indica il nome visualizzato per la colonna personalizzata.

Attributo colonna personalizzata

Indica l'attributo che verrà utilizzato per popolare la colonna personalizzata nella tabella delle attività. Ad esempio, se vengono ricercate attività svolte su dipendenti di un'organizzazione, è possibile aggiungere una colonna in cui visualizzare l'organizzazione di ciascun dipendente.

Annulla attività e eventi

Identifica i criteri per l'annullamento di attività o eventi. È possibile impostare l'ambito di questo campo selezionando una delle opzioni seguenti:

Il creatore dell'attività deve essere l'utente corrente

Specifica che l'utente può annullare o inoltrare nuovamente attività o eventi creati da lui.

Il creatore dell'attività deve essere nell'ambito

Specifica che è possibile annullare o inoltrare di nuovo attività iniziate da altri utenti che corrispondono ai criteri di ambito per il ruolo di amministrazione che consente di accedere alla scheda.

Ad esempio, è stato ricevuto il ruolo Gestore utente, che include Visualizza attività inoltrate, poiché sono soddisfatti i criteri in una regola di appartenenza che include l'ambito su tutti gli utenti nell'organizzazione Dipendente. È possibile annullare o inoltrare di nuovo attività inoltrate da tutti gli utenti nell'organizzazione Dipendente.

Nessuna restrizione

Specifica che qualsiasi utente può annullare o inoltrare di nuovo un'attività o un evento.

Non permesso

Specifica che non è consentito l'annullamento o il nuovo inoltro di un'attività o un evento.

Inoltra nuovamente attività e eventi

Identifica i criteri per inoltrare nuovamente un'attività o un evento. È possibile impostare l'ambito di questo campo selezionando una delle opzioni seguenti:

Il creatore dell'attività deve essere l'utente corrente

Specifica che l'utente può annullare o inoltrare nuovamente attività o eventi creati da lui.

Il creatore dell'attività deve essere nell'ambito

Specifica che è possibile annullare o inoltrare di nuovo attività iniziate da altri utenti che corrispondono ai criteri di ambito per il ruolo di amministrazione che consente di accedere alla scheda.

Ad esempio, è stato ricevuto il ruolo Gestore utente, che include Visualizza attività inoltrate, poiché sono soddisfatti i criteri in una regola di appartenenza che include l'ambito su tutti gli utenti nell'organizzazione Dipendente. È possibile annullare o inoltrare di nuovo attività inoltrate da tutti gli utenti nell'organizzazione Dipendente.

Nessuna restrizione

Specifica che qualsiasi utente può annullare o inoltrare di nuovo un'attività o un evento.

Non permesso

Specifica che non è consentito l'annullamento o il nuovo inoltro di un'attività o un evento.

Mostra attività

Determina le attività visualizzate nella scheda Cronologia utente.

Attività eseguite sull'utente

Visualizza tutte le attività eseguite sull'utente selezionato.

Attività eseguite dall'utente

Visualizza tutte le attività eseguite dall'utente selezionato.

Approvazioni del flusso di lavoro eseguite dall'utente

Visualizza tutte le attività approvate dall'utente come parte di un flusso di lavoro.

Attività Visualizza attività utente

L'attività utente è una cronologia delle attività che coinvolgono un utente specifico. Visualizza attività utente consente agli amministratori di tenere traccia delle informazioni utente seguenti:

- Attività eseguite sull'utente.
- Attività eseguite dall'utente.
- Approvazioni del flusso di lavoro eseguite dall'utente.

Come visualizzare l'attività dell'utente

1. Accedere a Utenti, Gestisci utenti, Visualizza attività utente.
Verrà visualizzato lo schermo Seleziona utente.
2. Cercare un utente e fare clic su Seleziona.
Verrà visualizzato lo schermo Visualizza attività utente.

Nota: per ulteriori informazioni sull'attività utente visualizzata, consultare la Guida in linea della console utente.

Pulitura delle attività inoltrate

Man mano che vengono inoltrate attività, le prestazioni runtime di attività ed eventi rallentano al crescere del database di persistenza delle attività. La garbage collection delle stored procedure riduce i possibili problemi di prestazioni o tempi di indisponibilità dei sistemi dovuti alla carenza di spazio nel database di persistenza delle attività. La capacità di archiviare le attività consente agli amministratori di visualizzare sia le informazioni relative ad attività ed eventi correnti, quanto ad attività ed eventi eliminati.

Gli amministratori di CA Identity Manager possono pianificare l'esecuzione automatica su base ricorrente della garbage collection da parte dei processi servendosi della console utente.

Scheda Ricorrenza

Utilizzare questa scheda per pianificare il processo. Di seguito sono elencati i campi presenti nella scheda:

Esegui ora

Il processo viene eseguito immediatamente.

Pianifica nuovo processo

Consente di pianificare un nuovo processo.

Modifica processo esistente

Consente di specificare che si desidera modificare un processo esistente.

Nota: questo campo viene visualizzato solo se per questa attività è già stato pianificato un processo.

Nome processo

Consente di specificare il nome del processo da creare o modificare.

Fuso orario

Consente di specificare il server del fuso orario.

Nota: se il fuso orario utilizzato è diverso da quello del server del fuso orario, viene visualizzata una casella a discesa nella quale è possibile selezionare il proprio fuso orario o quello del server per la pianificazione di un nuovo processo. Non è possibile modificare il fuso orario quando si modifica un processo esistente.

Pianificazione giornaliera

Consente di specificare che il processo venga eseguito a intervalli regolari.

Ogni (numero di giorni)

Consente di definire il numero di giorni che intercorrono tra le esecuzioni del processo.

Pianificazione settimanale

Consente di specificare che il processo venga eseguito a una determinata ora di un dato giorno o giorni della settimana.

Giorno della settimana

Consente di specificare il giorno o i giorni della settimana in cui viene eseguito il processo.

Pianificazione mensile

Consente di specificare un giorno della settimana o del mese in cui viene eseguito il processo, su base mensile.

Pianificazione annuale

Consente di specificare un giorno della settimana o del mese in cui viene eseguito il processo, su base annuale.

Pianificazione avanzata

Consente di specificare ulteriori informazioni di pianificazione.

Espressione cron

Per informazioni sulla compilazione di questo campo, consultare la pagina seguente:

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

Tempo di esecuzione

Consente di specificare l'ora del giorno, in formato a 24 ore, in cui viene eseguito il processo. Ad esempio, 14.15.

Esecuzione immediata di un processo

Per eseguire un processo immediatamente, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza della procedura guidata.
2. Selezionare Esegui ora e quindi Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate della procedura guidata.
3. Immettere durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il processo viene inoltrato immediatamente.

Pianificazione di un nuovo processo

Per pianificare un nuovo processo, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza.
2. Selezionare Pianifica nuovo processo, immettere il nome del processo e le relative informazioni di pianificazione, quindi fare clic su Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate.
3. Immettere durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il nuovo processo viene pianificato.

Modifica di un processo esistente

Per modificare un processo esistente, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza.
2. Selezionare Modifica processo esistente e scegliere un processo esistente, modificare le informazioni di pianificazione, quindi fare clic su Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate.
3. Modificare durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il processo esistente viene modificato.

Eliminazione di un'attività ricorrente

Per eliminare un'attività ricorrente, attenersi alla procedura riportata di seguito.

Procedere come descritto di seguito:

1. Accedere a Sistema, quindi selezionare Elimina attività ricorrente.
2. Selezionare l'attività da eliminare.
3. Fare clic su Inoltra.

Scheda Attività di pulitura inoltrate

Utilizzare questa scheda per specificare le seguenti informazioni per l'attività: durata minima, archivio, timeout di verifica, limite di tempo e limite attività. Dopo avere compilato i campi obbligatori, fare clic su Fine per due volte. Di seguito sono elencati i campi presenti nella scheda:

Durata minima

Consente di specificare la durata minima delle attività in stato finale (Completato, Impossibile, Rifiutato, Annullato o Aborted (Interrotto)) da pulire. Ad esempio, se è specificato un mese, le attività che hanno raggiunto uno stato finale nell'ultimo mese vengono conservate. Le attività che hanno raggiunto uno stato finale oltre un mese fa vengono assoggettate alla pulitura e all'archiviazione.

Campo obbligatorio.

Archive

Consente di eseguire il backup nel database di archiviazione prima di eliminare le attività dal database runtime.

Una volta eseguito il processo, se viene selezionato Archive, i dati vengono riportati nel database archivio e rimossi dal database di permanenza dell'attività runtime. I dati vengono rimossi solo dopo che sono stati riportati correttamente nel database archivio.

Timeout verifica

Consente di specificare il lasso di tempo che dovrà trascorrere prima che le attività in stato di verifica vengano assoggettate alla pulitura. Le attività in stato di verifica non sono considerate in uno stato finale finché non è trascorso questo lasso di tempo. Le attività in stato di verifica non sono state inoltrate.

Limite di tempo

Consente di limitare la pulitura a un lasso di tempo specifico.

Limite attività

Consente di limitare la pulitura a un numero specifico di attività.

Eliminazione di attività ricorrenti

Quando non è più necessario eseguire un'attività su base ricorrente, l'amministratore di CA Identity Manager può eliminarla. Dopo l'eliminazione dell'attività, per essa non vengono più eseguite la garbage collection e l'archiviazione.

In questa pagina sono elencate tutte le attività pianificate utilizzando la procedura guidata Attività di pulizia inoltrate: Ricorrenza e l'amministratore di CA Identity Manager può scegliere le attività da eliminare.

Nota: le attività continuano ad essere presenti nel database, viene eliminata solo la ricorrenza della pianificazione.

Configurazione della connessione Enterprise Log Manager

Utilizzare questa schermata per gestire le attività appena aggiunte di connessione di CA User Activity Reporting (CA UAR).

Nota: l'applicazione CA Enterprise Log Manager è stata rinominata. Adesso è nota come CA UAR.

Di seguito sono descritti i campi presenti in questa schermata:

Nome connessione

Nome univoco utilizzato per il singolo oggetto gestito connessione di CA UAR.

Il campo è di sola lettura.

Descrizione

Descrizione della connessione di CA UAR.

Nome host

Indica il nome host o l'indirizzo IP del server di CA UAR.

Campo obbligatorio.

Porta n.

Specifica la porta di connessione al server di CA UAR.

Impostazione predefinita: 52520

Campo obbligatorio.

Certificato SSL firmato dall'Autorità di certificazione

Se selezionata, questa opzione consente di specificare il controllo rigido di un certificato SSL durante la connessione al server di CA UAR.

Se si dispone di un certificato SSL autofirmato, ad esempio un certificato installato per impostazione predefinita in CA UAR, non selezionare questa casella di controllo poiché non esiste un percorso attendibile dell'autorità di certificazione.

Nome certificato

Nome del certificato CA UAR da utilizzare per l'autenticazione.

Campo obbligatorio.

Certificate password (Password certificato)

Specifica la password CA UAR.

Campo obbligatorio.

Attributo

Non supportato. La versione viene recuperata durante il tentativo di salvare le informazioni di connessione come prova.

Eliminazione della connessione Enterprise Log Manager

Selezionare una connessione nell'elenco, quindi fare clic su Elimina. La connessione di CA UAR viene eliminata.

Gestione delle chiavi segrete

Utilizzare Chiavi segrete per gestire le chiavi dinamiche di crittografia e decrittografia dei dati. Inoltre, se si suppone che un utente abbia avuto accesso non autorizzato a una chiave, è possibile modificare la password per il KeyStore. KeyStore è il database in cui sono archiviate le chiavi segrete. Una volta modificata la password, CA Identity Manager esegue nuovamente la crittografia dei valori delle chiavi.

Ciascun ambiente dispone di un insieme di chiavi dinamiche e di una password KeyStore. Se gli ambienti condividono una directory utente, utilizzare le stesse chiavi dinamiche e la stessa password KeyStore per ogni ambiente.

Le password KeyStore vengono crittografate mediante le chiavi integrate nel codice di crittografia o i parametri immessi durante l'installazione del server CA Identity Manager. In un cluster, tutti i nodi condividono i valori delle chiavi dinamiche e la password KeyStore.

Le operazioni di crittografia utilizzano la chiave dinamica più recente per l'algoritmo e l'ambiente corrispondenti. Le operazioni di decrittografia controllano se nei dati crittografati esiste un ID chiave, in modo che venga utilizzata la chiave corretta. Nella sezione Formati di testo crittografati della *Guida alla configurazione* vengono fornite ulteriori informazioni.

Procedere come descritto di seguito:

1. Immettere o modificare la password di KeyStore.
2. Fare clic su Aggiungi chiave se è necessaria un'altra chiave.
3. Selezionare un algoritmo.
4. Immettere una password per la chiave.
Per PBE e RC2, la lunghezza massima della chiave è pari a 128 byte.
Per AES, le dimensioni valide per la chiave sono 16, 24 e 32 byte.
5. Fare clic su Inoltra.
6. Se è stata modificata la password di KeyStore, fare clic su Invia.
CA Identity Manager crittografa nuovamente i valori delle chiavi.

Capitolo 20: Persistenza delle attività

Questa sezione contiene i seguenti argomenti:

[Pulitura ed archiviazione automatizzata della persistenza delle attività](#) (a pagina 601)

[Scheda Ricorrenza](#) (a pagina 602)

[Scheda Attività di pulitura inoltrate](#) (a pagina 603)

[Esecuzione immediata di un processo](#) (a pagina 604)

[Pianificazione di un nuovo processo](#) (a pagina 604)

[Modifica di un processo esistente](#) (a pagina 605)

[Eliminazione di un'attività ricorrente](#) (a pagina 605)

[Migrazione del database di persistenza delle attività](#) (a pagina 606)

Pulitura ed archiviazione automatizzata della persistenza delle attività

In questa versione, un amministratore è autorizzato a pianificare e modificare processi con determinati parametri utilizzando la pulitura delle attività inoltrate (Attività di pulitura inoltrate) per eseguire la pulitura ed archiviazione di attività ed informazioni su eventi nel database di persistenza delle attività ed eliminare le attività ricorrenti qualora fosse necessario.

Dalla scheda Sistema, è possibile avviare una procedura guidata selezionando l'opzione Attività di pulitura inoltrate. La procedura guiderà l'utente alla configurazione e pianificazione di processi e rileva i dati da archiviare o non archiviare. Qualora fosse necessario, è inoltre possibile scegliere di eliminare i processi ricorrenti selezionando l'opzione Elimina attività ricorrenti dalla scheda Sistema.

Attraverso la pianificazione delle attività di pulitura ed archiviazione di dati sulle attività, i rischi di problemi di funzionamento o interruzione del sistema vengono ridotti. Con la funzionalità di archiviazione, è possibile eseguire il backup delle attività nel database di archiviazione prima di eliminarle dal database runtime. Qualora fosse necessario rivedere le attività eliminate, selezionare la casella di controllo Cerca l'archivio delle attività inoltrate in Visualizza attività inoltrate per ricercare e visualizzare un elenco di tutte le attività eliminate o archiviate.

Scheda Ricorrenza

Utilizzare questa scheda per pianificare il processo. Di seguito sono elencati i campi presenti nella scheda:

Esegui ora

Il processo viene eseguito immediatamente.

Pianifica nuovo processo

Consente di pianificare un nuovo processo.

Modifica processo esistente

Consente di specificare che si desidera modificare un processo esistente.

Nota: questo campo è visualizzato solo se per questa attività è già stato pianificato un processo.

Nome processo

Consente di specificare il nome del processo da creare o modificare.

Fuso orario

Consente di specificare il server del fuso orario.

Nota: se il fuso orario utilizzato è diverso da quello del server del fuso orario, viene visualizzata una casella a discesa nella quale è possibile selezionare il proprio fuso orario o quello del server per la pianificazione di un nuovo processo. Non è possibile modificare il fuso orario quando si modifica un processo esistente.

Pianificazione settimanale

Consente di specificare che il processo viene eseguito a una determinata ora di un dato giorno o giorni della settimana.

Pianificazione avanzata

Consente di specificare ulteriori informazioni di pianificazione.

Giorno della settimana

Consente di specificare il giorno o giorni della settimana in cui viene eseguito il processo.

Ora di esecuzione;

Consente di specificare l'ora del giorno, in formato a 24 ore, in cui viene eseguito il processo. Ad esempio, 14.15.

Espressione cron

Per informazioni sulla compilazione di questo campo, consultare il seguente collegamento:

<http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html>

Nota: questo campo è visualizzato quando è selezionato Pianificazione avanzata.

Ulteriori informazioni

[Eliminazione di un'attività ricorrente](#) (a pagina 596)

[Pianificazione di un nuovo processo](#) (a pagina 596)

[Modifica di un processo esistente](#) (a pagina 596)

[Esecuzione immediata di un processo](#) (a pagina 595)

Scheda Attività di pulitura inoltrate

Utilizzare questa scheda per specificare le seguenti informazioni per l'attività: durata minima, archivio, timeout di verifica, limite di tempo e limite attività. Dopo avere compilato i campi obbligatori, fare clic su Fine per due volte. Di seguito sono elencati i campi presenti nella scheda:

Durata minima

Consente di specificare la durata minima delle attività in stato finale (Completato, Impossibile, Rifiutato, Annullato o Aborted (Interrotto)) da pulire. Ad esempio, se è specificato un mese, le attività che hanno raggiunto uno stato finale nell'ultimo mese vengono conservate. Le attività che hanno raggiunto uno stato finale oltre un mese fa vengono assoggettate alla pulitura e all'archiviazione.

Campo obbligatorio.

Archive

Consente di eseguire il backup nel database di archiviazione prima di eliminare le attività dal database runtime.

Una volta eseguito il processo, se viene selezionato Archive, i dati vengono riportati nel database archivio e rimossi dal database di permanenza dell'attività runtime. I dati vengono rimossi solo dopo che sono stati riportati correttamente nel database archivio.

Timeout verifica

Consente di specificare il lasso di tempo che dovrà trascorrere prima che le attività in stato di verifica vengano assoggettate alla pulitura. Le attività in stato di verifica non sono considerate in uno stato finale finché non è trascorso questo lasso di tempo. Le attività in stato di verifica non sono state inoltrate.

Limite di tempo

Consente di limitare la pulitura a un lasso di tempo specifico.

Limite attività

Consente di limitare la pulitura a un numero specifico di attività.

Esecuzione immediata di un processo

Per eseguire un processo immediatamente, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza della procedura guidata.
2. Selezionare Esegui ora e quindi Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate della procedura guidata.
3. Immettere durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il processo viene inoltrato immediatamente.

Pianificazione di un nuovo processo

Per pianificare un nuovo processo, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza.
2. Selezionare Pianifica nuovo processo, immettere il nome del processo e le relative informazioni di pianificazione, quindi fare clic su Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate.
3. Immettere durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il nuovo processo viene pianificato.

Modifica di un processo esistente

Per modificare un processo esistente, utilizzare la procedura guidata Attività di pulitura inoltrate.

Procedere come descritto di seguito:

1. Accedere a Sistema, Attività di pulitura inoltrate.
Verrà visualizzato il passaggio Ricorrenza.
2. Selezionare Modifica processo esistente e scegliere un processo esistente, modificare le informazioni di pianificazione, quindi fare clic su Avanti.
Verrà visualizzato il passaggio Attività di pulitura inoltrate.
3. Modificare durata minima, archivio, timeout di verifica, limite di tempo e limite attività, quindi fare clic su Fine.
Il processo esistente viene modificato.

Eliminazione di un'attività ricorrente

Per eliminare un'attività ricorrente, attenersi alla procedura riportata di seguito.

Procedere come descritto di seguito:

1. Accedere a Sistema, quindi selezionare Elimina attività ricorrente.
2. Selezionare l'attività da eliminare.
3. Fare clic su Inoltra.

Migrazione del database di persistenza delle attività

Nelle versioni precedenti, la migrazione veniva eseguita "al volo" e mediante la console di gestione. È disponibile uno strumento di migrazione della riga di comando per rimuovere colli di bottiglia delle prestazioni quando si esegue la migrazione di grandi quantità di attività. È inoltre possibile ottimizzare la migrazione per un ambiente specifico, per uno stato delle attività e per le attività create ed eseguite durante un intervallo di date specifico. Lo strumento di riga di comando runmigration si trova nella cartella seguente:

admin_tools/tools/tpmigration

Per eseguire la migrazione del database di persistenza delle attività, si deve procedere come segue:

1. Aggiornare il file tpmigration125.properties
2. Impostare la variabile JAVA_HOME.
3. Eseguire lo strumento runmigration.

Aggiornare il file tpmigration125.properties

Per configurare la migrazione del database di persistenza delle attività, è necessario aggiornare il file tpmigration.properties con l'archivio oggetti e le informazioni di persistenza delle attività, inclusi i valori di archivio. Il file tpmigration125.properties si trova nella posizione seguente:

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetp125

Per configurare la migrazione, completare le informazioni seguenti nel file delle proprietà:

```
#####
# The object store is required to obtain the environment details.
#####
os.db.hostname=<hostname>
os.db.dbname=<database-name or SID>
os.db.username=<db user name>
os.db.password=<db user's password>
os.db.port=<db port number>
os.db.dbType=<type of the database. For ex. for SQL server sql2005 and for
oracle 'oracle'>

#####
Task persistence data where the old and new tables are.
#####
tp.db.hostname=<hostname>
tp.db.dbname=<database-name or SID>
tp.db.username=<db user name>
tp.db.password=<db user's password>
tp.db.port=<db port number>
tp.db.dbType=<type of the database. For ex. for SQL server sql2005 and for
oracle 'oracle'>
```

Impostazione della variabile JAVA_HOME.

Perché lo strumento runmigration possa funzionare correttamente, assicurarsi che la variabile di ambiente JAVA_HOME sia impostata.

Esecuzione dello strumento runmigration.

Per avviare la migrazione, utilizzare la procedura seguente.

Da una riga di comando

1. Eseguire lo strumento runmigration.

Per Windows:

runmigration.bat

Per UNIX:

runmigration.sh

2. Inserire i seguenti dettagli:

- L'alias protetto di ambiente ("tutti" per tutti gli ambienti).

Nota: se non si specifica "tutti", è possibile immettere solo un ambiente.

- Lo stato dell'attività.

Nota: se non si specifica "tutti", è possibile immettere solo uno stato.

- La versione di CA Identity Manager da cui si desidera eseguire la migrazione (1-8.x, 2-12.0).

- Specificare un intervallo di date per le attività di cui eseguire la migrazione (y/n).

Nota: se si sceglie "y", immettere quanto segue:

- Immettere la data di inizio (mm/dd/yy)
- Immettere la data di fine (mm/dd/yy)

La migrazione viene avviata.

Al termine della migrazione, lo stato indica di quante attività è stata eseguita la migrazione.