NetIQ Directory and Resource Administrator

Guida dell'utente

Giugno 2021

Note legali

Sommario

Informazioni su questa guida

La *Guida dell'utente* fornisce informazioni concettuali su NetIQ Directory and Resource Administrator (DRA), definisce la terminologia e illustra vari concetti correlati.

Destinatari

Le informazioni contenute in questo manuale sono rivolte a coloro che devono apprendere i concetti relativi all'amministrazione e che devono implementare un modello di amministrazione sicuro e distribuito.

Documentazione aggiuntiva

Questa guida fa parte del set di documentazione di Directory and Resource Administrator. Pe la versione più recente di questa Guida e altre risorse su DRA, visitare il sito Web della documentazione di NetIQ DRA (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Informazioni di contatto

Saremo lieti di ricevere commenti e suggerimenti su questo manuale e sulla documentazione allegata al prodotto. A tal fine, utilizzare il collegamento **Inserisci un commento sull'argomento** in fondo a ciascuna pagina della documentazione online oppure inviare un'e-mail a Documentation-Feedback@microfocus.com.

Per problemi specifici del prodotto, visitare la pagina del Servizio clienti Micro Focus all'indirizzo https://www.microfocus.com/it-it/support-and-services/.

1 Introduzione

Prima di iniziare a gestire gli oggetti di Active Directory utilizzando NetIQ Directory and Resource Administrator (DRA), è necessario comprendere i concetti di base su ciò che DRA sarà in grado di offrire alla propria azienda e sul ruolo che i suoi componenti svolgono nell'architettura del prodotto.

Che cos'è Directory and Resource Administrator

NetIQ Directory and Resource Administrator è una soluzione sicura ed efficiente di amministrazione delle identità privilegiate di Microsoft Active Directory (AD). Consente di delegare in modo differenziato il "privilegio minimo", affinché amministratori e utenti ricevano solo le autorizzazioni necessarie a svolgere le funzioni corrispondenti alle loro responsabilità. Inoltre, assicura il rispetto delle policy, fornisce funzioni di revisione e generazione di rapporti dettagliati delle attività e semplifica l'esecuzione di task ripetitivi con l'automazione dei processi IT. Ciascuna di queste funzionalità contribuisce a proteggere gli ambienti Active Directory ed Exchange dei clienti dal rischio di aumento elevato dei privilegi, errori, attività dannose e non conformità alle norme, riducendo al contempo il carico di lavoro degli amministratori tramite funzioni self-service per utenti, manager aziendali e personale dell'help desk.

DRA amplia inoltre le potenti funzioni di Microsoft Exchange per semplificare la gestione degli oggetti di Exchange. Attraverso un'interfaccia utente unica e comune, DRA consente l'amministrazione basata su policy per la gestione di caselle postali, cartelle pubbliche e liste di distribuzione in tutto l'ambiente Microsoft Exchange.

DRA offre le soluzioni necessarie per il controllo e la gestione di ambienti Active Directory, Microsoft Windows, Microsoft Exchange e Azure Active Directory.

- **Supporto per Azure e per le installazioni locali di Active Directory, Exchange e Skype for Business:** fornisce la gestione amministrativa di Azure e delle installazioni locali di Active Directory, Exchange Server, Skype for Business, nonché di Exchange Online e Skype for Business Online.
- **Controlli differenziati dei privilegi di accesso di utenti e amministratori:** la tecnologia ActiveView brevettata delega solo i privilegi necessari a svolgere le funzioni corrispondenti a responsabilità specifiche e offre protezione contro l'escalation dei privilegi.
- **Console Web personalizzabile:** l'approccio intuitivo consente a personale non tecnico di eseguire task amministrativi in modo facile e sicuro mediante funzionalità e accesso limitati (e assegnati).
- **Revisioni e rapporti dettagliati delle attività:** offre un record di revisione completo di tutte le attività eseguite con il prodotto. Memorizza i dati a lungo termine e in modo sicuro, consentendo di dimostrare ai revisori (ad esempio PCI DSS, FISMA, HIPAA e NERC CIP) l'adozione di processi per il controllo degli accessi ad AD.
- **Automazione dei processi IT:** permette di automatizzare i workflow di svariati task, quali provisioning e deprovisioning, azioni di utenti e caselle postali, applicazione delle policy e task di self-service controllati, aumentando l'efficienza aziendale e riducendo le operazioni manuali e ripetitive.

- **Integrità operativa:** impedisce modifiche errate o dannose che incidono sulle prestazioni e la disponibilità di sistemi e servizi, fornendo un controllo differenziato degli accessi agli amministratori e gestendo l'accesso a sistemi e risorse.
- **Applicazione dei processi:** preserva l'integrità dei processi chiave di gestione delle modifiche per migliorare la produttività, ridurre gli errori, risparmiare tempo e aumentare l'efficienza amministrativa.
- **Integrazione con Change Guardian:** consente la revisione degli eventi generati in Active Directory al di fuori di DRA e di Workflow Automation.

Caratteristiche dei componenti di Directory and Resource Administrator

I componenti di DRA regolarmente utilizzati per gestire l'accesso con privilegi includono il server primario e il server secondario, le console di amministrazione, i componenti di generazione dei rapporti e il motore di workflow per automatizzare i processi di workflow.

Nella tabella seguente sono riportate le interfacce utente e i server di amministrazione utilizzati tipicamente da ciascun tipo di utente DRA:

Tipo di utente DRA	Interfacce utente	Server di amministrazione
Amministratore di DRA (la persona che si occuperà della configurazione del prodotto)	Delegation and Configuration Console (Console di delega e configurazione)	Server primario
Amministratore avanzato	DRA Reporting PowerShell Interfaccia della riga di comando Provider ADSI di DRA	Qualsiasi server DRA
Amministratore occasionale dell'help desk	Nodo Account and Resource Management (Gestione account e risorse) nella Console di delega e configurazione Console Web	Qualsiasi server DRA

Server di amministrazione DRA

Il server di amministrazione DRA archivia i dati di configurazione (relativi ad ambiente, accesso delegato e policy), esegue i task di operatore e automazione e revisiona l'attività di tutto il sistema. Oltre a supportare numerose console e client a livello di API, il server è concepito per garantire un'elevata disponibilità sia ai fini della ridondanza che per l'isolamento geografico tramite un

modello scalabile orizzontalmente basato su un set multimaster (MMS). In questo modello, tutti gli ambienti DRA necessitano di un server di amministrazione DRA primario che esegue la sincronizzazione con vari server di amministrazione DRA secondari aggiuntivi.

Si raccomanda di non installare i server di amministrazione nei controller di dominio di Active Directory. Per ciascun dominio gestito da DRA, verificare che vi sia almeno un controller di dominio nello stesso sito del server di amministrazione. Per default, il server di amministrazione accede al controller di dominio più vicino per tutte le operazioni di lettura e scrittura. Quando si eseguono task specifici del sito, ad esempio reimpostazioni delle password, è possibile indicare un controller di dominio specifico del sito per l'elaborazione dell'operazione. Come best practice, valutare la possibilità di riservare un server di amministrazione secondario alla generazione di rapporti, all'elaborazione batch e ai workload automatizzati.

Gestione account e risorse

Account and Resource Management (Gestione account e risorse) è un nodo della Console di delega e configurazione per gli amministratori aggiunti DRA per la visualizzazione e la gestione degli oggetti delegati di domini e servizi connessi.

Console Web

La console Web è un'interfaccia utente basata sul Web che fornisce un accesso rapido e semplice agli amministratori aggiunti di DRA, affinché possano visualizzare e gestire gli oggetti delegati di domini e servizi connessi.

Gli amministratori possono personalizzare l'aspetto e le modalità di utilizzo della console Web includendo branding aziendale personalizzato e proprietà personalizzate degli oggetti, nonché configurare l'integrazione con i server Change Guardian per abilitare la revisione delle modifiche apportate al di fuori di DRA.

L'amministratore di DRA può anche creare e modificare moduli di workflow automatizzati per eseguire task di routine automatizzati quando attivati.

Cronologia modifiche unificata è un'altra funzione della console Web che consente l'integrazione con i server di cronologia delle modifiche per la revisione delle modifiche apportate a oggetti AD al di fuori di DRA. Le opzioni dei rapporti di cronologia delle modifiche includono:

- Modifiche apportate a...
- Modifiche apportate da...
- Casella postale creata da...
- Utente, gruppo e indirizzo e-mail di contatto creati da...
- Utente, gruppo e indirizzo e-mail di contatto eliminati da...
- Attributo virtuale creato da...
- Oggetti spostati da...

Componenti per la generazione di rapporti

DRA Reporting include modelli integrati personalizzabili per la gestione di DRA e i dettagli dei domini e sistemi gestiti da DRA:

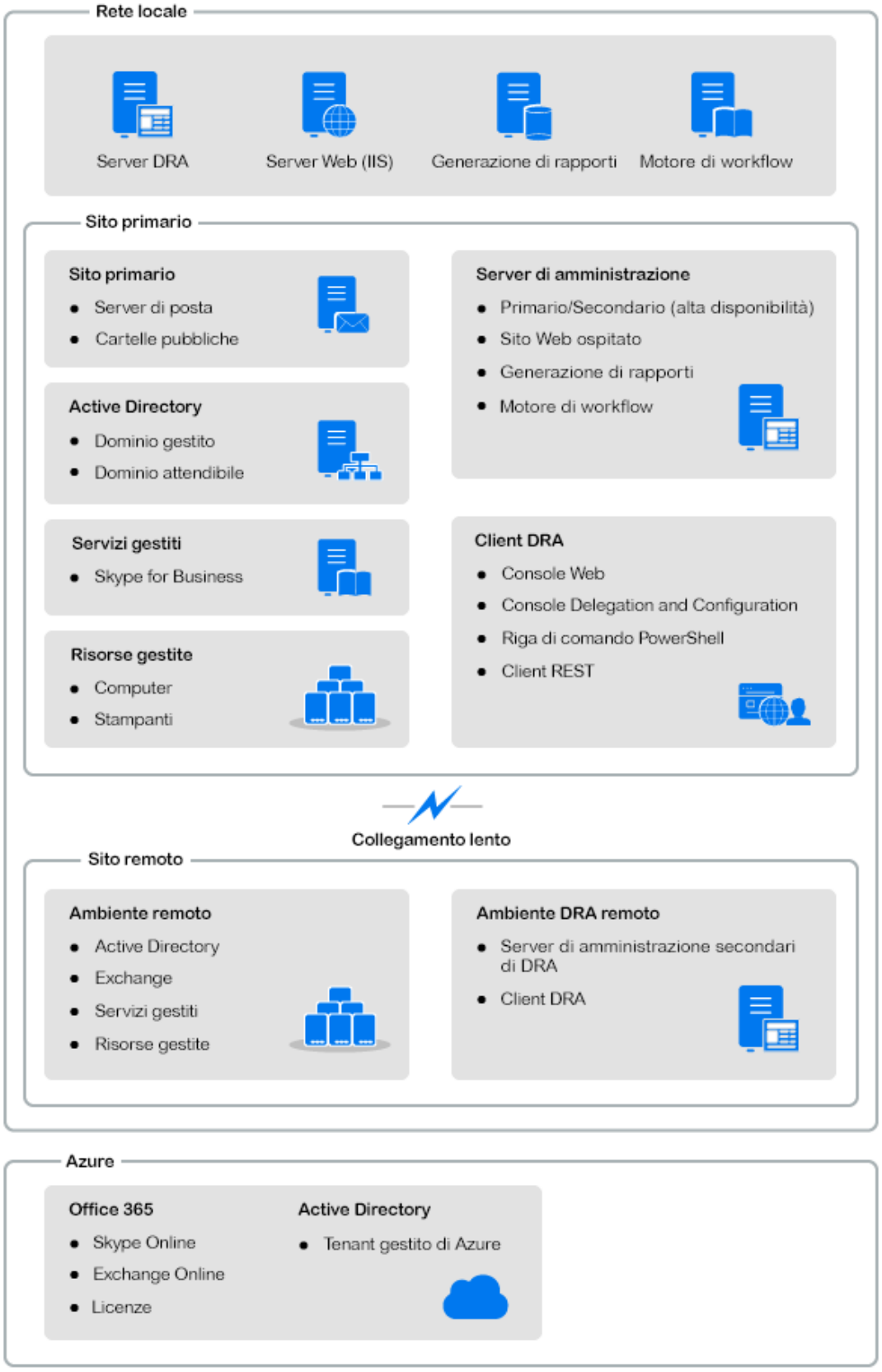
- Rapporti sulle risorse per oggetti AD
- Rapporti sui dati degli oggetti AD
- Rapporti di riepilogo di AD
- Rapporti di configurazione di DRA
- Rapporti di configurazione di Exchange
- Rapporti di Exchange Online di Office 365
- Rapporti dettagliati sulle tendenze delle attività (per mese, dominio e picco)
- Rapporti di riepilogo delle attività di DRA

I rapporti di DRA possono essere pianificati e pubblicati tramite SQL Server Reporting Services per una pratica distribuzione alle parti interessate.

Motore di workflow

DRA si integra con il motore di workflow per automatizzare i task di workflow mediante la console Web, in cui gli amministratori aggiunti possono configurare il server di workflow ed eseguire moduli di automazione dei workflow personalizzati, per poi visualizzare lo stato di tali workflow. Per ulteriori informazioni sul motore di workflow, vedere la documentazione di Workflow Automation sul sito della documentazione di NetIQ DRA.

Architettura del prodotto



2 Utilizzo delle interfacce utente

Le interfacce utente di DRA sono realizzate per soddisfare una vasta gamma di esigenze di amministrazione e comprendono:

Console Web

Consente di eseguire task di amministrazione di account e risorse comuni attraverso un'interfaccia basata sul Web. È possibile accedere alla console Web da qualsiasi computer in cui sia in esecuzione Internet Explorer, Google Chrome o Firefox.

PowerShell

Il modulo PowerShell consente ai client non DRA di richiedere operazioni con DRA mediante il comando cmdlet di PowerShell.

Console NetIQ Reporting Center

Consente di visualizzare e distribuire i rapporti Gestione affinché sia possibile controllare la sicurezza dell'azienda e registrare le attività di amministrazione. I rapporti Gestione includono rapporti sulle attività e sulla configurazione oltre a rapporti di riepilogo. Molti di questi rapporti possono essere visualizzati in una rappresentazione grafica.

Console Web

La console Web è un'interfaccia utente basata sul Web che fornisce accesso rapido e semplice a molti task su account utente, gruppi, computer, risorse e caselle postali di Microsoft Exchange. È possibile personalizzare le proprietà degli oggetti per aumentare l'efficienza dei task di routine. È inoltre possibile gestire le proprietà generali del proprio account utente, come l'indirizzo o il numero di telefono cellulare.

La console Web visualizza un task solo se si dispone dei poteri necessari per eseguirlo.

Avvio della console Web

È possibile avviare la console Web da qualsiasi computer su cui è in esecuzione uno dei seguenti browser supportati:

- Google Chrome

- Mozilla Firefox
- Microsoft Edge

Per avviare la console Web, specificare l'URL appropriato nel campo dell'indirizzo del browser Web in uso. Se, ad esempio, si è installato il componente Web nel computer con HOUserver, digitare `https://HOUserver.entDomain.com/draclient` nel campo dell'indirizzo del browser Web.

Nota: Per visualizzare l'account e le informazioni di Microsoft Exchange più recenti nella console Web, impostare il browser affinché controlli, ad ogni visita, la presenza di eventuali versioni più recenti delle pagine memorizzate nella cache.

Connessione server DRA

È possibile utilizzare una delle quattro opzioni disponibili per eseguire il login alla console Web. Il comportamento di ciascuna opzione durante il login è descritto nella seguente tabella:

Schermata di login - Opzioni	Descrizioni opzione di connessione
Usa rilevazione automatica	Consente di individuare il server DRA automaticamente; non è disponibile alcuna opzione di configurazione.
Connetti al server DRA di default	Vengono utilizzati i dettagli preconfigurati relativi al server e alla porta. **Nota:** Questa opzione viene visualizzata solo se è stato configurato il server DRA di default nella console Web. Inoltre, se si specifica che il client deve sempre connettersi al server DRA di default, è possibile visualizzare solo l'opzione **Connetti al server DRA di default** nella schermata di login.
Connetti a un server DRA specifico	L'utente configura il server e la porta
Connetti a un server DRA che gestisce un dominio specifico	L'utente specifica un dominio gestito e sceglie un'opzione di connessione: ◆ Usa rilevazione automatica (nel dominio fornito) ◆ Server primario per questo dominio ◆ Cerca un server DRA (nel dominio fornito)

Configurazione della console Web

Se si dispone dei poteri di amministrazione di DRA, è possibile configurare Advanced Authentication, il branding del client e le impostazioni della sessione, nonché tutte le connessioni server necessarie per la console Web. Per accedere a queste impostazioni, eseguire il login alla console Web e accedere ad **Amministrazione** > **Configurazione**.

Nota: La scheda **Amministrazione** non verrà visualizzata nel titolo se non si dispone dei poteri amministrativi necessari.

- “Advanced Authentication” a pagina 17
- “Branding della console Web” a pagina 17

- “Impostazioni sessione client” a pagina 19
- “Connessione al server” a pagina 19

Advanced Authentication

Advanced Authentication consente di passare dal semplice utilizzo di nome utente e password a un metodo di protezione delle informazioni riservate più sicuro mediante l'autenticazione a più fattori. L'autenticazione a più fattori è un metodo di controllo dell'accesso al computer che, per verificare l'identità di un utente, richiede più metodi di autenticazione che utilizzano categorie di credenziali separate.

Un volta che l'amministratore DRA ha configurato le catene e gli eventi, se l'utente dispone dei poteri richiesti, potrà eseguire il login alla console Web e abilitare Advanced Authentication. Dopo aver abilitato questo tipo di autenticazione, prima di poter accedere alla console Web, tutti gli utenti dovranno eseguire l'autenticazione tramite Advanced Authentication.

Per abilitare Advanced Authentication, selezionare **Advanced Authentication** dalla scheda Configurazione, fare clic su **Abilita Advanced Authentication** e configurare il modulo in base alle istruzioni fornite per ciascun campo.

Per ulteriori informazioni su Advanced Authentication, vedere la sezione “Autenticazione” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Branding della console Web

È possibile personalizzare la schermata di login e il titolo della console Web di DRA nel modo seguente:

- **Titolo:** barra di navigazione di alto livello nella parte superiore della console Web dopo il login.
  - *Immagine del logo o testo alternativo:* visualizzati all'estrema sinistra della barra del titolo. È possibile visualizzare un'immagine del logo o un testo alternativo ma non entrambi.
  - *Colore del titolo:* colore sovrapposto all'intero titolo, ad eccezione dell'area dell'immagine del logo.
- **Schermata di login con tema:** aspetto della pagina di login durante l'accesso all'URL della console Web nel browser. Il tema DRA è configurato e abilitato di default.
  - *Immagine del logo o testo alternativo:* visualizzati sopra i campi del titolo del prodotto e delle credenziali. È possibile visualizzare un'immagine del logo o un testo alternativo ma non entrambi.
  - *Titolo applicazione:* visualizzato tra i campi delle credenziali e l'immagine del logo.
  - *Finestra modale di notifica:* finestra di messaggio che si sovrappone e oscura la pagina di login fino a quando l'utente non fa clic su **OK**. In genere viene utilizzata per informare l'utente che l'accesso alla console implica il consenso ad attenersi alle policy di sicurezza aziendali. Una volta abilitata, tutti gli utenti che accedono alla console Web visualizzeranno la richiesta.

Configurazione del titolo

Per configurare il titolo:

1. Eseguire il login alla console Web e accedere ad **Amministrazione** > **Configurazione** > **Branding**.
2. Effettuare una delle seguenti operazioni. Se si aggiungono sia del testo che un file di immagine, verrà visualizzata solo l'immagine.
   - Aggiornare l'immagine del logo:
     1. Aggiungere il nome del file di immagine salvato, inclusa l'estensione, nel campo Immagine logo del riquadro **Titolo**.
     2. Salvare l'immagine del logo nella directory "`assets`" sul server Web. Ad esempio:

        `C:\inetpub\wwwroot\DRAClient\assets`

        La dimensione ottimale dell'immagine è 56x56 pixel.
   - Digitare o sovrascrivere il testo esistente nel campo Testo alternativo immagine logo del riquadro **Titolo**, in base alle esigenze.
3. Fare clic su **Salva** in basso nella pagina per applicare le modifiche alla configurazione.

Configurare la schermata di login

La procedura riportata di seguito fornisce informazioni per la modifica di tutte e tre le opzioni configurabili, il logo aziendale, il titolo dell'applicazione e la finestra modale di notifica. È possibile modificare una, due o tutte le tre opzioni.

Per modificare il tema di default nella schermata di login:

1. Salvare il logo aziendale nella cartella "`assets`" sul server Web. Ad esempio:

   `C:\inetpub\wwwroot\DRAClient\assets`

   La dimensione ottimale dell'immagine è 115x28 pixel.
2. Eseguire il login alla console Web e accedere ad **Amministrazione** > **Configurazione** > **Branding**.
3. Sostituire il nome del file nel campo Immagine logo aziendale del riquadro **Login** con il nome del file di immagine salvato, inclusa l'estensione.
4. Modificare il testo nel campo **Titolo applicazione**, se applicabile.
5. Fare clic su **Mostra una notifica obbligatoria durante il login** per abilitare questa impostazione, quindi digitare un titolo per il prompt di notifica. Digitare o incollare il contenuto del messaggio che si desidera visualizzare nel campo **Contenuto**. Ad esempio:

   Si sta accedendo a una rete sicura. Accedendo a questo sistema si acconsente a rispettare le policy di sicurezza aziendali relative all'accesso alla rete.
6. Selezionare lo stile del messaggio. Lo stile modifica il flag dell'immagine allegata alla finestra di messaggio (illustrato di seguito). Se lo si desidera, è possibile fare clic su Anteprima per visualizzare il messaggio.

 Informazioni	 Errore
Avviso	 Domanda

7 Fare clic su **Salva** in basso nella pagina per applicare le modifiche alla configurazione.

Impostazioni sessione client

In Impostazioni sessione client è possibile definire un intervallo d'inattività per il logout automatico della Console Web oppure scegliere di non eseguire mai il logout automatico.

Per configurare il Logout automatico nella console Web, accedere ad **Amministrazione** > **Configurazione** >**Impostazioni sessione client**. Abilitare la funzione di logout automatico con l'interruttore di attivazione/disattivazione e, se necessario, modificare l'impostazione per il tempo di inattività, in minuti.

Connessione al server

Quando si accede alla pagina di login della console Web nel browser, è possibile configurare le impostazioni delle **Opzioni** per definire la modalità di connessione a DRA. Queste impostazioni si trovano anche tramite l'opzione **Connessione al server** nel menu del profilo utente della console Web. La porta del servizio per il server DRA ha l'impostazione di default 8775. È possibile impostare un nuovo valore di default per il server DRA nel profilo utente o nelle Opzioni della schermata di login se non è abilitato alcun valore di default. Le impostazioni di connessione per la configurazione della Connessione al server vengono conservate con il profilo utente di Windows.

Di seguito sono riportate le informazioni sulle impostazioni che è possibile modificare dalla configurazione di **Connessione al server**, dal menu Opzioni della schermata di login o dal menu del profilo utente dopo il login:

Impostazioni del server DRA	Descrizione
Usa rilevazione automatica	Consente di individuare automaticamente un server DRA; non è disponibile alcuna opzione di configurazione.
Connetti al server DRA di default (visualizzato solo se l'impostazione di default è abilitata nella configurazione di Connessione al server)	Utilizza l'impostazione di default della configurazione di Connessione al server (se abilitata); non sono disponibili opzioni di configurazione
Connetti a un server DRA specifico	L'utente configura il server e la porta

Se necessario, è possibile configurare un'ubicazione, un server e un dominio di default per il server DRA dalla configurazione di **Connessione al server** nella console Web.

Per abilitare le impostazioni di default, eseguire il login alla console Web e accedere ad **Amministrazione** > **Configurazione** > **Connessione server DRA**. Abilitare le impostazioni di connessione che si desidera utilizzare e fare clic su **Salva**.

Connessione server DRA

La configurazione per la connessione server DRA include l'impostazione di un'ubicazione del server di default, la modifica della porta (se necessario) e un timeout di connessione espresso in secondi. È inoltre possibile disabilitare l'impostazione con l'interruttore di attivazione/disattivazione.

Quando si specifica l'ubicazione del server DRA, utilizzare il formato mostrato nell'esempio seguente:

```
NomeServer.NomeDominio.com
```

Personalizzazione della console Web

È possibile personalizzare le proprietà degli oggetti nella console Web. Quando implementate correttamente, le personalizzazioni consentono di automatizzare i task con la gestione degli oggetti.

Personalizzazione delle pagine delle proprietà

Se si dispone dei poteri di amministrazione di DRA, è possibile personalizzare i moduli delle proprietà degli oggetti utilizzati nel proprio ruolo di gestione di Active Directory in base al tipo di oggetto. Questo prevede la creazione e la personalizzazione di nuove pagine degli oggetti in base ai tipi di oggetti integrati in DRA. È anche possibile modificare le proprietà dei tipi di oggetti integrati.

Gli oggetti delle proprietà sono chiaramente definiti nell'elenco Pagine delle proprietà all'interno della console Web consentendo di individuare facilmente quali pagine di un oggetto sono integrate, quali pagine integrate sono personalizzate e quali pagine non sono integrate e sono state create dall'amministratore.

Personalizzazione di una pagina delle proprietà di un oggetto

È possibile personalizzare i moduli delle proprietà degli oggetti aggiungendo o rimuovendo le pagine, modificando i campi e le pagine esistenti e creando gestori personalizzati per gli attributi delle proprietà. I gestori personalizzati su un campo vengono eseguiti ogni volta che viene modificato il valore del campo. È possibile anche configurare l'intervallo di tempo, in modo che l'amministratore possa specificare se i gestori devono essere eseguiti immediatamente (alla pressione di qualunque tasto), quando il campo perde lo stato attivo, o dopo un ritardo di tempo specificato.

L'elenco di oggetti presente in Pagine delle proprietà fornisce, per ciascun tipo di oggetto, i tipi di operazione Crea oggetto e Modifica proprietà. Queste sono le operazioni principali eseguite dall'amministratore aggiunto sulla Console Web. Tali operazioni vengono eseguite accedendo a **Gestione** > **Ricerca** o **Ricerca avanzata**. Qui è possibile creare oggetti dal menu a discesa Crea o modificare gli oggetti esistenti selezionati nella tabella dei risultati della ricerca tramite l'icona Proprietà.

Per personalizzare la pagina delle proprietà di un oggetto nella console Web:

1. Eseguire il login alla console Web con i privilegi di amministrazione di DRA.
2. Accedere ad **Amministrazione** > **Personalizzazione** > **Pagine delle proprietà**.
3. Selezionare un tipo di oggetto e di operazione (Crea oggetto o Modifica proprietà) nell'elenco Pagine delle proprietà.
4. Fare clic sull'icona **Proprietà** .
5. Personalizzare il modulo delle proprietà dell'oggetto effettuando una o più delle seguenti operazioni, quindi applicare le modifiche:
   - Aggiungere una nuova pagina delle proprietà mediante **+ Aggiungi pagine**
   - Riordinare ed eliminare pagine delle proprietà
   - Selezionare una pagina delle proprietà e personalizzarla:
     - Riordinare i campi di configurazione nella pagina:
     - Modificare i campi o i campi secondari:
     - Aggiungere uno o più campi: o **Inserire un nuovo campo**
     - Rimuovere uno o più campi:
   - Creare gestori personalizzati per le proprietà utilizzando gli script, le caselle per il testo del messaggio o le query (LDAP, DRA o REST)

     Per ulteriori informazioni sull'uso dei gestori personalizzati, vedere "Aggiunta di gestori personalizzati" nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Creazione di una nuova pagina delle proprietà dell'oggetto

Per creare una nuova pagina delle proprietà dell'oggetto:

1. Eseguire il login alla console Web con i poteri di amministrazione di DRA, accedere ad **Amministrazione** > **Personalizzazione** > **Pagine delle proprietà**, quindi fare clic su **Crea**.
2. Creare il modulo iniziale delle proprietà dell'oggetto definendo il nome, l'icona, il tipo dell'oggetto e la configurazione dell'operazione.

   Dopo aver fatto clic su **OK**, le azioni di creazione vengono aggiunte al menu a discesa Crea, mentre le azioni delle proprietà vengono visualizzate nel modulo dell'oggetto quando l'utente seleziona e modifica un oggetto dall'elenco di ricerca.
3. Personalizzare il nuovo modulo in base alle esigenze. Vedere la sezione Personalizzazione di una pagina delle proprietà di un oggetto.

Gestione degli oggetti nella console Web

Per gestire gli oggetti nella console Web, passare al titolo Gestione. Qui è possibile eseguire una ricerca per tipo di oggetto per gli oggetti nei domini gestiti, nei tenant di Azure, nei container e nel Cestino. All'interno di un dominio o un tenant di Azure è possibile gestire ed eseguire azioni sugli oggetti Active Directory e Azure Active Directory tramite DRA.

Se si seleziona un oggetto nell'elenco dei risultati della ricerca, tutte le azioni pertinenti che è possibile eseguire su tale oggetto sono disponibili sulla barra delle applicazioni sopra la griglia. Le opzioni disponibili si basano sul tipo di oggetto selezionato, i componenti attualmente configurati per DRA e i privilegi di amministratore assegnati.

Per modificare le proprietà di un oggetto, spostare il mouse sull'oggetto e fare clic sull'icona **Proprietà** visualizzata sulla riga dell'oggetto. In questa pagina è possibile accedere a tutte le pagine delle proprietà dell'oggetto nel riquadro di navigazione sinistro.

Importante: Se si desidera **proteggere un oggetto da una cancellazione accidentale**, scorrere fino alla fine della sezione**Generale** nella pagina Proprietà, selezionare la casella di controllo per abilitare questa funzione e scegliere **Applica** per applicare le modifiche.

Per ulteriori informazioni sulle azioni che è possibile eseguire sugli oggetti, vedere i seguenti argomenti:

- Gestione di oggetti Active Directory
- Gestione degli oggetti Azure
- Gestione delle caselle postali e delle cartelle pubbliche di Exchange
- Gestione delle risorse

Generazione di rapporti di Cronologia modifiche

Se la Cronologia modifiche è configurata dall'amministratore DRA e si dispone del potere **Generate UI Reports** (Genera rapporti UI), è possibile generare rapporti di Cronologia modifiche ed esportare i rapporti per gli oggetti gestiti in DRA. Sono incluse le modifiche apportate all'interno e all'esterno di DRA. È possibile generare rapporti della cronologia delle modifiche solo dalla console Web, che include i seguenti tipi di rapporti:

- Modifiche apportate dall'utente
- Modifiche apportate all'utente
- Caselle postali dell'utente create dall'utente
- Caselle postali dell'utente cancellate dall'utente
- Indirizzi e-mail di gruppo o dei contatti definiti dall'utente
- Indirizzi e-mail di gruppo o dei contatti cancellati dall'utente
- Attributi virtuali creati o disabilitati dall'utente
- Oggetti spostati dall'utente

Per generare rapporti di Cronologia modifiche unificata (UCH, Unified Change History):

1. Avviare la console Web.
2. Accedere a **Gestione > Ricerca**.
3. Definire i criteri di ricerca utilizzando le opzioni **Ricerca per**, **search term** (termine di ricerca) e **Filtri**.
4. Fare clic sul pulsante **Ricerca** per visualizzare i risultati della ricerca.
5. Selezionare gli oggetti per i quali si desidera generare i rapporti.
6. Fare clic sull'icona **Visualizza rapporti cronologia modifiche** .

   Nel modulo Rapporto cronologia modifiche unificato è possibile modificare e generare i criteri del rapporto dalle opzioni **Tipo**, **Oggetti di destinazione** e **Filtri**, in modo da includere la definizione dei server in cui vengono rilevate le modifiche (DRA e Change Guardian).
7. Fare clic su **Genera** per recuperare i dati di revisione e generare un rapporto della Cronologia modifiche unificata.
8. È possibile ordinare ed esportare il rapporto nel formato richiesto, ad esempio HTML e CSV.

Per creare un file CSV del rapporto visualizzato, è possibile esportare tutte le modifiche generate o solo quelle visualizzate nella pagina corrente, scegliendo una delle seguenti opzioni dopo aver generato il rapporto seguendo i passaggi descritti sopra:

- Fare clic su **Esporta tutto** e salvare il rapporto esportato.
- Fare clic su **Esporta pagina corrente** e salvare il rapporto esportato.

  Se necessario, è possibile modificare il numero di modifiche che vengono mostrate nella pagina, fino a 200 elementi.

Utilizzo di Workflow Automation

Con Workflow Automation è possibile automatizzare i processi IT mediante l'avvio di moduli di workflow che vengono eseguiti all'esecuzione di un workflow o che vengono attivati da un evento di workflow denominato, creato nel server di Workflow Automation.

Quando creati o modificati, i moduli del workflow vengono salvati sul server Web. Quando si accede alla console Web per il server, si avrà accesso ai moduli in base ai poteri delegati e alla modalità di configurazione dei moduli. I moduli sono generalmente disponibili per tutti gli utenti mediante l'utilizzo delle credenziali del server Web. Per poter inviare il modulo sono necessari poteri appropriati.

Avvio di un modulo del workflow: i workflow vengono creati sul server di Workflow Automation, che deve essere integrato con DRA tramite la console Web. Per salvare un nuovo modulo, è necessario che nelle proprietà del modulo sia configurata l'opzione **Avvia workflow specifico** o **Attiva workflow in base all'evento**. Di seguito sono fornite ulteriori informazioni su queste opzioni:

- **Avvio di un workflow specifico:** questa opzione consente di elencare tutti i workflow disponibili nell'ambiente di produzione del server dei workflow per DRA. Affinché i workflow siano visualizzati in questo elenco, devono essere creati nella cartella `DRA_Workflows` nel server di Workflow Automation.
- **Attiva workflow in base all'evento:** questa opzione consente di eseguire i workflow con trigger predefiniti. I workflow con trigger vengono inoltre creati nel server di Workflow Automation.

Nota: solo per i moduli di workflow configurati con Avvia workflow specifico è disponibile una cronologia di esecuzione che può essere utilizzata per eseguire query nel riquadro di ricerca principale in **Task** > **Richieste**.

Ulteriori informazioni su Workflow Automation sono incluse nelle seguenti guide nel sito della documentazione di DRA:

- *DRA Administrator Guide* (Guida all'amministrazione di DRA)
- *WFA Administrator Guide* (Guida all'amministrazione di WFA)
- *WFA User Guide* (Guida dell'utente di WFA)
- *WFA Process Authoring Guide* (Guida alla creazione dei processi di WFA)

Gestione account e risorse

Il nodo Account and Resource Management (Gestione account e risorse) nella Console di delega e configurazione consente di accedere alla maggior parte dei task degli amministratori aggiunti DRA, soddisfacendo le esigenze di gestione aziendale, a partire dalle operazioni di amministrazione di base fino a problemi complessi sottoposti all'help desk. Attraverso Account and Resource Management (Gestione account e risorse) è possibile eseguire task di gestione di account e risorse e gestire le caselle postali di Microsoft Exchange.

Account and Resource Management (Gestione account e risorse) contiene i seguenti nodi:

Tutti i miei oggetti gestiti

Consente di gestire gli oggetti, ad esempio gli account utente, i gruppi, i contatti, le risorse, i gruppi dinamici, i gruppi di distribuzione dinamici, le caselle postali risorsa e le cartelle pubbliche per ciascun dominio per cui l'utente dispone di poteri.

Temporary Group Assignments (Assegnazioni temporanee ai gruppi)

Consente di gestire le appartenenze ai gruppi per gli utenti che richiedono l'appartenenza al gruppo solo per un periodo di tempo specifico.

Query avanzate

Consente di creare, salvare, importare, esportare, copiare e gestire query con attributi virtuali e LDAP sia personali che pubbliche.

Cestino

Consente di gestire gli account utente, i gruppi, i contatti e le risorse cancellati per un dominio Microsoft Windows in cui è abilitato il Cestino.

Per accedere al nodo Account and Resource Management (Gestione account e risorse), fare clic su **Delegation and Configuration (Delega e configurazione)** nella cartella di programma NetIQ Administrator (Amministratore NetIQ) ed espandere il nodo Delegation and Configuration (Delega e configurazione) nella console.

Quando si avvia la Console di delega e configurazione, la connessione viene inizialmente stabilita con il server di amministrazione maggiormente disponibile nel dominio locale. Il server di amministrazione maggiormente disponibile è il server più vicino, che generalmente è un server del sito di rete. Grazie alla ricerca del server di amministrazione maggiormente disponibile, DRA è in grado di fornire una connessione più veloce e prestazioni migliori.

Per ulteriori informazioni sull'utilizzo di Account and Resource Management (Gestione account e risorse), vedere i seguenti argomenti:

Connessione a un server di amministrazione o a un dominio gestito

Di default, DRA si connette al server di amministrazione maggiormente disponibile per un computer o un dominio gestito. Il server di amministrazione maggiormente disponibile è il server più vicino, che generalmente è un server del sito di rete. Se nel sito non è presente un server di amministrazione, DRA si connette al successivo server disponibile nel dominio o nel sottoalbero gestito. È inoltre possibile specificare il server di amministrazione o un dominio a cui si desidera connettersi.

Al primo avvio delle interfacce utente, DRA inizialmente si connette al dominio dell'account di login dell'utente. Se si è connessi a un dominio che non è gestito da un server di amministrazione oppure DRA non riesce a connettersi a un server di amministrazione per tale dominio, potrebbe essere visualizzato un messaggio di errore. Verificare che il server di amministrazione sia disponibile e riprovare.

Per connettersi a un server di amministrazione:

1. Nel menu File fare clic su **Connect to DRA server** (Connetti al server DRA).
2. Fare clic su **Connect to this DRA server** (Connetti a questo server DRA).
3. Digitare il nome del server di amministrazione utilizzando il seguente formato: *nomecomputer*.
4. Fare clic su **OK**.

Per connettersi a un dominio o a un computer gestito:

1. Nel menu File fare clic su **Connect to DRA server** (Connetti al server DRA)
2. Selezionare l'opzione appropriata, quindi digitare il nome del dominio o del computer gestito.

3 Ad esempio, per connettersi al dominio HOULAB, fare clic su **Connect to a DRA server that manages this domain (Connetti a un server DRA che gestisce questo dominio)**, quindi digitare HOULAB.

4 Per specificare un server di amministrazione per il dominio o il computer gestito, fare clic su **Advanced**(Avanzate), quindi selezionare l'opzione appropriata.

5 Fare clic su **OK**.

Modifica del titolo della console

È possibile modificare le informazioni visualizzate nella barra del titolo della Console di delega e configurazione. Per motivi di chiarezza e comodità, è possibile aggiungere il nome utente con cui è stata avviata la console e il server di amministrazione a cui questa è connessa. In ambienti complessi, in cui è necessario connettersi a più server di amministrazione utilizzando credenziali differenti, questa funzione consente di capire rapidamente quale console è necessario utilizzare.

Per modificare la barra del titolo della console:

1 Avviare la Console di delega e configurazione.

2 **Fare clic su View (Visualizza)** > **Options** (Opzioni).

3 Selezionare la scheda Window Title (Titolo finestra).

4 Specificare le impostazioni appropriate, quindi fare clic su **OK**.

Personalizzazione delle colonne dell'elenco

È possibile selezionare le proprietà dell'oggetto che DRA deve visualizzare nelle colonne dell'elenco. Questa flessibile funzione consente di personalizzare gli elementi dell'interfaccia utente, ad esempio gli elenchi dei risultati della ricerca, per soddisfare al meglio le esigenze di amministrazione specifiche della propria azienda. È possibile impostare le colonne per visualizzare il nome di login dell'utente o il tipo di gruppo, affinché sia possibile trovare e ordinare in modo rapido ed efficace i dati di cui si ha bisogno.

Per personalizzare le colonne dell'elenco:

1 Selezionare il nodo appropriato. Ad esempio, per specificare quali colonne mostrare quando si visualizzano i risultati della ricerca sugli oggetti gestiti, selezionare **Tutti i miei oggetti gestiti**.

2 Nel menu Visualizza fare clic su **Choose Columns** (Scegli colonne).

3 Nell'elenco delle proprietà disponibili per il nodo selezionare le proprietà dell'oggetto che si desidera visualizzare.

4 Per modificare l'ordine delle colonne, selezionare una colonna, quindi fare clic su **Sposta su** o su **Sposta giù**.

5 Per specificare la larghezza delle colonne, selezionare una colonna, quindi digitare il numero di pixel appropriato nell'apposito campo.

6 Fare clic su **OK**.

Gestione degli oggetti in Account and Resource Management (Gestione account e risorse)

Per gestire gli oggetti in Account and Resource Management (Gestione account e risorse), è possibile selezionare **Tutti i miei oggetti gestiti** o un nodo secondario nell'albero della directory. In questa pagina è possibile eseguire una ricerca per tipo di oggetto per gli oggetti in domini, container e unità organizzative.

Se si seleziona un oggetto nell'elenco dei risultati della ricerca, tutte le azioni pertinenti che è possibile eseguire su tale oggetto sono disponibili nel menu **Task** sulla barra degli strumenti o nel menu di scelta rapida. Le opzioni disponibili si basano sul tipo di oggetto selezionato, i componenti attualmente configurati per DRA e i privilegi di amministratore assegnati.

Per modificare le proprietà di un oggetto, selezionare l'oggetto, quindi fare clic su **Proprietà** nel menu **Task**. In questa pagina è possibile accedere a tutte le pagine delle proprietà dell'oggetto facendo clic su collegamenti alle pagine nel riquadro di navigazione sinistro.

Importante: Se si desidera **proteggere un oggetto da una cancellazione accidentale**, selezionare l'oggetto e aprire **Proprietà**, selezionare **Generale** nel riquadro di navigazione, selezionare la casella di controllo per abilitare questa funzione e scegliere **Applica** per applicare le modifiche.

Per ulteriori informazioni sulle azioni che è possibile eseguire sugli oggetti, vedere i seguenti argomenti:

- Gestione di oggetti Active Directory
- Gestione delle caselle postali e delle cartelle pubbliche di Exchange
- Gestione delle risorse

Esecuzione di query avanzate salvate

Utilizzando le query avanzate è possibile cercare utenti, contatti, gruppi, computer, stampanti, unità organizzative e qualsiasi altro oggetto supportato da DRA. Se si dispone dei diritti per eseguire query avanzate salvate, è possibile eseguire le query avanzate disponibili nell'elenco **Saved Queries** (Query salvate) per qualsiasi container del nodo Account and Resource Management (Gestione account e risorse). Per ulteriori informazioni sui poteri assegnati, vedere la sezione Visualizzazione dei poteri e dei ruoli assegnati.

Per eseguire query avanzate salvate:

1. Espandere **Account and Resource Management**(Gestione account e risorse) > **Tutti i miei oggetti gestiti**.
2. Selezionare il container appropriato. Se, ad esempio, si desidera che DRA ricerchi informazioni sull'account utente, selezionare **Utenti**.
3. Per visualizzare il riquadro Advanced Search (Ricerca avanzata), fare clic su **Advanced Search** (Ricerca avanzata).
4. Nel riquadro Ricerca avanzata selezionare una query di ricerca avanzata dall'elenco **Saved Queries** (Query salvate).
5. Fare clic su **Load Query** (Carica query), quindi fare clic su **Find Now** (Trova ora).

Ripristino delle impostazioni della console

DRA consente di ridimensionare le finestre e di mantenere le dimensioni scelte. DRA mantiene anche molte altre impostazioni, incluso l'ultimo server di amministrazione a cui si è connesso l'utente, le colonne che ha aggiunto o rimosso dai risultati dell'elenco e la larghezza delle colonne. Se si desidera ripristinare queste impostazioni sui valori originali, con il quale si è installato DRA, l'opzione Restore Default Settings (Ripristina impostazioni di default) consente di eseguire questa operazione.

Per ripristinare le impostazioni di default della console:

1. Fare clic su **Visualizza** > **Opzioni**.
2. Selezionare la scheda **Saved Settings**(Impostazioni salvate).
3. Verificare le informazioni contenute nella finestra, quindi fare clic su **Restore Default Settings** (Ripristina impostazioni di default).

Restrizioni dei caratteri speciali

Non è possibile utilizzare i seguenti caratteri speciali per la denominazione di account utente, gruppi, contatti, unità organizzative, computer, viste attive, gruppi amministratori aggiunti, ruoli, policy o trigger di automazione. Queste restrizioni per i nomi si applicano al nome dell'oggetto e al nome della regola che definisce l'oggetto.

Denominazione di account utente, gruppi e computer

Quando si specifica un nome in sistemi operativi precedenti a Windows 2000, non è possibile utilizzare i seguenti caratteri speciali:

Barra rovesciata	\
Due punti	:
Virgola	,
Virgolette	"
Segno di uguale	=
Barra	/
Maggiore di	>
Parentesi quadra aperta	[
Minore di	<
Segno più	+
Parentesi quadra chiusa	]
Punto e virgola	;
Barra verticale	|

Importante: Per la gestione delle cartelle pubbliche, il carattere \ non è supportato.

Per la denominazione di account utente, gruppi e computer nei domini di Microsoft Windows, è possibile utilizzare qualsiasi carattere speciale.

Denominazione di contatti e unità organizzative

Per la denominazione di contatti e unità organizzative è possibile utilizzare qualsiasi carattere speciale.

Denominazione di viste attive, gruppi amministratori aggiunti e ruoli

Per la denominazione di viste attive, gruppi amministratori aggiunti e ruoli non è possibile utilizzare la barra rovesciata (\).

Denominazione di policy e di trigger di automazione

Per la denominazione di policy e di trigger di automazione non è possibile utilizzare la barra rovesciata (\).

Caratteri non validi in Azure

L'utilizzo di caratteri non validi compromette la sincronizzazione tra Azure Active Directory e la directory locale. Per ulteriori informazioni su questi caratteri non validi, vedere l'argomento secondario *Preparazione di oggetti directory e attributi* sul sito Web di supporto di Microsoft Office.

Per accertarsi che tali caratteri non vengano utilizzati nelle proprietà della casella postale online, effettuare le seguenti operazioni:

1. Fare clic sul nodo Configuration Management (Gestione configurazione) nella Console di delega e configurazione e selezionare **Update Administration Server Options** (Aggiorna opzioni server di amministrazione).
2. Fare clic su **Azure Sync** (Sincronizzazione Azure) nel menu della scheda.
3. Fare clic su **Enforce online mailbox policies for invalid characters and character length** (Applica policy di casella postale online per caratteri non validi e lunghezza dei caratteri) e infine su **OK**.

Utilizzo di caratteri jolly

DRA supporta i caratteri jolly in molti campi all'interno delle console DRA e nei comandi dell'interfaccia della riga di comando. I caratteri jolly consentono di definire le regole che stabiliscono una corrispondenza di più oggetti con una condizione o standard specifici, ad esempio una convenzione di denominazione. È possibile utilizzare i caratteri jolly anziché le espressioni regolari per ridurre o ampliare l'ambito della regola. La corrispondenza dei caratteri jolly è senza distinzione maiuscole/minuscole. È inoltre possibile utilizzare i caratteri jolly punto interrogativo (?),

asterisco (*) o cancelletto (#) come caratteri normali, anteponendo come prefisso una barra rovesciata (\) al carattere jolly in questione. Ad esempio, per ricercare abc *, è possibile digitare il testo da ricercare abc\ *.

DRA supporta i seguenti caratteri jolly. Non è possibile utilizzare i caratteri jolly nei nomi.

Elemento corrispondente	Carattere	Definizione
Qualsiasi carattere	Punto interrogativo ?	Corrisponde esattamente a un carattere
Qualsiasi numero	Simbolo di cancelletto #	Corrisponde a una cifra
Qualsiasi carattere, 0 o più elementi	Asterisco *	Corrisponde a zero o a più caratteri

Nella tabella seguente sono forniti alcuni esempi di specifiche di caratteri jolly, gli elementi a cui corrispondono e gli elementi a cui non corrispondono

Esempio	Elementi corrispondenti	Elementi non corrispondenti
Den???	Denton e Dennis	Denison
El ????o	Campo EL ed El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA non supporta specifiche dei caratteri jolly contenenti operazioni logiche.

Visualizzazione dei poteri e dei ruoli assegnati

I ruoli e i poteri definiscono il modo in cui l'utente gestisce gli oggetti. Un ruolo è un gruppo di poteri che fornisce le autorizzazioni necessarie per eseguire un task di amministrazione specifico, ad esempio la creazione di un account utente o lo spostamento di directory condivise.

L'amministratore DRA assegna i ruoli, aggiunge l'utente a gruppi di amministratori aggiunti specifici e lo associa a viste attive (gruppi di oggetti del dominio che l'utente può gestire). È possibile visualizzare queste assegnazioni mediante la Console di delega e configurazione. Non è necessario disporre di alcun potere ausiliario per visualizzare i ruoli e i poteri assegnati all'utente.

Per visualizzare i poteri e i ruoli assegnati:

1. Nel menu File fare clic su **DRA Properties** (Proprietà DRA).
2. Fare clic su **Poteri**.
3. Selezionare la vista appropriata. Ad esempio, fare clic su **Flat View** (Vista semplice) per visualizzare una tabella contenente le appartenenze al proprio gruppo di amministratori aggiunti, i poteri e i ruoli assegnati e le viste attive associate.
4. Espandere l'elemento appropriato. Ad esempio, nella colonna **Has Power** (Ha il potere) espandere **Roles and Powers** (Ruoli e poteri) per visualizzare i singoli ruoli o poteri assegnati all'utente.
5. Fare clic su **OK**.

Visualizzazione del numero di versione del prodotto e delle correzioni HotFix installate

È possibile visualizzare il numero di versione del prodotto e le correzioni HotFix installate dalla finestra di dialogo DRA Properties (Proprietà DRA). Questa finestra di dialogo fornisce il numero di versione ed elenchi delle correzioni HotFix installate per il server di amministrazione e il computer client DRA.

Per visualizzare il numero di versione del prodotto e le correzioni HotFix installate:

1. Nel menu File fare clic su **DRA Properties** (Proprietà DRA).
2. Fare clic su **Generale**.
3. Visualizzare le informazioni necessarie.
4. Fare clic su **OK**.

Visualizzazione della licenza attuale

Per DRA è necessario disporre di un file della chiave di licenza. È possibile visualizzare la licenza del prodotto da qualsiasi computer del server di amministrazione. Per visualizzare la licenza del prodotto, non è necessario alcun potere ausiliario.

Per visualizzare la propria licenza:

1. Nel menu File fare clic su **DRA Properties** (Proprietà DRA).
2. Fare clic su **License** (Licenza).
3. Esaminare le proprietà della licenza, quindi fare clic su **OK**.

Recupero di una password di BitLocker

Microsoft BitLocker memorizza le proprie password di recupero in Active Directory. Con i poteri necessari è possibile utilizzare la funzione di recupero di BitLocker di DRA per trovare e recuperare le password BitLocker perse per gli utenti finali.

Importante: Prima di utilizzare la funzione Password di recupero BitLocker, verificare che il computer sia assegnato a un dominio e che BitLocker sia attivato.

Visualizzazione e copia di una password di recupero BitLocker

Se la password BitLocker per un computer viene persa, può essere reimpostata mediante la chiave Recovery Password (Password di recupero) dalle proprietà del computer in Active Directory. Copiare la chiave della password e fornirla all'utente finale.

Per visualizzare e copiare la password di recupero:

1. Avviare la Console di delega e configurazione e passare a **Account and Resource Management** (Gestione account e risorse) > **Tutti i miei oggetti gestiti**.
2. Selezionare il dominio ed eseguire una ricerca per visualizzare un elenco di tutti i computer presenti nel dominio.

3 Nell'elenco di computer fare clic con il pulsante destro del mouse sul computer desiderato, quindi selezionare **Proprietà**> **Password di recupero BitLocker**.

4 Fare clic con il pulsante destro del mouse e copiare la password di recupero BitLocker, quindi incollare il testo della password in un file di testo.

Ricerca di una password di recupero

Se è stato modificato il nome di un computer, è necessario cercare la password di recupero nel dominio utilizzando i primi otto caratteri dell'ID della password.

Per trovare una password di recupero utilizzando un ID della password:

1 Avviare la Console di delega e configurazione e passare a **Account and Resource Management** (Gestione account e risorse) > **Tutti i miei oggetti gestiti**.

2 Fare clic con il pulsante destro del mouse sul**dominio gestito**, quindi fare clic su **Trova password di recupero BitLocker**.

Per vedere come trovare i primi otto caratteri della password di recupero, vedere la sezione Visualizzazione e copia di una password di recupero BitLocker.

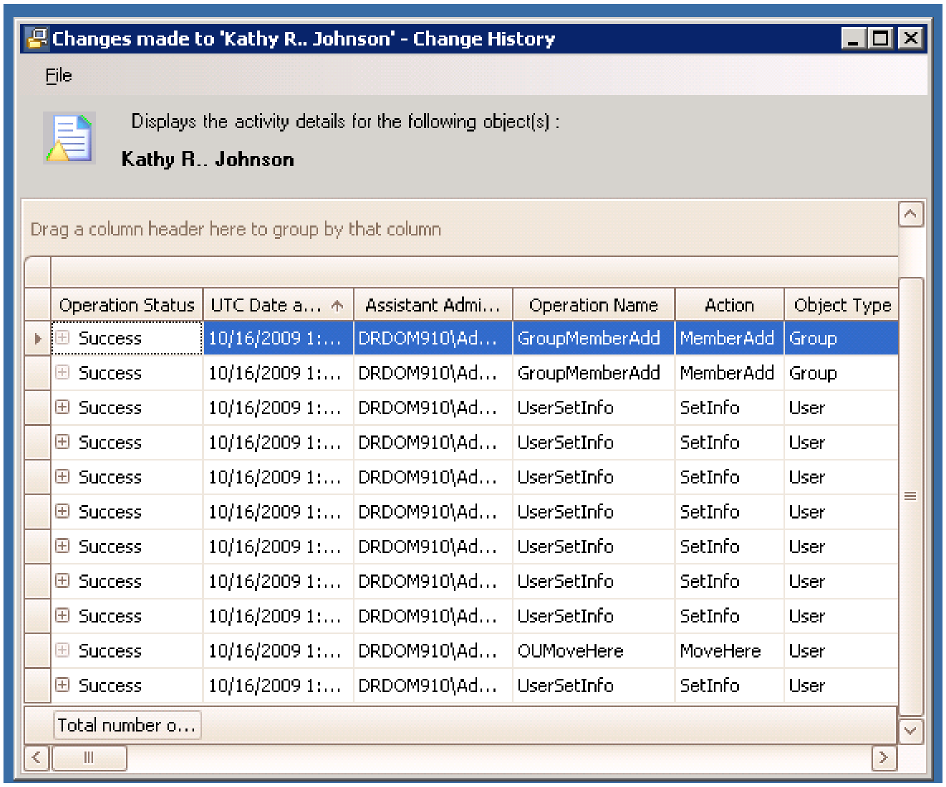
3 Nella pagina **Trova password di recupero BitLocker** incollare i caratteri copiati nel campo di ricerca, quindi fare clic su **Cerca**.

DRA Reporting

DRA Reporting fornisce rapporti integrati e pronti all'uso che consentono di tenere traccia rapidamente di account duplicati, ultimi login degli account, dettagli delle caselle postali di Microsoft Exchange e molto altro ancora. Reporting fornisce inoltre informazioni dettagliate e in tempo reale sulle modifiche apportate nell'ambiente, compresi i valori precedenti e successivi delle proprietà modificate. È possibile esportare, stampare o visualizzare i rapporti o pubblicarli in Microsoft SQL Server Reporting Services.

DRA fornisce due metodi di generazione dei rapporti che consentono di raccogliere ed esaminare le definizioni degli account utente, dei gruppi e delle risorse presenti nel proprio dominio: **rapporti Activity Detail** (Dettagli attività) e **rapporti Gestione di DRA**. I rapporti Activity Detail (Dettagli attività), che vengono visualizzati tramite la Console di delega e configurazione, forniscono informazioni in tempo reale sulle modifiche relativamente agli oggetti del proprio dominio. Grazie a questi rapporti, è ad esempio possibile visualizzare un elenco delle modifiche apportate a un oggetto o da un oggetto durante un periodo di tempo specificato.

La seguente figura mostra un esempio del rapporto Activity Detail (Dettagli attività):



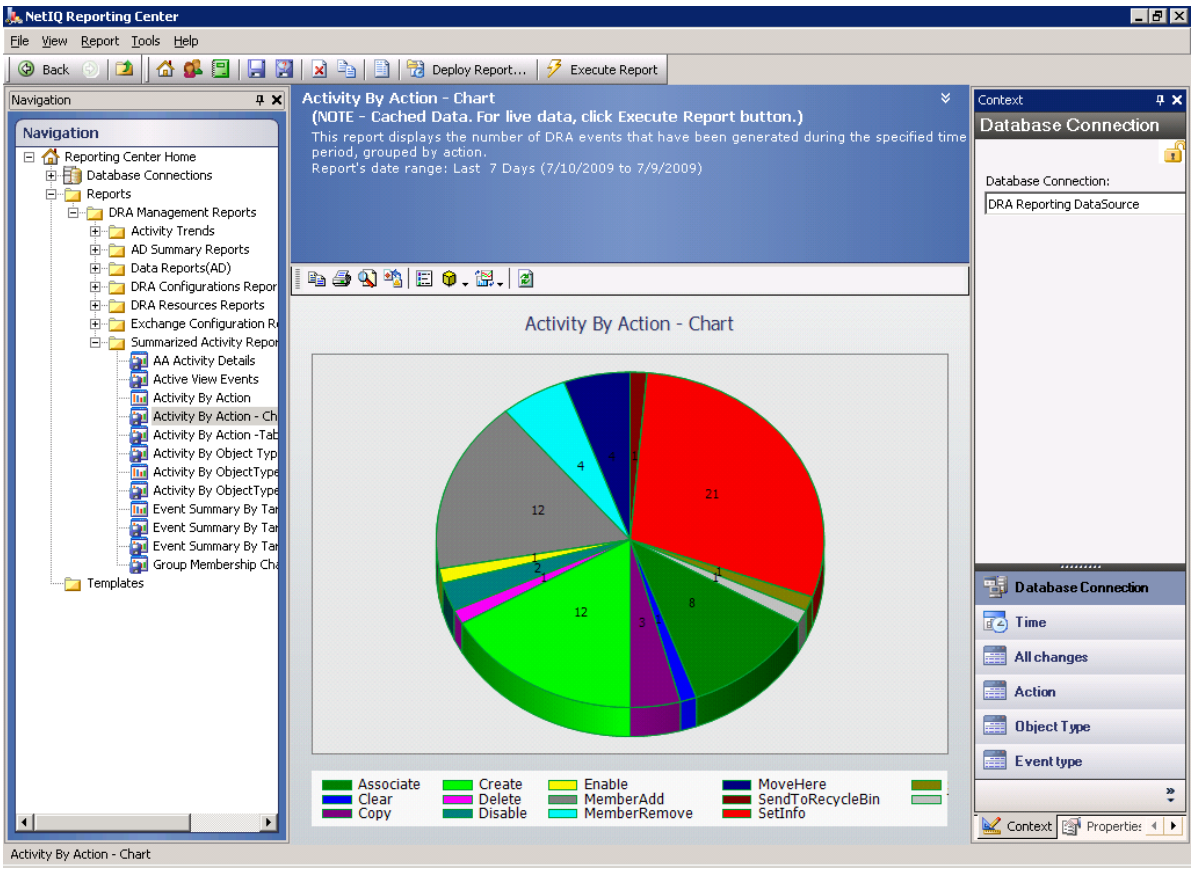
I rapporti facoltativi **Management** (Gestione) di DRA, visualizzati tramite NetIQ Reporting Center, forniscono informazioni su attività e configurazione oltre a informazioni di riepilogo sugli eventi che si verificano nei domini gestiti. Alcuni rapporti Gestione sono disponibili come rappresentazioni grafiche dei dati. Questi rapporti integrati possono essere inoltre personalizzati per fornire esattamente le informazioni di cui si ha bisogno.

Mediante i rapporti Gestione è ad esempio possibile visualizzare un grafico che mostri il numero di eventi in ciascun dominio gestito durante un periodo di tempo specificato La generazione dei rapporti consente di visualizzare i dettagli sul modello di sicurezza DRA, come le definizioni della vista attiva e del gruppo amministratori aggiunti.

Prima di poter visualizzare questi rapporti, è necessario installare e configurare i rapporti Gestione facoltativi. Per ulteriori informazioni sull'installazione dei componenti di generazione dei rapporti, vedere la *Installation Guide* (Guida all'installazione). Per ulteriori informazioni su DRA Reporting vedere la sezione "DRA Reporting" a pagina 32.

Avviare la console Reporting Center in NetIQ > gruppo dei programmi Reporting Center.

La seguente figura mostra l'interfaccia di Reporting Center con i rapporti Gestione di DRA selezionati.



Per ulteriori informazioni su DRA Reporting, vedere i seguenti argomenti:

- “Informazioni su DRA Reporting” a pagina 34
- “Modalità con cui DRA utilizza gli archivi dei log” a pagina 35
- “Informazioni su data e ora” a pagina 36
- “Task di DRA Reporting” a pagina 36

Informazioni su DRA Reporting

DRA Reporting fornisce due metodi di generazione dei rapporti che consentono di visualizzare le ultime modifiche apportate nel proprio ambiente e di raccogliere ed esaminare informazioni sulle definizioni di account utente, gruppi e risorse presenti nel proprio dominio.

Rapporti Activity Detail (Dettagli attività)

Questi rapporti, accessibili mediante il nodo Account and Resource Management (Gestione account e risorse) della Console di delega e configurazione, forniscono informazioni in tempo reale sulle modifiche apportate agli oggetti del dominio.

Rapporti Gestione di DRA

Accessibili mediante Reporting Center, questi rapporti forniscono informazioni sulle attività e sulla configurazione oltre a informazioni di riepilogo sugli eventi che si verificano nei domini gestiti. Alcuni rapporti sono disponibili come rappresentazioni grafiche dei dati.

Mediante i rapporti Activity Detail (Dettagli attività), è ad esempio possibile visualizzare un elenco delle modifiche apportate a un oggetto o da un oggetto durante un periodo di tempo specificato. È anche possibile visualizzare un grafico che mostri il numero di eventi che si verificano in ciascun dominio gestito durante un periodo di tempo specificato mediante i rapporti Gestione. Reporting consente di visualizzare i dettagli sul modello di sicurezza di DRA, come le definizioni delle viste attive e dei gruppi di amministratori aggiunti.

DRA disabilita le funzioni e i rapporti non supportati dalla licenza dell'utente. Inoltre, per eseguire e visualizzare i rapporti, è necessario disporre dei poteri appropriati. Di conseguenza, si potrebbe non disporre dell'accesso ad alcuni rapporti.

I rapporti Gestione di DRA possono essere installati e configurati come una funzione facoltativa e vengono visualizzati in Reporting Center. Quando si abilita e si configura la raccolta dei dati, DRA raccoglie informazioni relative agli eventi sottoposti a revisione e le esporta in un database SQL Server in base a una pianificazione definita dall'utente. Quando ci si connette a questo database nel Reporting Center, sarà possibile accedere a oltre 60 rapporti integrati:

- Rapporti sulle attività che mostrano il tipo di azione e quando è stata eseguita
- Rapporti sulla configurazione che mostrano lo stato di Active Directory o di DRA in un punto temporale specifico
- Rapporti di riepilogo che mostrano il volume delle attività

Per ulteriori informazioni sulla configurazione della raccolta dei dati per i rapporti Gestione, vedere la *Administration Guide* (Guida dell'amministratore).

Modalità con cui DRA utilizza gli archivi dei log

Per esaminare e fornire informazioni sulle azioni dell'amministratore aggiunto, DRA registra tutte le operazioni degli utenti nell'archivio dei log nel computer server di amministrazione. Le operazioni degli utenti includono tutti i tentativi di modifica delle definizioni, ad esempio l'aggiornamento degli account utente, la cancellazione dei gruppi o la ridefinizione delle viste attive. DRA registra inoltre le operazioni interne specifiche, ad esempio l'inizializzazione del server di amministrazione e le informazioni sul server correlate. Oltre alla registrazione di questi eventi, DRA registra i valori precedenti e successivi di un evento, consentendo di sapere esattamente cosa è stato modificato.

Il programma utilizza una cartella, **NetIQLogArchiveData**, denominata **archivio dei log** per memorizzare senza rischi i dati di log archiviati. DRA archivia i log nel corso del tempo, quindi cancella i dati precedenti per creare spazio per i dati più recenti mediante un processo denominato pulitura.

DRA utilizza gli eventi di revisione memorizzati nei file degli archivi dei log per visualizzare i rapporti Activity Detail (Dettagli attività), mostrando, ad esempio, le modifiche apportate a un oggetto durante un periodo di tempo specificato. È inoltre possibile configurare DRA per esportare le informazioni da questi file di archivio dei log in un database SQL Server che NetIQ Reporting Center utilizza per visualizzare i rapporti Gestione.

DRA registra sempre gli eventi di revisione nell'archivio dei log. È possibile abilitare o disabilitare la funzione di registrazione degli eventi di DRA nei registri degli eventi di Windows.

Per ulteriori informazioni sulla funzione di revisione di DRA, vedere la *Administrator Guide* (Guida dell'amministratore).

Informazioni su data e ora

Per la visualizzazione dei rapporti, DRA utilizza il **formato breve della data** e il **formato dell'ora** specificati nell'applicazione Impostazioni internazionali nel Pannello di controllo. I rapporti DRA mostrano la data e l'ora UTC nonché la data e l'ora locale degli eventi. I rapporti DRA supportano i formati di data seguenti:

- `m/g/aa`
- `m-g-aa`
- `m/g/aaaa`
- `m-g-aaaa`
- `mm/gg/aa`
- `mm-gg-aa`
- `gg/mm/aaaa`
- `mm-gg-aaaa`
- `gg/mm/aa`
- `gg-mm-aa`
- `gg/mm/aaaa`
- `gg-mm-aaaa`

Task di DRA Reporting

Per generare rapporti Gestione di DRA, installare Reporting Center e abilitare la raccolta dei dati in DRA. Per ulteriori informazioni sull'abilitazione della raccolta dei dati, vedere la *Administrator Guide*(Guida dell'amministratore). Per generare i rapporti Activity Detail (Dettagli attività), fare clic con il pulsante destro su un oggetto, quindi fare clic su **Reporting** (Generazione rapporti) per visualizzare le opzioni disponibili per i rapporti su tale oggetto. Le seguenti sezioni consentono di completare i vari task di Reporting.

Visualizzazione dei rapporti Activity Detail (Dettagli attività)

I rapporti Activity Detail (Dettagli attività) visualizzano informazioni sulle modifiche apportate al proprio ambiente. È possibile visualizzare o stampare un rapporto, nonché salvarlo in formato Excel, CSV o TXT. Per visualizzare o stampare i rapporti, è necessario essere associati al ruolo Reporting Administration (Amministrazione generazione rapporti).

Durante la visualizzazione dei rapporti, immettere i criteri per specificare il periodo di tempo di cui si desidera visualizzare le informazioni. È inoltre possibile scegliere di visualizzare un rapporto limitandosi alle modifiche apportate su server DRA specifici, quindi limitare il numero di righe da includere nel rapporto. Se la dimensione del rapporto supera uno dei limiti riportati di seguito, DRA visualizza un messaggio indicante che il rapporto non è stato completato:

- La dimensione supera 500 MB
- Il tempo necessario per eseguire una query su tutti i server DRA supera i 5 minuti
- Il numero di righe da visualizzare è superiore a 1.000

È possibile scegliere di visualizzare il rapporto contenente solo le informazioni recuperate prima del raggiungimento di uno di questi limiti oppure è possibile modificare i criteri per visualizzare un rapporto che li rispetti.

Per visualizzare un rapporto:

1. Nel riquadro sinistro espandere **Tutti i miei oggetti gestiti**.
2. Per specificare l'oggetto di cui si desidera visualizzare un rapporto, effettuare le seguenti operazioni:
   - **2a** ***Se si conosce l'ubicazione dell'oggetto***, selezionare il dominio e l'unità organizzativa contenente l'oggetto.
   - **2b** Nel riquadro Cerca specificare gli attributi dell'oggetto, quindi fare clic su **Find Now** (Trova ora).
3. Nel riquadro con l'elenco fare clic con il pulsante destro del mouse sull'oggetto, quindi fare clic su **Reporting** (Generazione rapporti).
4. Selezionare il tipo di rapporto, ad esempio **Modifiche apportate a NomeOggetto** o **Modifiche apportate da NomeOggetto**. I rapporti disponibili variano a seconda del tipo di oggetto selezionato.
5. Selezionare le date di inizio e di fine per specificare le modifiche che si desidera visualizzare.
6. ***Se si desidera modificare il numero di righe da visualizzare***, digitare un numero sovrascrivendo il valore di default 250.

   Nota: Il numero di righe visualizzato si applica a ciascun server di amministrazione presente nell'ambiente. Se si includono i 3 server di amministrazione nel rapporto e si utilizza il valore di default di 250 righe per la visualizzazione, nel rapporto possono essere visualizzate fino a 750 righe.

7. ***Se si desidera includere solo i server di amministrazione specifici nel rapporto***, selezionare **Restrict query to these DRA servers** (Limita query a questo server DRA) e digitare il nome o i nomi del server o dei server da includere nel rapporto. Separare più nomi di server con le virgole.
8. Fare clic su **OK**.

   Nota: In DRA la visualizzazione delle modifiche recenti nei rapporti potrebbe richiedere fino a 5 secondi. Pertanto, è necessario attendere almeno 5 secondi dopo aver apportato le modifiche prima di tentare di visualizzare un rapporto che le contenga.

Esportazione dei rapporti Activity Detail (Dettagli attività)

È possibile esportare i rapporti Activity Detail (Dettagli attività) nei seguenti formati: XLS, CSV e TXT. Il formato di default è Microsoft Excel.

Per esportare i rapporti Activity Detail (Dettagli attività):

1. Nella finestra del rapporto, menu File, fare clic su **Preview and Export** (Visualizza anteprima ed esporta).
2. Nella finestra di anteprima, menu File, fare clic su **Export Document** (Esporta documento) > **Excel File** (File Excel).

3 Selezionare le opzioni di esportazione, quindi fare clic su **OK**.

4 Nella finestra Sal. con come, digitare un nome per il file e fare clic su **Salva**.

Stampa dei rapporti Activity Detail (Dettagli attività)

Per stampare i rapporti, è necessario essere associati al ruolo Reporting Administration (Amministrazione generazione rapporti). È possibile visualizzare o stampare rapporti Activity Detail (Dettagli attività), nonché salvare un rapporto in vari formati.

Per stampare rapporti Activity Detail (Dettagli attività):

1 Nella finestra del rapporto, menu File, fare clic su **Preview and Export** (Visualizza anteprima ed esporta).

2 Nella finestra di anteprima, menu File, fare clic su **Print** (Stampa).

Visualizzazione dei rapporti Gestione

Per poter visualizzare i rapporti Gestione in Reporting Center è necessario installare DRA Reporting e configurare i servizi di raccolta dati di DRA. Per ulteriori informazioni sull'installazione di DRA Reporting e sulla configurazione dei servizi di raccolta di DRA, vedere la *Administrator Guide*(Guida dell'amministratore).

Quando si accede a Reporting Center il servizio Web utilizza IIS per convalidare le credenziali dell'account, in base al modo in cui il servizio Web è stato configurato durante l'installazione.

Per visualizzare i rapporti Gestione:

1 Eseguire il login al computer in cui è in esecuzione la console Reporting Center.

2 Avviare la **console Reporting Center** nel gruppo di programmi NetIQ >) Reporting Center.

3 Immettere le informazioni richieste nella finestra di dialogo Login e fare clic su **Logon** (Esegui login).

4 Nel riquadro di navigazione espandere **Reports** (Rapporti) > **DRA Management Reports** (Rapporti di gestione DRA).

5 Espandere le categorie di rapporti e individuare un rapporto che si desidera visualizzare.

6 Fare clic sul nome del rapporto nel riquadro di navigazione e il rapporto verrà caricato nel riquadro dei risultati del centro, visualizzando i dati memorizzati nella cache.

7 ***Se si desidera visualizzare il rapporto utilizzando i dati più recenti,*** fare clic su **Execute Report** (Esegui rapporto) nel riquadro dei risultati.

È possibile modificare le impostazioni del contesto di default per visualizzare risultati dei rapporti differenti. Per ulteriori informazioni sulle impostazioni del contesto in Reporting Center vedere la *Administrator Guide* (Guida dell'amministratore).

Personalizzazione dei rapporti Gestione

DRA consente di ottenere oltre 60 rapporti Gestione. Reporting Center offre la flessibilità necessaria a personalizzare e distribuire tali rapporti in molti modi. Per ulteriori informazioni sulla personalizzazione e la distribuzione di rapporti in Reporting Center, vedere la *Administrator Guide* (Guida dell'amministratore).

Per personalizzare un rapporto Gestione:

1. Visualizzare un rapporto simile a un rapporto che si desidera creare. Per ulteriori informazioni, vedere la sezione Visualizzazione dei rapporti Gestione.
2. Personalizzare il rapporto modificando le proprietà e le impostazioni del contesto per visualizzare le informazioni desiderate.
3. Fare clic su **Execute Report** (Esegui rapporto).
4. Nel menu Report (Rapporto) fare clic su **Save Report As** (Salva rapporto con nome), quindi specificare il titolo del rapporto e l'ubicazione in cui si desidera salvare il rapporto.
5. Fare clic su **Salva**.

Per ulteriori informazioni sull'utilizzo dei rapporti Gestione in Reporting Center, vedere la *Administrator Guide* (Guida dell'amministratore).

3 Ricerca degli oggetti

In questo capitolo vengono fornite informazioni concettuali e procedurali sulle funzionalità di Ricerca e Ricerca LDAP.

Ricerca

DRA consente di cercare gli oggetti in domini Active Directory locali, Microsoft Exchange e tenant di Azure. È possibile cercare utenti, gruppi e contatti nei tenant di Azure, oggetti quali utenti, gruppi, contatti, computer, stampanti, unità organizzative e account gMSA (group Managed Service Account, Account del servizio gestito del gruppo) nei domini Active Directory, nonché oggetti, ad esempio caselle postali di sale, di attrezzature, condivise e gruppi di distribuzione dinamici in Exchange. È possibile utilizzare i filtri di ricerca per eseguire ricerche più efficienti ed efficaci. DRA tronca automaticamente gli spazi iniziali o finali dell'input di ricerca e restituisce i risultati della ricerca.

Per accedere alla funzione di ricerca nella console Web, passare a **Gestione** > **Ricerca**. Per eseguire una ricerca, selezionare uno o più filtri, selezionare un'opzione Ricerca per, immettere un termine di ricerca e fare clic su **Ricerca**.

Ad esempio, la ricerca eseguita di seguito ha restituito tutti gli utenti presenti nel dominio o nel container che avevano come cognome "Beck" o un cognome che terminava con queste quattro lettere.

Ricerca per	Termine di ricerca immesso	Filtro selezionato
• Nome • termina con	beck	Utente

Nota: Per ottenere risultati precisi degli oggetti cercati quando si usano i filtri, è necessario apportare eventuali modifiche alla paginazione prima di applicare i filtri ed eseguire la ricerca. La modifica dell'impostazione **elementi per pagina** nella parte inferiore della console Web non è supportata se sono applicati filtri per tipo di oggetto.

Per accedere alla funzione di ricerca nella Console di delega e configurazione, accedere a Account and Resource Management (Gestione account e risorse) e fare clic su **Accounts and Resources** (Account e risorse) nel riquadro di visualizzazione.

Utilizzo di caratteri jolly

DRA supporta i caratteri jolly, ad esempio il punto interrogativo (?), l'asterisco (*) o il simbolo del cancelletto (#) per massimizzare i risultati della ricerca. La corrispondenza dei caratteri jolly è senza distinzione maiuscole/minuscole.

Nella tabella seguente sono forniti alcuni esempi di specifiche di caratteri jolly, gli elementi a cui corrispondono e gli elementi a cui non corrispondono

Carattere	Elemento corrispondente
Punto interrogativo ?	Un carattere qualsiasi o una cifra
Simbolo di cancelletto #	Una qualsiasi cifra
Asterisco *	Qualsiasi numero di caratteri o cifre

Ricerca di più campi

L'opzione Corrispondenza di più campi consente di ricercare le corrispondenze a più attributi con una singola ricerca. Quando si esegue una ricerca utilizzando Corrispondenza di più campi, la stringa di ricerca viene confrontata con più attributi quali il nome, il nome visualizzato, il nome e il cognome; se la stringa di ricerca corrisponde ad almeno uno di questi attributi, l'oggetto viene restituito nei risultati della ricerca.

L'opzione Corrispondenza di più campi supporta solo il criterio di ricerca **"inizia con"**.

Ad esempio, se sono presenti due utenti, uno con *nome visualizzato* "`Martin Smith`" e l'altro con nome principale utente `martha.jones@acme.com`, una ricerca con la stringa "`Mart`" restituirebbe entrambi gli utenti.

Nella seguente tabella vengono elencati gli attributi ricercati per ciascun tipo di oggetto:

Tipo di oggetto	Attributi ricercati
Contatto Azure	displayName, givenName, mail, mailNickname, surname
Gruppo Azure	displayName, mail
Utente Azure	displayName, employeeId, givenName, mail, surname, userPrincipalName
Computer	displayName, name, sAMAccountName
Contatto	displayName, employeeId, givenName, mail, mailNickname, name, surname
Gruppo di distribuzione dinamico	displayName, mail, mailNickname, name
Gruppo	displayName, mail, mailNickname, name, sAMAccountName
Account del servizio gestito del gruppo	displayName, name, sAMAccountName
Unità organizzativa	name

Tipo di oggetto	Attributi ricercati
Cestino	name, sAMAccountName
Utente	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

Nota: La funzione di corrispondenza multipla non è supportata nelle ricerche Selettore oggetti della Console di delega e configurazione quando si aggiungono deleghe o autorizzazioni per gli oggetti Exchange elencati di seguito:

- cassetta postale utente
- utente abilitato alla posta
- gruppo abilitato alla posta
- contatto abilitato alla posta
- gruppo di distribuzione dinamico
- cassetta postale condivisa
- cassetta postale delle risorse

Aggiunta e ordinamento delle colonne

È possibile ordinare gli oggetti dei risultati di ricerca in base a uno dei seguenti attributi, facendo clic sull'intestazione di colonna dell'attributo:

- Alias
- Nome visualizzato
- E-mail
- ID dipendente
- Name (Nome)
- Last Name (Cognome)
- Ubicazione
- Nome
- Nome precedente a Windows 2000
- Nome principale utente

Per aggiungere o rimuovere le colonne di attributi, fare clic sull'icona della colonna.

Esportazione dei risultati di ricerca

DRA consente agli amministratori aggiunti di esportare i risultati della **Ricerca** nella console Web in un file CSV. Per esportare i risultati della **Ricerca** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic sull'icona **Download**.

Nota: Vengono esportate solo le colonne selezionate. Se si desidera includere dati aggiuntivi che non sono visualizzati, aggiungere prima tali colonne, quindi esportare i risultati della **Ricerca**.

Ricerca avanzata

DRA consente di eseguire query LDAP e di attributi virtuali nei domini Active Directory locali dalla pagina Ricerca avanzata. È possibile eseguire la ricerca utilizzando o modificando una query esistente, creando una nuova query e salvando le query nuove e modificate per l'uso futuro come query pubbliche o private. È possibile utilizzare i filtri di ricerca per eseguire ricerche più efficienti ed efficaci.

Per accedere alle query di Ricerca avanzata nella console Web, passare a **Gestione** > **Ricerca avanzata**.

Per accedere alle query di Ricerca avanzata nella Console di delega e configurazione, selezionare il dominio, il tenant di Azure o il nodo secondario in Account and Resource Management (Gestione account e risorse), quindi fare clic su **Ricerca avanzata** sulla barra degli strumenti.

Query di ricerca avanzate

DRA supporta sia le query di attributo virtuale che LDAP per cercare gli oggetti DRA e Active Directory. Gli attributi virtuali possono essere associati a tipi di oggetto Active Directory quali utenti, gruppi, gruppi di distribuzione dinamici, contatti, computer e unità organizzative. Con una query di attributo virtuale è possibile filtrare i risultati restituiti dalla query LDAP per restituire solo i risultati che corrispondono alla query di attributo virtuale. È necessario che le stringhe della query di attributo virtuale comincino con `(objectCategory=<tipo di oggetto>)`. Per eseguire una query di attributo virtuale, è necessario specificare le stringhe sia per le query LDAP che per le query di attributo virtuale.

Esempi di query LDAP:

- Per ricercare "tutti gli oggetti computer" in DRA:

  Query LDAP: `(objectCategory=computer)`
- Per ricercare gli oggetti utente con la descrizione "East\West Sales" in DRA:

  Query LDAP: `(&(objectCategory=user)(description=East\5CWest Sales))`
- Per ricercare "tutti gli oggetti computer" in DRA:

  Query LDAP: `(objectCategory=computer)`

  Importante: nei filtri LDAP, per la barra rovesciata è necessario utilizzare il carattere di escape. Sostituire \5C.
- Per "elencare tutti gli oggetti utente disabilitati" in DRA:

Query LDAP:

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840
.113556.1.4.803:=2))
```

La stringa `1.2.840.113556.1.4.803`specifica `LDAP_MATCHING_RULE_BIT_AND`. In questo modo viene specificato un AND bit per bit di un attributo flag (numero intero), ad esempio userAccountControl, groupType o systemFlags, e una maschera di bit (ad esempio 2, 32 o 65536). La clausola è True se l'AND bit per bit del valore dell'attributo e la maschera di bit sono diversi da zero, a indicare che il bit è impostato.

Esempi di query di attributo virtuale:

- Per trovare tutti gli utenti il cui nome dell'azienda è ABC:

  Query: `(&(objectCategory=User)(CompanyName=ABC))`

  L'oggetto DRA è "User" e l'attributo virtuale è "CompanyName" (associato a User).

- Per trovare tutti gli utenti con il nome dell'azienda ABC nel dominio Storage:

  Query: `(&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))`

  L'oggetto DRA è "User" e gli attributi virtuali sono "CompanyName" e "Domain" (associati a User).

- Per trovare tutti i gruppi con il nome del prodotto DRA o tutti gli utenti con il nome dell'azienda ABC:

  Query:

  ```
  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=Use
  r)(CompanyName=ABC)))
  ```

  Gli oggetti DRA sono "Group" e "User" e gli attributi virtuali sono CompanyName (associato a User), ProductGroupName (associato a Group).

- Per trovare tutti i gruppi il cui nome del prodotto è DRA o tutti gli utenti con il nome dell'azienda ABC nel dominio Storage:

  Query:

  ```
  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=Use
  r)(CompanyName=ABC)(Domain=Storage)))
  ```

  Gli oggetti DRA sono "Group" e "User" e gli attributi virtuali sono CompanyName (associato a User), ProductGroupName (associato a Group), Domain (associato a User).

Gestione delle query avanzate

Per supportare la funzione di query Ricerca avanzata, DRA utilizza LDAP. Utilizzando le query avanzate è possibile cercare utenti, contatti, gruppi, computer, unità organizzative e qualsiasi altro oggetto supportato da DRA. Se si dispone dei diritti per eseguire query avanzate salvate, è possibile eseguire le query avanzate disponibili negli elenchi **Le mie ricerche** e **Ricerche pubbliche** per qualsiasi container.

Oltre a eseguire una ricerca con una query avanzata salvata e a visualizzarne i dettagli, con le autorizzazioni pertinenti è possibile effettuare le seguenti query avanzate della pagina Ricerca avanzata:

Creazione di una nuova query

Creare una query avanzata sul server di amministrazione primario o sul server di amministrazione secondario specificando la stringa della query (LDAP e, se applicabile, attributo virtuale) per la nuova query avanzata. Una volta eseguita la ricerca, espandere il menu a discesa **Ricerca** per salvare la query nell'elenco Le mie ricerche o nell'elenco Ricerche pubbliche.

Modifica di una query

Selezionare una query avanzata esistente in Le mie ricerche o Ricerche pubbliche e utilizzare l'opzione **Modifica** per modificare i criteri di ricerca. Una volta eseguita la ricerca con i criteri di ricerca aggiornati, è possibile espandere il menu a discesa **Ricerca** e selezionare **Salva** per salvare le modifiche apportate alla query.

Copia di una query

Selezionare una query avanzata esistente in Le mie ricerche o Ricerche pubbliche ed eseguire la ricerca. Una volta eseguita la ricerca, è possibile espandere il menu a discesa **Ricerca** e selezionare **Sal. con nome** per salvare la query con un nome diverso.

Personalizzazione dei risultati della query

DRA fornisce un gruppo di default di colonne nell'elenco dei risultati della ricerca. Per personalizzare i risultati della ricerca tramite una query salvata o non salvata, fare clic sull'icona di **Aggiungi/Rimuovi colonne** sul lato destro della pagina per modificare la modalità di visualizzazione dei risultati della ricerca.

Cancellazione di una query

È possibile cancellare qualsiasi query avanzata presente nell'elenco **Le mie ricerche**. Con le autorizzazioni pertinenti, è inoltre possibile cancellare le query avanzate nell'elenco **Ricerche pubbliche**. Per eliminare una query avanzata salvata, selezionarla nell'elenco pertinente, quindi fare clic su **Cancella** nel menu a discesa Ricerca.

Eliminazione di una query

La console Web consente di eliminare i campi del modulo di una query salvata o non salvata per apportare modifiche da un modulo pulito. Per azzerare i campi di una query, selezionare **Elimina** dal menu a discesa Ricerca.

Esportazione dei risultati di una ricerca avanzata

DRA consente agli amministratori aggiunti di esportare i risultati della **Ricerca avanzata** nella console Web in un file CSV. Per esportare i risultati della **Ricerca avanzata** dalla console Web, accedere a **Gestione** > **Ricerca avanzata** e fare clic sull'icona **Download**.

Nota: Vengono esportate solo le colonne selezionate. Se si desidera includere dati aggiuntivi che non sono visualizzati, aggiungere prima tali colonne, quindi esportare i risultati della **Ricerca avanzata**.

---

4 Gestione di oggetti Active Directory

In questo capitolo vengono fornite informazioni sui concetti e sulle procedure per la gestione di account utente, gruppi, gruppi dinamici, gruppi di distribuzione dinamici e contatti sia nel nodo Account and Resource Management (Gestione account e risorse) della Console di delega e configurazione sia nella console Web. Le informazioni sugli account utente sono più complete per fornire un esempio su come è possibile gestire gli oggetti in generale in entrambe le applicazioni client.

Gestione degli account utente

Microsoft Windows si basa sul tipo di account utente per determinare le autorizzazioni di accesso per l'account utente associato. Un account utente può essere globale o locale. DRA supporta anche gli oggetti InetOrgPerson, tuttavia riconosce tali oggetti come normali utenti.

Account utente globale

Un account utente che può essere utilizzato in qualsiasi dominio che considera attendibile il dominio in cui l'account utente è stato creato. È possibile concedere autorizzazioni specifiche a un account utente. Infine è possibile rendere un account utente un membro di un gruppo, quindi assegnare autorizzazioni a tale gruppo. L'inserimento degli account utente nei gruppi consente di semplificare il processo di gestione delle autorizzazioni di rete nel caso di un numero di account utente elevato.

Account utente locale

Un account utente locale è identico a qualsiasi account utilizzato per eseguire il login al sistema operativo Windows e consente di accedere alle risorse del sistema nel proprio spazio utente.

Per ulteriori informazioni sulla gestione degli account utente, vedere i seguenti argomenti:

Account utente in domini attendibili

Microsoft Windows memorizza le definizioni degli account utente e dei gruppi nella directory del dominio gestito. Pertanto, un server di amministrazione non può modificare le informazioni sulla directory di un dominio attendibile a meno che tale dominio non sia gestito anche da DRA.

Ad esempio, in Account and Resource Management (Gestione account e risorse) è possibile vedere gli account utente e i gruppi che non è possibile modificare. Questi account utente e gruppi sono definiti nei domini attendibili da uno dei domini gestiti. Tuttavia, è possibile aggiungere account e gruppi da un dominio attendibile in altri gruppi del dominio gestito.

Task di gestione degli account utente

In questa sezione vengono fornite informazioni sull'amministrazione degli account utente nel nodo Account and Resource Management (Gestione account e risorse) della Console di delega e configurazione e nella console Web. Con i poteri appropriati è possibile eseguire diversi task di gestione degli account utente come, ad esempio la creazione e la cancellazione di account. Se si selezionano più account utente, è possibile eseguire i task selezionati in un'unica operazione, ad esempio la cancellazione, lo spostamento o l'aggiunta di utenti a un gruppo. Per ulteriori informazioni sui poteri assegnati, vedere la sezione Visualizzazione dei poteri e dei ruoli assegnati.

Task degli account utente in Account and Resource Management (Gestione account e risorse)

È possibile eseguire tutti i task applicabili riportati di seguito dal menu **Task** o dal menu di scelta rapida. In genere, si seleziona il nodo **Tutti i miei oggetti gestiti** e si esegue il comando **Find Now** (Trova ora) per individuare e selezionare l'oggetto utente desiderato. Il menu Task indica quali task è possibile eseguire quando si seleziona un account utente singolo o più account utente. Per un utente singolo saranno disponibili più opzioni.

Nel caso della creazione di un nuovo utente, è necessario selezionare il dominio o l'unità organizzativa in cui si desidera creare l'utente. Ad esempio:

1. Selezionare il container **Utenti** in un dominio in Tutti i miei oggetti gestiti.
2. Selezionare **Nuovo** > **Utente** dal menu Task.
3. Completare i passaggi della creazione guidata dell'utente.

Gestione dell'account personale

È possibile gestire il proprio account personale modificandone le proprietà generali, ad esempio il numero di telefono. Prima di iniziare a gestire l'account, assicurarsi di disporre del potere appropriato.

Copia di un account utente in un'altra vista attiva

È possibile copiare un account utente in un'altra vista attiva. Questa azione viene chiamata trasferimento di un account utente. Per copiare un account utente in un'altra vista attiva, è necessario disporre del diritto Copy User to Another ActiveView (Copia utente in un'altra vista attiva) sia nella vista attiva di origine che nella vista attiva di destinazione. Il trasferimento di un account utente in un'altra vista attiva non determina la rimozione dell'account dalla vista attiva di origine.

Nota: La copia di un account utente in un'altra vista ActiveView può essere eseguita solo dalla Console di delega e configurazione tramite il nodo Account and Resource Management (Gestione account e risorse).

Ridenominazione di un account utente

È possibile rinominare gli account utente nel dominio o nel sottoalbero gestito. La modifica del nome di login dell'utente modifica anche il nome della casella postale associata all' account utente.

Task degli account utente nella console Web

È possibile eseguire la maggior parte dei task dalla scheda **Gestione** > **Ricerca** della console Web. Per individuare e selezionare l'oggetto utente desiderato, eseguire un'operazione di ricerca. Dopo la selezione di uno o più oggetti nell'elenco, la barra dei task si attiva con opzioni della barra degli strumenti e di menu a discesa per **Account** ed **Exchange**. Posizionare il puntatore del mouse su un'icona della barra degli strumenti o fare clic su un menu a discesa per visualizzarne le funzioni o le opzioni.

Creazione di un account utente

È possibile creare account utente nel dominio o nel sottoalbero gestito. È inoltre possibile modificare le proprietà, creare una casella postale, abilitare l'e-mail e specificare appartenenze ai gruppi per il nuovo account.

Nota

- L'azienda può avere una convenzione di denominazione applicata mediante una policy che determina il nome che è possibile assegnare al nuovo account utente.
- Di default, DRA inserisce il nuovo account utente nell'unità organizzativa degli utenti del dominio gestito.
- In DRA non è possibile creare oggetti InetOrgPerson.

Clonazione di un account utente

Quando si clona un account utente, eventuali gruppi di cui l'utente è membro vengono aggiunti automaticamente al nuovo account utente durante la configurazione. È possibile aggiungere o rimuovere gruppi dal nuovo account, abilitare l'e-mail ed eseguire eventuali altre configurazioni delle proprietà come si farebbe con qualsiasi altro nuovo account.

Nota: Quando si clona un oggetto InetOrgPerson, si crea un account utente.

Modifica delle proprietà degli account utente

È possibile gestire le proprietà degli account utente nel dominio o nel sottoalbero gestito. I poteri di cui si dispone determinano le proprietà di un account utente che è possibile modificare. Se si è installato Exchange e si è abilitato il supporto di Microsoft Exchange, è possibile modificare le proprietà delle caselle postali associate mentre si gestiscono gli account utente.

Nota: Se le policy della home directory sono abilitate, DRA modifica automaticamente la home directory di un account utente quando viene gestito. Ad esempio, se si modifica l'ubicazione della home directory, DRA tenta di creare la home directory specificata e sposta il contenuto della home directory precedente nella nuova ubicazione. DRA applica inoltre gli ACL (elenchi di controllo di accesso) assegnati dalla directory precedente alla nuova directory.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Abilitazione di un account utente

È possibile abilitare un account utente nel dominio o nel sottoalbero gestito. Se si sta gestendo un account Microsoft Windows, è possibile specificare il controller del dominio in cui DRA applicherà questa modifica.

Quando si applica questa modifica a un controller del dominio specifico, DRA la applica anche al controller del dominio di default per il dominio gestito. Per verificare quale controller del dominio di default DRA sta utilizzando, visualizzare le proprietà del dominio.

Disabilitazione di un account utente

È possibile disabilitare un account utente nel dominio gestito. Se si sta gestendo un account Microsoft Windows, è possibile specificare il controller del dominio in cui DRA applica la modifica.

Quando si applica questa modifica a un controller del dominio specifico, DRA la applica anche al controller del dominio di default per il dominio gestito. Per verificare quale controller del dominio di default DRA sta utilizzando, visualizzare le proprietà del dominio.

Sblocco di un account utente

È possibile sbloccare un account utente nel dominio o nel sottoalbero gestito.

Poiché DRA recupera lo stato dell'account utente dalla cache degli account, l'interfaccia utente può indicare che l'account selezionato è sbloccato quando in realtà è bloccato. DRA consente di sbloccare un account utente, anche se lo stato dell'account indica che non è attualmente bloccato. Quando si sblocca un account utente tramite la console DRA è anche possibile specificare un controller del dominio senza la necessità di reimpostare la password dell'account.

Reimpostazione della password di un account utente

È possibile reimpostare la password per un account che si trova nel dominio o nel sottoalbero gestito. I poteri di cui si dispone determinano i campi di tale account utente che è possibile modificare.

Quando si reimposta la password per un account utente, DRA sblocca automaticamente l'account. È possibile specificare se DRA deve generare una nuova password per l'account utente. È anche possibile modificare varie opzioni relative alle password per l'account. Se si sta gestendo un account Microsoft Windows, è possibile specificare il controller del dominio in cui DRA applicherà queste modifiche

Nota: Quando si applica questa modifica a un controller del dominio specifico, DRA la applica anche al controller del dominio di default per il dominio gestito. Per verificare quale controller del dominio di default DRA sta utilizzando, visualizzare le proprietà del dominio.

Spostamento di un account utente in un altro container

È possibile spostare un account utente in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Cancellazione di un account utente

È possibile cancellare un account utente dal dominio o dal sottoalbero gestito. Se il Cestino è disabilitato per il dominio, l'eliminazione di un account utente ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, la cancellazione di un account utente ne determina lo spostamento nel Cestino.

Avviso: Quando si crea un account utente, Microsoft Windows assegna all'account un identificatore di sicurezza (SID). Il SID non viene generato dal nome dell'account. Microsoft Windows utilizza i SID per registrare i privilegi negli ACL (elenchi di controllo di accesso) per ciascuna risorsa. Se si cancella un account utente, non è possibile restituire le funzionalità di accesso per l'account mediante la creazione di un nuovo account utente con lo stesso nome.

Specifica dell'appartenenza ai gruppi per gli account utente

È possibile aggiungere o rimuovere gli account utente da un gruppo specifico nel dominio o nel sottoalbero gestito. È inoltre possibile visualizzare o modificare le proprietà di gruppi esistenti a cui l'account appartiene.

Trasformazione degli account utente

DRA offre la possibilità di trasformare gli account utente in modo rapido ed efficiente. Quando l'utente associato all'account utente passa a nuove mansioni lavorative, è possibile utilizzare le funzionalità di gestione delle trasformazioni di DRA. Usufruendo del vantaggio offerto dai modelli del ruolo di lavoro, è possibile aggiungere, rimuovere o aggiornare rapidamente le appartenenze ai gruppi associate a un account. Se un dipendente viene promosso, cambia reparto o lascia l'azienda, la possibilità di trasformare un account utente consentirà di risparmiare tempo, denaro e congetture.

Informazioni sul processo di trasformazione

È possibile utilizzare le funzionalità di trasformazione degli account utente per soddisfare le seguenti esigenze:

- Rimuovere l'appartenenza a un gruppo da un account utente
- Aggiungere l'appartenenza a un gruppo a un account utente
- Modificare le proprietà dell'utente
- Rimuovere le appartenenze a un gruppo specifico mentre si aggiungono altre appartenenze a un account utente

Prima di provare a trasformare un account utente, esaminare il seguente processo:

1. Stabilire se si desidera aggiungere o rimuovere le appartenenze ai gruppi o entrambe le cose.
2. Esaminare gli attuali modelli sottrattivi e additivi per assicurarsi di disporre di account utente con i modelli necessari.
3. Se necessario, creare eventuali modelli obbligatori.
4. Completare la procedura guidata Transform User (Trasforma utente).

Man mano che DRA trasforma un utente, le appartenenze ai gruppi designate dal modello sottrattivo vengono rimosse dall'account utente, mentre le appartenenze designate dal modello additivo vengono assegnate all'account. DRA lascia inalterate le appartenenze al di fuori dei modelli sottrattivi o additivi. Ad esempio, un dipendente del reparto vendite esterno viene trasferito dal reparto vendite degli Stati Uniti a quello dell'Europa. L'organizzazione dispone sia di gruppi di distribuzione che di gruppi sicurezza univoci per tali team di vendita sia di un certo numero di gruppi che è stato condiviso tra tutti i team di vendita. Il team di vendita degli Stati Uniti ha i gruppi di distribuzione Elenco di distribuzione hotspot USA ed Elenco di distribuzione Gestione vendite USA, mentre il team di vendita europeo ha i gruppi di distribuzione Hotspot Europa e Gestione vendite Europa. Entrambi i team sono membri del gruppo di sicurezza Sicurezza vendite globali, ma possiedono anche gruppi di sicurezza specifici delle singole sedi.

Il modello sottrattivo, denominato Modello vendite USA, verrà assegnato alle seguenti appartenenze ai gruppi:

- Elenco di distribuzione hotspot USA
- Elenco di distribuzione Gestione vendite USA
- Sicurezza vendite globali
- Sicurezza USA

Il modello additivo, denominato Modello vendite Europa, verrà assegnato alle seguenti appartenenze ai gruppi:

- Elenco di distribuzione hotspot Europa
- Elenco di distribuzione Gestione vendite Europa
- Sicurezza vendite globali
- Sicurezza Europa

Durante il processo di trasformazione, l'account utente dell'addetto alle vendite trasferito viene prima rimosso da tutte le appartenenze ai gruppi designate da Modello vendite USA, quindi viene aggiunto a tutte le appartenenze ai gruppi designate da Modello vendite Europa. Se questa persona fosse stata anche membro del gruppo di distribuzione Giocatori di Poker, l'appartenenza a questo gruppo sarebbe rimasta inalterata.

I poteri indicati di seguito consentono all'amministratore aggiunto di modificare ulteriormente un account utente durante il processo di trasformazione:

- Modify Address Properties while Transforming a User Account (Modifica delle proprietà dell'indirizzo durante la trasformazione di un account utente)
- Modify Description while Transforming a User Account (Modifica descrizione durante la trasformazione di un account utente)

- Modify Office while Transforming a User Account (Modifica sede durante la trasformazione di un account utente)
- Modify Telephone Properties while Transforming a User Account (Modifica proprietà del numero di telefono durante la trasformazione di un account utente)

È inoltre possibile limitare la possibilità di aggiungere o rimuovere appartenenze ai gruppi assegnando a un amministratore aggiunto uno solo dei poteri seguenti:

- Add a user to groups found in a template (Aggiungi un utente ai gruppi disponibili in un modello)
- Add a user to groups found in a template (Rimuovi un utente da gruppi disponibili in un modello)

È possibile utilizzare una di queste opzioni di limitazione basate sui poteri per creare un livello di sicurezza all'interno della propria organizzazione. Concedendo ad alcune persone il potere di rimuovere solo i gruppi disponibili in un modello, è possibile creare account utente provvisori. Questi account provvisori possono poi essere modificati prima che un altro amministratore aggiunto utilizzi un account modello aggiuntivo per concedere le nuove appartenenze ai gruppi.

Creazione di modelli per la trasformazione dell'utente

La trasformazione degli account utente è direttamente associata ai ruoli e alla gerarchia delle mansioni della propria organizzazione. Si consiglia di creare un modello per ciascun ruolo o mansione all'interno dell'azienda. DRA non distingue tra un modello di account utente utilizzato come sottrattivo rispetto a un modello utilizzato come additivo. Creare un singolo account utente modello per ciascun ruolo all'interno dell'organizzazione. Durante la trasformazione, sarà possibile selezionare il modello come sottrattivo o additivo. Se si seleziona un modello come sottrattivo, questo non impedisce allo stesso modello di essere utilizzato come additivo in una trasformazione futura.

Per creare un modello di trasformazione dell'utente, è necessario disporre di poteri per creare un account utente e assegnarlo ai gruppi appropriati. Questi poteri possono essere ottenuti mediante l'associazione del proprio account con i ruoli Create and Delete User Accounts (Crea e cancella account utente) e Group Administration (Amministrazione gruppi) nelle viste attive appropriate o mediante l'assegnazione di poteri individuali.

Trasformazione degli account utente

La trasformazione di un account utente consente di aggiungere o rimuovere le appartenenze ai gruppi di account utente o di eseguire entrambe le cose. Utilizzare il seguente workflow come supporto per la transizione dei dipendenti da un ruolo professionale a un altro all'interno dell'organizzazione. È necessario disporre del ruolo Transform a User (Trasforma un utente) o di un ruolo che contiene i poteri appropriati per trasformare gli account utente. Questa funzione può essere eseguita solo dalla Console di delega e configurazione tramite il nodo Account and Resource Management (Gestione account e risorse).

Per trasformare un account utente:

1. Nel riquadro sinistro espandere **Tutti i miei oggetti gestiti**.
2. Per specificare l'account utente che si desidera gestire, eseguire il comando **Find Now** (Trova ora)per individuare e selezionare l'oggetto utente.

3. Fare clic su **Task** > **Transform** (Trasforma).
4. Controllare la finestra di benvenuto, quindi fare clic su **Next** (Avanti).
5. Nella finestra Select User Template (Seleziona modello utente), utilizzare **Sfoglia** per selezionare l'utente con il modello sottrattivo appropriato.
6. Se si desidera esaminare le proprietà dell'account utente con il modello sottrattivo, fare clic su **Visualizza**.
7. Utilizzare **Sfoglia** per selezionare l'utente con modello additivo appropriato.
8. Se si desidera esaminare le proprietà dell'account utente con modello additivo, fare clic su **Visualizza**.
9. Se si dispone dei poteri appropriati, è possibile selezionare **Change other properties of the user** (Modifica altre proprietà dell'utente) e selezionare le proprietà da modificare. Fare clic su **Next** (Avanti) per scorrere le proprietà disponibili.
10. Fare clic su **Next** (Avanti).
11. Controllare la finestra di riepilogo, quindi fare clic su**Finish** (Fine).

Gestione dei gruppi

In qualità di amministratore aggiunto, è possibile utilizzare DRA per gestire i gruppi e modificarne le proprietà. I gruppi consentono di assegnare autorizzazioni specifiche a un gruppo di account utente definito. Consentono inoltre di controllare a quali dati e risorse un account utente può accedere in qualsiasi dominio.

È possibile gestire gruppi di qualsiasi tipo e ambito. Ad esempio, è possibile nidificare i gruppi, consentendo a un gruppo di ereditare le autorizzazioni da un altro gruppo. È anche possibile controllare in modo efficace le appartenenze ai gruppi nei domini aggiungendo gruppi da domini attendibili ad altri gruppi che si trovano nel dominio gestito, quindi gestendo le assegnazioni temporanee ai gruppi.

Per ulteriori informazioni sulla gestione dei gruppi, vedere i seguenti argomenti:

- “Task di gestione dei gruppi” a pagina 54
- “Gestione delle assegnazioni temporanee ai gruppi nella Console di delega e configurazione” a pagina 57
- “Gestione delle assegnazioni temporanee ai gruppi nella console Web” a pagina 58

Task di gestione dei gruppi

In questa sezione viene illustrato come amministrare i gruppi nella Console di delega e configurazione tramite il nodo Account and Resource Management (Gestione account e risorse). Con i poteri appropriati è possibile eseguire diversi task di gestione dei gruppi, ad esempio la modifica delle appartenenze ai gruppi. Se si selezionano più gruppi, è possibile eseguire i task selezionati in un'unica operazione, ad esempio la cancellazione, lo spostamento o l'aggiunta di membri a un gruppo. Il menu Task indica quali task è possibile eseguire quando si selezionano uno o più gruppi.

Aggiunta di account ai gruppi

È possibile aggiungere account utente, contatti e computer a un gruppo gestito.

Nota: Questo task consente di aggiungere più account a un gruppo selezionato. È possibile aggiungere un singolo account a un gruppo selezionando l'account desiderato, quindi facendo clic su Aggiungi ai gruppi nel menu Task.

Se l'aggiunta di un account a un altro gruppo, aumenta i poteri assegnati a quell'account, DRA non consentirà di eseguire l'operazione.

Aggiunta di gruppi ad altri gruppi

È possibile nidificare i gruppi mediante l'aggiunta di un gruppo a un altro gruppo gestito. Quando un gruppo viene nidificato in un altro gruppo, il gruppo secondario può ereditare le autorizzazioni del gruppo principale.

Nota: Se l'aggiunta di un gruppo a un altro gruppo, aumenta i poteri assegnati a quel gruppo, DRA non consentirà di eseguire l'operazione.

Modifica delle proprietà dei gruppi

È possibile modificare le proprietà dei gruppi locali e globali. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un gruppo nel dominio o nel sottoalbero gestito. Se si è installato Exchange e si è abilitato il supporto di Microsoft Exchange, è possibile modificare le proprietà dell'elenco di distribuzione mentre si gestiscono i gruppi.

Creazione di un gruppo

È possibile creare un gruppo nel dominio o nel sottoalbero gestito. È anche possibile modificare le proprietà, ad esempio i membri dei gruppi per il nuovo gruppo.

Nota

- Nell'azienda potrebbe essere applicata una convenzione di denominazione mediante una policy che determina il nome che è possibile assegnare al nuovo gruppo.
- Di default, in DRA il nuovo gruppo verrà inserito nell'unità organizzativa degli utenti del dominio gestito.

Specifica dei membri del gruppo

È possibile aggiungere o rimuovere account utente, contatti, computer o altri gruppi da un gruppo gestito. DRA consente di rimuovere solo le entità principal di sicurezza esterne. È inoltre possibile visualizzare o modificare le proprietà dei membri dei gruppi esistenti, ad eccezione delle entità principal di sicurezza esterne.

Quando si rimuovono membri da un gruppo, DRA non cancella gli oggetti. Se si aggiungono membri a un gruppo, è necessario disporre dei poteri per modificare gli oggetti che si desidera aggiungere.

Nota

- Non è possibile aggiungere account utente o gruppi a uno qualsiasi dei gruppi speciali di Windows (amministratori, operatori di account, operatori di backup o del server) a meno che non si ricopra il ruolo di amministratore di Windows o di membro di tale gruppo speciale specifico.
- DRA consente di esportare i risultati di **Membri** come file CSV. Per esportare i risultati di **Membri** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membri** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Specifica dell'appartenenza ai gruppi per i gruppi

È possibile aggiungere o rimuovere un gruppo da altri gruppi nel dominio o nel sottoalbero gestito. È inoltre possibile visualizzare o modificare le proprietà dei gruppi esistenti a cui appartiene il gruppo.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Configurazione delle autorizzazioni di sicurezza delle appartenenze ai gruppi

È possibile impostare le autorizzazioni di sicurezza di Active Directory per le appartenenze ai gruppi. Queste autorizzazioni consentono di specificare chi può visualizzare (lettura) e modificare (scrittura) le appartenenze ai gruppi utilizzando Microsoft Outlook. Consentono inoltre di proteggere con maggiore efficacia gli elenchi di distribuzione e i gruppi di sicurezza del proprio ambiente. Non è possibile modificare le autorizzazioni di sicurezza ereditate.

Nota: Quando si gestisce la sicurezza delle appartenenze ai gruppi, le autorizzazioni disabilitate possono indicare le autorizzazioni ereditate.

Configurazione della proprietà di un gruppo

È possibile impostare la proprietà di qualsiasi gruppo di distribuzione o di sicurezza di Microsoft Windows. È possibile concedere l'autorizzazione di proprietà del gruppo a un account utente, a un gruppo o a un contatto. La concessione della proprietà di un gruppo consente all'account utente, al gruppo o al contatto specificato di modificare l'appartenenza del gruppo.

Nota: DRA disabilita la casella di controllo **Manager can update membership list** (Il manager può aggiornare l'elenco delle appartenenze) quando l'appartenenza al gruppo non è visibile al server Microsoft Exchange. Per attivare questa casella di controllo, fare clic su **Expose Group Membership** (Esponi appartenenza al gruppo) nella scheda Exchange della finestra Group Properties (Proprietà gruppo).

Clonazione di un gruppo

È possibile clonare i gruppi locali e i gruppi globali nei domini gestiti. La clonazione dei gruppi consente di creare nuovi gruppi dello stesso tipo e con attributi uguali a quelli del gruppo originale. DRA tenta inoltre di aggiungere tutti i membri del gruppo originale al nuovo gruppo.

Clonando un gruppo, è possibile creare rapidamente gruppi basati su altri gruppi con proprietà simili. Quando si clona un gruppo, DRA popola i campi della procedura guidata Clone Group (Clona gruppo) con i valori del gruppo selezionato. È anche possibile modificare le proprietà del nuovo gruppo.

Nota

- Nell'azienda potrebbe essere applicata una convenzione di denominazione mediante una policy che determina il nome che è possibile assegnare al nuovo gruppo.
- Di default, in DRA il nuovo gruppo verrà inserito nell'unità organizzativa degli utenti del dominio gestito.

Cancellazione di un gruppo

È possibile cancellare i gruppi locali e globali nel dominio o nel sottoalbero gestito. Se il Cestino è disabilitato per tale dominio, l'eliminazione di un gruppo ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, la cancellazione di un gruppo ne determina lo spostamento nel Cestino disabilitandone le proprietà.

Per ulteriori informazioni sul Cestino, vedere la sezione Gestione del Cestino.

Avviso: Quando si crea un gruppo, Microsoft Windows assegna al gruppo un identificatore di sicurezza (SID). Il SID non viene generato dal nome del gruppo. Microsoft Windows utilizza i SID per registrare i privilegi negli ACL (elenchi di controllo di accesso) per ciascuna risorsa. Se si cancella un gruppo, non è possibile restituire le funzionalità di accesso per il gruppo mediante la creazione di un nuovo gruppo con lo stesso nome.

Spostamento di un gruppo in un altro container

È possibile spostare un gruppo in un altro container, ad esempio in un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Esposizione delle appartenenze ai gruppi negli elenchi di distribuzione

È possibile esporre le appartenenze ai gruppi negli elenchi di distribuzione nel dominio o nel sottoalbero gestito.

Come nascondere le appartenenze ai gruppi dagli elenchi di distribuzione

È possibile nascondere le appartenenze ai gruppi negli elenchi di distribuzione dei gruppi nel dominio o nel sottoalbero gestito.

Gestione delle assegnazioni temporanee ai gruppi nella Console di delega e configurazione

Le assegnazioni temporanee ai gruppi consentono di gestire le appartenenze ai gruppi per gli utenti che richiedono l'appartenenza a un gruppo solo per un periodo di tempo specifico. In questa sezione viene illustrato come amministrare le assegnazioni temporanee ai gruppi nella Console di delega e

configurazione in **Account and Resource Management** (Gestione account e risorse). Con i poteri appropriati è possibile eseguire task come la creazione di assegnazioni temporanee ai gruppi oppure la rimozione di tali assegnazioni.

Gli amministratori aggiunti possono solo visualizzare le assegnazioni temporanee ai gruppi per i gruppi di cui l'amministratore aggiunto dispone dei poteri di modifica dell'appartenenza a un gruppo (aggiunta o rimozione dei membri).

Non è possibile modificare il gruppo associato o modificare l'elenco di utenti mentre l'assegnazione temporanea a un gruppo è nello stato attivo. Per modificare questi elementi è necessario annullare l'assegnazione temporanea a un gruppo.

Gestione delle proprietà di assegnazione temporanee ai gruppi

È possibile gestire le proprietà relative alle assegnazioni temporanee ai gruppi o alle assegnazioni temporanee ai gruppi scadute.

Se si desidera modificare la pianificazione dell'assegnazione temporanea a un gruppo, modificare la pianificazione nelle **Proprietà** dell'assegnazione e salvare le modifiche apportate.

Creazione di un'assegnazione temporanea a un gruppo

È possibile creare un'assegnazione temporanea a un gruppo sui server di amministrazione primari e secondari.

Per default, l'assegnazione temporanea a un gruppo viene cancellata dopo sette giorni dalla sua scadenza, a meno che non sia stata selezionata l'opzione **Mantenere questa assegnazione gruppo temporaneo per utilizzi futuri**. Per modificare il periodo di conservazione, fare clic con il pulsante destro del mouse sul nodo **Assegnazioni gruppi temporanei** in Tutti i miei oggetti gestiti, selezionare **Proprietà** e modificare il numero di giorni per cui conservare le assegnazioni temporanee ai gruppi.

Gestione degli account utente in un'assegnazione temporanea a un gruppo

È possibile aggiungere o rimuovere gli account utente dalle assegnazioni temporanee ai gruppi sui server di amministrazione primari e secondari.

Nota: È possibile gestire gli account utente solo per le assegnazioni temporanee ai gruppi che non sono ancora attive.

Cancellazione di un'assegnazione temporanea a un gruppo

È possibile cancellare qualsiasi assegnazione temporanea a un gruppo sui server di amministrazione primari e secondari.

Gestione delle assegnazioni temporanee ai gruppi nella console Web

Le assegnazioni temporanee ai gruppi consentono di gestire le appartenenze ai gruppi per gli utenti che richiedono l'appartenenza a un gruppo per un periodo di tempo specifico. Se Azure Active Directory è configurato dall'amministratore DRA, è possibile creare assegnazioni temporanee al gruppo per i gruppi Azure e aggiungere utenti Azure e utenti sincronizzati a un'appartenenza a un

gruppo Azure. La console Web consente di creare e gestire le assegnazioni da server primari e secondari DRA. Tuttavia, le azioni che è possibile eseguire sulle assegnazioni esistenti variano a seconda dello stato di assegnazione.

Gli amministratori aggiunti possono visualizzare le assegnazioni temporanee ai gruppi solo per i gruppi di cui dispongono del potere per modificare le assegnazioni ActiveView, ad esempio l'aggiunta o la rimozione di membri del gruppo.

Per gestire le assegnazioni temporanee ai gruppi nella console Web, passare a **Task** > **Assegnazioni gruppi temporanei**.

È possibile eseguire le seguenti azioni:

Creazione di un'assegnazione temporanea a un gruppo

È possibile creare assegnazioni temporanee ai gruppi utilizzando i gruppi per i quali si dispone dei poteri di modifica, nonché specificare il controller del dominio. Il gruppo di destinazione può essere un gruppo di un tenant gestito Azure o un gruppo di un dominio Active Directory. Una volta scaduta, DRA cancella automaticamente l'assegnazione temporanea dopo sette giorni, a meno che non si scelga l'opzione che consente di mantenere l'assegnazione temporanea a un gruppo per l'utilizzo futuro.

Nota: Se l'assegnazione temporanea al gruppo configurata con l'appartenenza al gruppo Azure viene modificata al di fuori di DRA, l'assegnazione temporanea al gruppo diventa non valida.

Per creare una nuova assegnazione temporanea a un gruppo:

1. Passare a **Task** > **Assegnazioni temporanee al gruppo** e fare clic su **Crea**.
2. Fare clic su **Seleziona** e individuare il gruppo eseguendo una Ricerca nel container appropriato.
3. Se è necessario aggiungere membri al gruppo, fare clic su **Aggiungi** in **Membri** nella pagina Crea assegnazione temporanea al gruppo, individuare e utilizzare l'opzione **Aggiungi** ➕ nell'elenco dei risultati per aggiungere membri al gruppo.
4. Configurare la pianificazione.
5. Assegnare un nome all'assegnazione temporanea al gruppo in Informazioni generali, quindi fare clic su **Crea**.

Ricerca di assegnazioni esistenti

Quando si esegue la ricerca di assegnazioni temporanee ai gruppi (TGA) esistenti, queste vengono elencate nei risultati in base al loro stato, tra cui:

- **In sospeso:** L'assegnazione temporanea a un gruppo è pianificata per l'avvio futuro. È possibile eseguire le operazioni di annullamento, cancellazione e modifica della pianificazione.
- **Attivo:** L'assegnazione temporanea a un gruppo è stata avviata e i membri pertinenti al gruppo sono stati aggiunti. È possibile eseguire le operazioni di annullamento e cancellazione.
- **Attivo con errore:** L'assegnazione temporanea a un gruppo è stata avviata ma non è stato possibile aggiungere tutti i membri pertinenti al gruppo. È possibile eseguire le operazioni di annullamento e cancellazione.

- **Completato:** L'assegnazione temporanea a un gruppo è scaduta e tutti i membri pertinenti sono stati rimossi dal gruppo. È possibile eseguire le operazioni di cancellazione e modifica della pianificazione.
- **Completato con errore:** L'assegnazione temporanea a un gruppo è scaduta ma non è stato possibile rimuovere tutti i membri pertinenti dal gruppo. È possibile eseguire le operazioni di cancellazione e modifica della pianificazione.
- **Annullato:** L'assegnazione temporanea a un gruppo è stata annullata da un utente e tutti i membri pertinenti sono stati rimossi dal gruppo. È possibile eseguire le operazioni di cancellazione e modifica della pianificazione.
- **Annullato con errore:** L'assegnazione temporanea a un gruppo è stata annullata da un utente ma non è stato possibile rimuovere tutti i membri pertinenti dal gruppo. È possibile eseguire le operazioni di cancellazione e modifica della pianificazione.
- **Errore:** L'assegnazione temporanea a un gruppo non è stata in grado di aggiungere o rimuovere tutti i membri. È possibile eseguire le operazioni di cancellazione e modifica della pianificazione.

È possibile filtrare i risultati in base a questi stati e a altri criteri, tra cui il nome dell'assegnazione, il gruppo di destinazione, la durata e l'amministratore che ha creato l'assegnazione.

Visualizzazione o modifica delle proprietà di assegnazione temporanea a un gruppo

È possibile visualizzare o modificare le assegnazioni temporanee ai gruppi definite al momento della creazione dell'assegnazione temporanea a un gruppo. Dopo l'esecuzione di una ricerca di assegnazioni temporanee ai gruppi, selezionare un'assegnazione per visualizzarne o modificarne le proprietà.

Se si desidera modificare la pianificazione dell'assegnazione temporanea a un gruppo, modificare la pianificazione nelle **Proprietà** dell'assegnazione e salvare le modifiche apportate. Se l'assegnazione è nello stato Attivo, è possibile modificare solo la data di fine.

Importante: Non è possibile modificare il gruppo associato o modificare l'elenco di utenti mentre l'assegnazione temporanea a un gruppo è nello stato attivo. Per modificare questi elementi, è necessario prima annullare l'assegnazione.

Annullamento di un'assegnazione temporanea a un gruppo

È possibile annullare l'assegnazione temporanea a un gruppo solo in presenza di uno dei seguenti stati:

- Attivo
- Attivo con errore
- In sospeso

Cancellazione di un'assegnazione temporanea a un gruppo

È possibile selezionare più assegnazioni temporanee ai gruppi ed eliminarle. Se le assegnazioni temporanee ai gruppi selezionate sono in stato Attivo, Attivo con errore o In sospeso, anche l'opzione **Annulla** è abilitata.

Gestione di gruppi di distribuzione dinamici

Un gruppo di distribuzione dinamico è un oggetto del gruppo Active Directory abilitato per la posta che è possibile creare per velocizzare l'invio in massa di messaggi e-mail e di altre informazioni.

L'elenco delle appartenenze per un gruppo di distribuzione dinamico viene calcolato ogni volta che un messaggio viene inviato al gruppo, in base ai filtri e alle condizioni definiti dall'utente. Questa tipologia di gruppi differisce dai gruppi di distribuzione normale, che contiene un insieme definito di membri. Quando un messaggio e-mail viene inviato a un gruppo di distribuzione dinamico, esso viene inviato a tutti i destinatari dell'organizzazione che soddisfano i criteri definiti per tale gruppo.

DRA supporta le seguenti funzioni:

- Revisione e generazione di rapporti dell'interfaccia utente
- Supporto dell'enumerazione per gruppi di distribuzione dinamici
- Rapporti di NetIQ Reporting Center (NRC) per i gruppi di distribuzione dinamici
- Attivazione del supporto delle operazioni per i gruppi di distribuzione dinamici
- Supporto dell'estensione dell'interfaccia utente per i gruppi di distribuzione dinamici di Exchange

Task dei gruppi di distribuzione dinamici:

Creazione di un gruppo di distribuzione dinamico

È possibile creare un gruppo di distribuzione dinamico nel dominio o nel sottoalbero gestito. È anche possibile modificare le proprietà, ad esempio i membri, del nuovo gruppo di distribuzione dinamico.

Nota

- Nell'azienda potrebbe essere applicata una convenzione di denominazione mediante una policy che determina il nome che è possibile assegnare al nuovo gruppo di distribuzione dinamico.
- Di default, in DRA, il nuovo gruppo di distribuzione dinamico viene inserito nell'unità organizzativa degli utenti del dominio gestito.

Per creare un gruppo di distribuzione dinamico nella Console di delega e configurazione:

1. Selezionare il container in cui creare un gruppo da Tutti i miei oggetti gestiti nel nodo Account and Resource Management (Gestione account e risorse).
2. Selezionare **Nuovo** > **Gruppo di distribuzione dinamico** nel menu Task.
3. Completare i passaggi della procedura guidata.

Per creare un gruppo di distribuzione dinamico nella console Web:

1. Selezionare il titolo **Gestione** e il container in cui creare un gruppo da Tutti i miei oggetti gestiti nel nodo Account and Resource Management (Gestione account e risorse).
2. Selezionare **Gruppo di distribuzione dinamico** dal menu a discesa Crea.
3. Immettere le informazioni richieste nel modulo e fare clic su **Crea**.

Clonazione di un gruppo di distribuzione dinamico

È possibile clonare i gruppi di distribuzione dinamici locali e globali che si trovano nei domini gestiti. La clonazione di gruppi di distribuzione dinamici consente di creare nuovi gruppi di distribuzione dinamici dello stesso tipo e con gli stessi attributi del gruppo di distribuzione dinamico originale.

Clonando un gruppo di distribuzione dinamico, è possibile creare rapidamente gruppi di distribuzione dinamici basati su altri gruppi di distribuzione dinamici con proprietà simili. Quando si clona un gruppo di distribuzione dinamico, DRA popola i campi della procedura guidata Clone Dynamic Distribution Group (Clona gruppo di distribuzione dinamico) con i valori del gruppo di distribuzione dinamico selezionato. È anche possibile modificare le proprietà del nuovo gruppo di distribuzione dinamico.

Spostamento di un gruppo di distribuzione dinamico in un altro container

È possibile spostare un gruppo di distribuzione dinamico in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Cancellazione di un gruppo di distribuzione dinamico

È possibile cancellare i gruppi di distribuzione dinamici locali e globali nel dominio o nel sottoalbero gestito. Se il Cestino è disabilitato per il dominio, l'eliminazione di un gruppo di distribuzione dinamico ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, la cancellazione del gruppo di distribuzione dinamico ne determina lo spostamento nel Cestino disabilitandone le proprietà.

Per ulteriori informazioni sul Cestino, vedere la sezione Gestione del Cestino.

Avviso: Quando si crea un gruppo di distribuzione dinamico, Microsoft Windows assegna un identificatore di sicurezza (SID) al gruppo. Il SID non viene generato dal nome del gruppo di distribuzione dinamico. Microsoft Windows utilizza i SID per registrare i privilegi negli ACL (elenchi di controllo di accesso) per ogni risorsa. Se si cancella un gruppo di distribuzione dinamico, non è possibile restituire le funzionalità di accesso del gruppo mediante la creazione di un nuovo gruppo di distribuzione dinamico avente lo stesso nome.

Modifica delle proprietà del gruppo di distribuzione dinamico

È possibile modificare le proprietà per gruppi di distribuzione dinamici locali e globali. Le competenze sono determinate dalle proprietà che è possibile modificare per un gruppo nel dominio o nel sottoalbero gestito.

Specifica di un filtro

L'appartenenza dell'elenco di distribuzione dinamico dipende dal relativo filtro. Il filtro può essere definito.

Specifica delle condizioni

Le condizioni definiscono i criteri che un oggetto deve soddisfare per essere un membro del gruppo di distribuzione dinamico.

Gestione dei gruppi dinamici

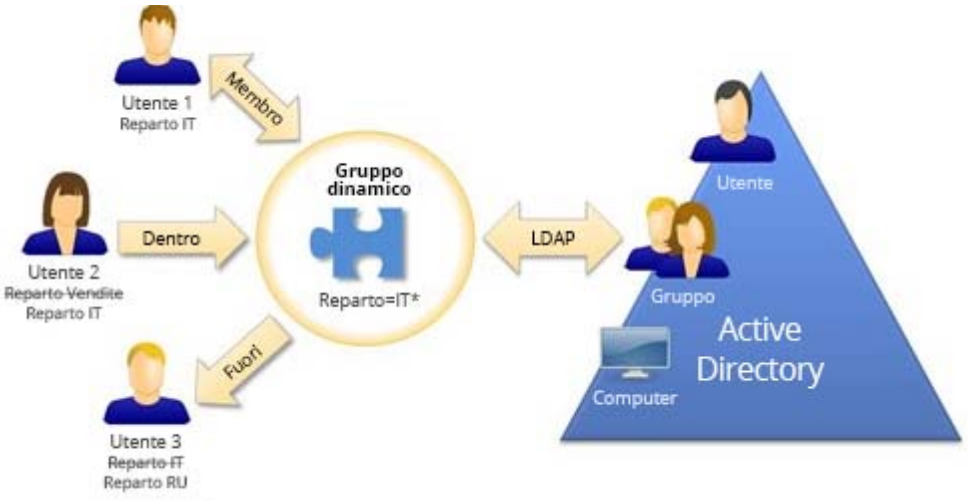
Un gruppo dinamico è un gruppo la cui appartenenza cambia in base a un insieme di criteri definiti. In DRA è possibile creare gruppi dinamici senza disporre di un ambiente Exchange. I filtri di appartenenza utilizzati per la gestione dei gruppi dinamici in Active Directory sono specifici per DRA.

L'amministratore DRA configura la pianificazione dell'aggiornamento del dominio per i gruppi dinamici nella Console di delega e configurazione. I nuovi membri vengono aggiunti dinamicamente al gruppo quando vengono aggiornate una o più proprietà utente corrispondenti ai criteri di Filtro membri del gruppo e viene eseguito un aggiornamento. Analogamente, un membro può essere rimosso dinamicamente dal gruppo quando le proprietà corrispondenti vengono modificate o rimosse dall'utente.

Esempio di scenario

La figura riportata di seguito mostra l'utilizzo tipico di un gruppo dinamico di Active Directory. Nella figura sono presenti tre gruppi dinamici. Ciascun gruppo contiene una serie di criteri che determinano chi può essere aggiunto al gruppo e chi no. Ciascun gruppo controlla l'accesso a un gruppo specifico di file, cartelle e applicazioni.

Suggerimento: È possibile creare un *elenco di membri statici* che contenga membri permanenti del gruppo dinamico; è inoltre possibile creare un *elenco dei membri esclusi* che impedisce a tali utenti l'appartenenza al gruppo dinamico.



User2 è stato recentemente aggiunto al reparto IT. Quando il gruppo dinamico del reparto IT viene aggiornato, User2 verrà aggiunto al gruppo. Quando il gruppo dinamico del reparto vendite viene aggiornato, User2 verrà rimosso dall'elenco dei membri.

User3, che ha lasciato il reparto IT ed è entrato a far parte del reparto HR, verrà rimosso dal gruppo dinamico del reparto IT e verrà aggiunto al gruppo dinamico del reparto HR.

Preparazione dello scenario

Le seguenti informazioni forniscono un esempio delle azioni da intraprendere nella console Web per abilitare lo scenario precedente. È possibile rendere dinamico un gruppo esistente o creare un nuovo gruppo dinamico. Per semplificare la procedura, non verranno aggiunti membri statici o esclusi e tre gruppi esistenti verranno resi dinamici: Gruppo HR, Gruppo IT e Gruppo vendite.

Configurazione del gruppo dinamico:

1. Per ciascun gruppo specificato in precedenza, eseguire un'operazione di ricerca con il filtro Gruppo abilitato per individuare il gruppo.
2. Aprire le **Proprietà** del gruppo e accedere alla pagina **Filtro membri dinamici**.
3. Fare clic sul dispositivo di scorrimento **Rendi dinamico il gruppo** per abilitare la funzione.
4. Fare clic su **Modifica** e digitare o incollare i criteri di Filtro membri nel campo della query LDAP. In questo caso si stanno cercando i criteri nella proprietà **Utente** > **Reparto**. Gli esempi riportati di seguito mostrano i criteri LDAP che verranno utilizzati per ciascun gruppo nell'esempio di scenario:
   - Gruppo HR: *(&(objectClass=user)(objectCategory=person)(department=HR*))*
   - Gruppo IT: *(&(objectClass=user)(objectCategory=person)(department=IT*))*
   - Gruppo Vendite: *(&(objectClass=user)(objectCategory=person)(department=Sales*))*
5. Fare clic su **Applica** per salvare le modifiche.

Azioni intraprese per modificare dinamicamente l'affiliazione al gruppo di utenti nelle proprietà dell'utente selezionato:

- User2: la proprietà **Organizzazione** > **Reparto** è stata modificata da "Vendite" a "IT".
- User3: la proprietà **Organizzazione** > **Reparto** è stata modificata da "IT" a "HR".

Le modifiche dinamiche vengono applicate durante l'aggiornamento pianificato del gruppo dinamico o durante l'aggiornamento manuale seguito dall'amministratore DRA.

Task dei gruppi dinamici

I task dei gruppi dinamici che è possibile eseguire nella console Web sono descritti di seguito.

Creazione di un gruppo

È possibile creare un gruppo dinamico nel dominio o nel sottoalbero gestito. È anche possibile modificare le proprietà, ad esempio i membri dei gruppi per il nuovo gruppo dinamico. Per creare un nuovo gruppo dinamico, passare a **Crea** > **Gruppo dinamico** nel titolo Gestione.

Nota: Nell'azienda potrebbe essere applicata una convenzione di denominazione mediante una policy che determina il nome che è possibile assegnare al nuovo gruppo dinamico.

Creazione di un filtro

Il gruppo dinamico utilizza il **Filtro membri dinamici** per aggiungere o rimuovere utenti dal proprio elenco di appartenenze ogni volta che il gruppo viene aggiornato. Per esempi di creazione di query LDAP e di attributi virtuali per il filtro, è possibile fare riferimento agli esempi illustrati in “Query di ricerca avanzate”. Gli esempi di query sono ancora applicabili quando il filtro viene utilizzato come criterio per l'appartenenza ai gruppi e non come ricerca:

- Esempi di query LDAP
- Esempi di query di attributo virtuale

Gestione dell'elenco dei membri statici

Gli utenti inseriti nell'elenco dei membri statici del gruppo dinamico diventano membri permanenti del gruppo finché non vengono rimossi manualmente. È possibile modificare questo elenco dalla pagina delle proprietà Filtro membri dinamici di un utente selezionato.

Quando si rimuovono i membri da un gruppo dinamico, DRA non cancella gli oggetti. Se si aggiungono membri a un gruppo dinamico, è necessario disporre dei poteri di modifica per gli oggetti che si desidera aggiungere.

Gestione dell'elenco dei membri esclusi

Gli utenti inseriti nell'elenco dei membri esclusi del gruppo dinamico non potranno entrare a far parte del gruppo fino a quando non verranno manualmente rimossi dall'elenco. È possibile modificare questo elenco dalla pagina delle proprietà Filtro membri dinamici di un utente selezionato.

Aggiornamento dell'elenco dei membri

È possibile aggiornare i membri in un gruppo dinamico, eseguendo un'azione **Update Member** (Aggiorna membri).

Clonazione di un gruppo dinamico

È possibile clonare i gruppi dinamici locali e globali nei domini gestiti. La clonazione dei gruppi dinamici consente di creare nuovi gruppi dinamici dello stesso tipo e con gli stessi attributi del gruppo dinamico originale.

La clonazione di un gruppo dinamico consente di creare rapidamente gruppi dinamici basati su altri gruppi dinamici con proprietà simili. Quando si clona un gruppo dinamico, DRA popola i campi della procedura guidata Clone Dynamic Group (Clona gruppo dinamico) con i valori del gruppo dinamico selezionato. È anche possibile modificare le proprietà del nuovo gruppo dinamico.

Per clonare un gruppo dinamico, selezionarlo nel riquadro dei risultati della ricerca e fare clic su **Clona** sulla barra degli strumenti.

Spostamento di un gruppo dinamico in un altro container

È possibile spostare un gruppo dinamico in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Per spostare un gruppo dinamico, selezionarlo nel riquadro dei risultati della ricerca e fare clic su **Sposta oggetti** sulla barra degli strumenti.

Cancellazione di un gruppo dinamico

È possibile cancellare i gruppi dinamici locali e globali nel dominio o nel sottoalbero gestito. Se il Cestino è disabilitato per tale dominio, l'eliminazione di un gruppo dinamico ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, la cancellazione di un gruppo dinamico ne determina lo spostamento nel Cestino disabilitandone le proprietà. Per ulteriori informazioni sul Cestino, vedere la sezione Gestione del Cestino.

Per eliminare un gruppo dinamico, selezionarlo nel riquadro dei risultati della ricerca e fare clic su **Cancella** sulla barra degli strumenti.

Avviso: Quando si crea un gruppo dinamico, Microsoft Windows assegna un identificatore di sicurezza (SID) al gruppo. Il SID non viene generato dal nome del gruppo dinamico. Microsoft Windows utilizza i SID per registrare i privilegi negli ACL (elenchi di controllo di accesso) per ogni risorsa. Se si cancella un gruppo dinamico, non è possibile restituire le funzionalità di accesso per tale gruppo mediante la creazione di un nuovo gruppo di dinamico con lo stesso nome.

Modifica delle proprietà del gruppo dinamico

È possibile modificare le proprietà per i gruppi dinamici locali e globali. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un gruppo nel dominio o nel sottoalbero gestito.

Nota: DRA consente di esportare i risultati di **Membri** e **Membro di** come file CSV. Per esportare i risultati di **Membri** o **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membri** o **Membro di**e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Per modificare le proprietà di un gruppo dinamico, selezionarlo nel riquadro dei risultati della ricerca e fare clic su **Proprietà** sulla barra degli strumenti.

Aggiunta di gruppi dinamici ad altri gruppi dinamici

È possibile nidificare gruppi dinamici aggiungendo un gruppo dinamico a un altro gruppo dinamico gestito. Quando un gruppo dinamico viene nidificato in un altro gruppo dinamico, il gruppo dinamico secondario può ereditare le autorizzazioni dal gruppo dinamico principale.

Per aggiungere un gruppo dinamico a un altro gruppo dinamico, selezionarlo nel riquadro dei risultati della ricerca e fare clic su **Aggiungi ai gruppi** sulla barra degli strumenti.

Nota: Se l'aggiunta di un gruppo dinamico a un altro gruppo dinamico aumenta i poteri del gruppo dinamico di origine, DRA non consentirà di eseguire l'operazione.

Configurazione delle autorizzazioni di sicurezza per le appartenenza ai gruppi

È possibile impostare le autorizzazioni di sicurezza di Active Directory per le appartenenze ai gruppi dinamici. Queste autorizzazioni consentono di specificare chi può visualizzare (lettura) e modificare (scrittura) le appartenenze ai gruppi dinamici utilizzando Microsoft Outlook. Consentono inoltre di proteggere con maggiore efficacia gli elenchi di distribuzione e i gruppi dinamici di sicurezza presenti nel proprio ambiente. Non è possibile modificare le autorizzazioni di sicurezza ereditate.

È possibile aggiornare queste impostazioni dalla pagina delle proprietà **Sicurezza appartenenza**di un gruppo dinamico selezionato.

Nota: Quando si gestisce la sicurezza dell'appartenenza ai gruppi dinamici, le autorizzazioni disabilitate possono indicare le autorizzazioni ereditate.

Configurazione della proprietà di un gruppo dinamico

È possibile concedere l'autorizzazione di proprietà del gruppo dinamico in un account utente, gruppo o contatto. La concessione della proprietà di un gruppo dinamico consente all'account utente, al gruppo o al contatto specificato di modificare le appartenenze al gruppo.

È possibile aggiornare queste impostazioni dalla pagina delle proprietà **Gestito da**di un gruppo dinamico selezionato.

Esposizione delle appartenenze ai gruppi dinamici negli elenchi di distribuzione

È possibile esporre le appartenenze ai gruppi dinamici negli elenchi di distribuzione per i gruppi nel dominio o nel sottoalbero gestito.

È possibile accedere a questa opzione dal menu a discesa **Exchange** sulla barra degli strumenti per un gruppo dinamico selezionato.

Come nascondere le appartenenze ai gruppi dinamici dagli elenchi di distribuzione

È possibile nascondere le appartenenze ai gruppi dinamici negli elenchi di distribuzione per gruppi nel dominio o nel sottoalbero gestito.

È possibile accedere a questa opzione dal menu a discesa **Exchange** sulla barra degli strumenti per un gruppo dinamico selezionato.

Nota: L'opzione **Hide Group Membership** (Nascondi appartenenza ai gruppi) è disabilitata per gli elenchi di distribuzione di Microsoft Exchange 2007.

Gestione dei contatti

DRA consente di gestire molti oggetti di rete, inclusi i contatti e gli indirizzi e-mail associati. I contatti sono disponibili solo nei domini Microsoft Windows in modalità mista o nativa. I contatti non possiedono un identificatore di sicurezza (SID), come gli account utente e i gruppi. È possibile utilizzare la scheda contatti per aggiungere membri a gruppi o a elenchi di distribuzione senza concedere loro accesso ai servizi di rete.

È possibile aggiungere contatti a gruppi di sicurezza o di distribuzione nei domini in modalità mista e nativa. Poiché i gruppi di sicurezza possono essere utilizzati come elenchi di distribuzione in Microsoft Windows, si consiglia di aggiungere contatti a questi gruppi. La presenza di un contatto in un gruppo di sicurezza globale non impedisce al gruppo di essere convertito in un gruppo di sicurezza universale quando si esegue la migrazione di un dominio Microsoft Windows in modalità nativa.

È possibile eseguire la maggior parte dei task dalla scheda **Gestione** > **Ricerca** della console Web. Per individuare e selezionare il contatto desiderato, eseguire un'operazione di ricerca. Dopo la selezione di uno o più contatti nell'elenco, la barra dei task si attiva con opzioni della barra degli strumenti e di menu a discesa per **Exchange**. Posizionare il puntatore del mouse su un'icona della barra degli strumenti o fare clic su un menu a discesa per visualizzarne le funzioni o le opzioni.

Modifica delle proprietà dei contatti

È possibile modificare le proprietà dei contatti. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un contatto nel dominio gestito. Se si è installato Exchange e si è abilitato il relativo supporto, è possibile modificare le proprietà dell'indirizzo e-mail mentre si gestiscono i contatti.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Creazione di un nuovo contatto

È possibile creare contatti nel dominio o nel sottoalbero gestito. È inoltre possibile modificare le proprietà, abilitare l'e-mail e specificare gli indirizzi e-mail nonché le appartenenze ai gruppi per il nuovo contatto.

Per creare un nuovo contatto, accedere a **Gestione** > **Ricerca** e selezionare **Contatto** nel menu a discesa Crea.

Clonazione di un contatto

Per clonare un contatto, è possibile creare rapidamente contatti in base ad altri contatti con proprietà simili. Quando si clona un contatto, DRA popola i campi della procedura guidata contatto Clone Contact (Clona contatto) con i valori del contatto selezionato. È inoltre possibile modificare le proprietà, abilitare l'e-mail e specificare indirizzi e-mail nonché le appartenenze ai gruppi per il nuovo contatto.

Gestione delle appartenenze ai gruppi per i contatti

È possibile aggiungere o rimuovere i contatti da un gruppo specifico nel dominio o nel sottoalbero gestito. È inoltre possibile visualizzare o modificare le proprietà di gruppi esistenti a cui appartiene il contatto.

Spostamento di un contatto in un'altra unità organizzativa

È possibile spostare un contatto in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Cancellazione di un contatto

È possibile cancellare un contatto dal dominio o dal sottoalbero gestito. Se il Cestino è disabilitato per tale dominio, l'eliminazione di un contatto ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, la cancellazione di un contatto ne determina lo spostamento nel Cestino.

Per ulteriori informazioni sul Cestino, vedere la sezione Gestione del Cestino.

Gestione degli account del servizio gestito del gruppo

Un account gMSA (group Managed Service Account) è un account di dominio gestito che è possibile assegnare ai servizi sulle risorse del computer. Non è necessario aggiornare manualmente la password per questi account in Active Directory poiché vengono gestite automaticamente da Windows Server.

È possibile creare e gestire un account gMSA dalla console Web di DRA. Un account del servizio gestito dal gruppo può essere utilizzato con più computer per eseguire i servizi. I computer che utilizzano un account gMSA richiedono la password corrente da Active Directory per avviare i servizi.

Con i poteri appropriati, è possibile eseguire diversi task correlati agli account gMSA. Per individuare e selezionare l'oggetto gMSA desiderato, eseguire un'operazione di ricerca. Dopo aver selezionato uno o più oggetti nell'elenco, la barra delle applicazioni diventa attiva con opzioni per eliminare oggetti, aggiungere oggetti a gruppi, rimuovere oggetti da gruppi, spostare oggetti da un container a un altro e modificare le proprietà dell'account gMSA. È inoltre possibile effettuare il download dei risultati della ricerca come file CSV. Fare clic sulle opzioni per visualizzarne le funzioni.

Creazione di un account gMSA

Quando si crea un account gMSA, è necessario specificare l'host in cui viene utilizzato l'account e gli oggetti Computer che possono utilizzare l'account. Gli oggetti Computer definiti nella policy di appartenenza possono utilizzare l'account gMSA per eseguire i servizi. In alternativa, è possibile specificare un gruppo di sicurezza contenente un elenco di oggetti Computer.

Per creare un nuovo account gMSA, accedere a **Gestione** > **Ricerca** e selezionare **Account del servizio gestito del gruppo** nel menu a discesa Crea.

Modifica delle proprietà dell'account gMSA

È possibile modificare le proprietà dell'account gMSA. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un account gMSA nel dominio gestito.

Abilitazione dell'account gMSA

L'abilitazione di un account gMSA consente di utilizzare l'account gMSA come credenziali di login per un servizio del computer. È possibile abilitare o disabilitare un account gMSA dalla scheda Account.

Gestione delle appartenenze ai gruppi per gli account gMSA

È possibile aggiungere o rimuovere gli account gMSA da un gruppo specifico nel dominio o nel sottoalbero gestito.

Spostamento di un account gMSA in un altro container

Un account gMSA viene creato di default nel container dell'account del servizio gestito in Active Directory. È possibile spostare un account gMSA dal container di default in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Eliminazione di un account gMSA

È possibile eliminare in modo definitivo un account gMSA dal dominio o dal sottoalbero gestito.

5 Gestione degli oggetti Azure

In questo capitolo sono riportate informazioni concettuali e procedurali per la gestione di account utente Azure, contatti Azure e gruppi Azure nella console Web. Con i poteri appropriati è possibile eseguire diversi task di gestione degli utenti, dei contatti e dei gruppi Azure, ad esempio la creazione e l'eliminazione di oggetti account utente Azure.

È possibile eseguire la maggior parte dei task per gli oggetti utente Azure, contatto Azure e gruppo Azure dalla scheda **Gestione** > **Ricerca** nella console Web eseguendo la ricerca di oggetti in uno dei seguenti nodi:

- Tutti i miei oggetti gestiti
- Tutti i miei tenant gestiti
- Un nodo secondario di Tutti i miei tenant gestiti

Gli argomenti includono quanto segue:

Gestione degli account utente Azure

In qualità di amministratore aggiunto, è possibile utilizzare DRA per gestire gli account utente Azure e modificarne le proprietà quando Azure Active Directory è configurato dall'amministratore DRA.

Per individuare e selezionare l'oggetto utente Azure desiderato, eseguire un'operazione di ricerca. Dopo aver selezionato uno o più oggetti dell'elenco, la barra dei task diventa attiva con opzioni quali opzioni di cancellazione, opzioni di concessione o blocco dell'accesso, opzioni di reimpostazione della password e opzioni di modifica delle proprietà. È inoltre possibile effettuare il download dei risultati della ricerca come file CSV. Fare clic sulle opzioni per visualizzarne le funzioni.

Creare un account utente Azure

È possibile creare account utente Azure in Azure Active Directory. È inoltre possibile abilitare l'e-mail e specificare le appartenenze ai gruppi per il nuovo account.

Modificare le proprietà degli account utente Azure

È possibile gestire le proprietà degli account utente Azure in Azure Active Directory. I poteri di cui si dispone determinano quali proprietà è possibile modificare per un account utente Azure. Se l'account utente Azure dispone di una casella postale Office 365 o se è abilitato per la posta, è possibile gestire le proprietà correlate alla casella postale e alla posta per l'account utente Azure. È possibile gestire le policy delle casella postale, impostare le restrizioni e le opzioni di consegna, impostare i limiti di memorizzazione, delegare le autorizzazioni della casella postale, impostare un blocco una controversia legale, gestire gli indirizzi e-mail e così via.

Nota

- È possibile aggiornare le proprietà Telefono cellulare e Telefoni ufficio solo per gli utenti Azure non amministratori.
- DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Consentire il login a un account utente Azure

È possibile abilitare un account utente Azure per il login ad Azure Active Directory.

Bloccare il login a un account utente Azure

È possibile impedire il login di un account utente Azure ad Azure Active Directory.

Reimpostare la password di un account utente Azure

È possibile reimpostare la password di un account utente Azure in Azure Active Directory e scegliere se DRA deve generare una nuova password per l'account.

Cancellare un account utente Azure

È possibile cancellare un account utente Azure da Azure Active Directory ma non è possibile ripristinarlo da DRA.

Specificare l'appartenenza a un gruppo Azure per gli account utente Azure

È possibile aggiungere o rimuovere account utente Azure da un gruppo Azure specifico in Azure Active Directory.

Gestione dei gruppi Azure

In qualità di amministratore aggiunto, è possibile utilizzare DRA per gestire i gruppi Azure quando Azure Active Directory è configurato dall'amministratore DRA. I gruppi Azure consentono di assegnare autorizzazioni specifiche a un gruppo di account utente definito. Consentono inoltre di controllare a quali dati e risorse un account utente può accedere in qualsiasi tenant.

Per individuare e selezionare l'oggetto gruppo Azure desiderato, eseguire un'operazione di ricerca. Dopo aver selezionato uno o più oggetti nell'elenco, la barra dei task diventa attiva con opzioni per eliminare oggetti, aggiungere oggetti a gruppi, rimuovere oggetti da gruppi, aggiungere gruppi ad altri gruppi, rimuovere gruppi da gruppi esistenti e modificare le proprietà del gruppo. Fare clic sulle opzioni per visualizzarne le funzioni.

Nota: Membri supportati: i membri del gruppo Azure possono essere utenti Azure, gruppi Azure, contatti Azure, utenti sincronizzati, contatti sincronizzati e gruppi sincronizzati.

Aggiunta di account a gruppi Azure

È possibile aggiungere account utente, contatti e gruppi (sia locali che Azure) a un gruppo gestito Azure.

Questo task consente di aggiungere più account a un gruppo selezionato. È possibile aggiungere un singolo account a un gruppo selezionando l'account appropriato. Se l'aggiunta di un account a un altro gruppo aumenta i poteri dell'account, DRA non consentirà di aggiungerlo.

Nidificazione dei gruppi in Azure

È possibile nidificare i gruppi aggiungendo altri gruppi (locali ed Azure) a un gruppo Azure gestito. Quando un gruppo viene nidificato in un gruppo Azure, il gruppo secondario eredita le autorizzazioni dal gruppo principale.

Se l'aggiunta di un dominio o di un gruppo Azure a un altro gruppo Azure aumenta i poteri assegnati a quel gruppo, DRA non consentirà di eseguire l'operazione.

Creazione di un gruppo Azure

È possibile creare un gruppo Azure in Azure Active Directory. È anche possibile modificare le proprietà, ad esempio l'aggiunta di membri di un gruppo Azure al nuovo gruppo.

Se non si specifica un proprietario, per default DRA fornisce l'account di accesso tenant di Azure come proprietario.

Modifica delle proprietà del gruppo Azure

I poteri di cui si dispone determinano le proprietà modificabili per un gruppo in Azure Active Directory. Se la policy di Exchange è abilitata, è possibile gestire le proprietà di Exchange per i gruppi Azure abilitati alla posta, come il gruppo Office 365, il gruppo di sicurezza abilitato per la posta e la lista di distribuzione. A seconda del tipo di gruppo, è possibile gestire gli indirizzi e-mail del gruppo, specificare chi può inviare e-mail al gruppo, specificare gli utenti che possono inviare e-mail per conto del gruppo, impostare le opzioni di approvazione e-mail e così via.

Nota: DRA consente di esportare i risultati di **Membri** e **Membro di** come file CSV. Passare alla scheda **Membri** o **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Configurazione della proprietà di un gruppo Azure

È possibile impostare la proprietà di qualsiasi gruppo. È possibile concedere l'autorizzazione di proprietà del gruppo a un account utente o a un gruppo. La concessione della proprietà di un gruppo consente all'account utente o al gruppo specificato di gestire il gruppo comprensivo dell'appartenenza.

Cancellazione di un gruppo Azure

È possibile cancellare gruppi Azure da Azure Active Directory ma non è possibile ripristinarli da DRA.

Gestione dei contatti Azure

I contatti Azure sono oggetti abilitati per la posta che contengono un indirizzo e-mail esterno. In qualità di amministratore aggiunto, è possibile utilizzare DRA per gestire i contatti Azure e modificarne le proprietà quando Azure Active Directory è configurato dall'amministratore DRA.

Per individuare e selezionare l'oggetto contatto Azure desiderato, eseguire un'operazione di ricerca. Dopo aver selezionato uno o più oggetti nell'elenco, la barra dei task diventa attiva con opzioni per eliminare oggetti, aggiungere oggetti a gruppi, rimuovere oggetti da gruppi e modificare le proprietà del contatto. È inoltre possibile effettuare il download dei risultati della ricerca come file CSV. Fare clic sulle opzioni per visualizzarne le funzioni.

Creazione di un contatto Azure

È possibile creare un contatto Azure nel tenant gestito e specificare le informazioni di contatto e gli indirizzi e-mail per il nuovo contatto Azure.

Modifica delle proprietà del contatto Azure

È possibile modificare le proprietà dei contatti Azure. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un contatto Azure nel tenant gestito. Se la policy di Exchange è abilitata, è possibile gestire le proprietà relative alla posta, ad esempio impostare le restrizioni di consegna per i messaggi, specificare chi può inviare messaggi per conto di questo contatto Azure, specificare se il contatto Azure è visibile nell'elenco di indirizzi e così via.

Abilitazione della moderazione dei messaggi

È possibile impostare le opzioni per la moderazione dei messaggi inviati a un contatto Azure. Quando si abilita la moderazione, i messaggi inviati al contatto Azure vengono approvati da un moderatore definito prima della consegna dei messaggi. È inoltre possibile specificare gli utenti e i gruppi esentati dal processo di approvazione.

Gestione delle appartenenze ai gruppi per i contatti Azure

È possibile aggiungere o rimuovere contatti Azure nei gruppi di sicurezza abilitati per la posta e nelle liste di distribuzione.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Passare alla scheda **Membro di** e fare clic sull'icona **Download appartenenza salvata**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Eliminazione di un contatto Azure

È possibile eliminare contatti Azure da Azure Active Directory ma non è possibile ripristinarli da DRA.

6 Gestione delle caselle postali e delle cartelle pubbliche di Exchange

Utilizzando DRA è possibile gestire le caselle postali di Microsoft Exchange come un'estensione delle proprietà dell'account utente. Questa integrazione consente di semplificare i workflow di amministrazione affinché sia possibile amministrare in modo efficace le proprietà di Exchange. È inoltre possibile collegare le caselle postali di foreste di account utente e di account Exchange e gestire caselle postali risorsa, caselle postali condivise e cartelle pubbliche.

Gestione dei task della casella postale nella Console di delega e configurazione

Quando utilizza il nodo Account and Resource Management (Gestione account e risorse), l'utente esegue i task delle caselle postali pertinenti dalla scheda **Exchange Tasks** (Task di Exchange) nelle proprietà dell'oggetto, accessibile anche dal menu **Task** o dal menu di scelta rapida di un oggetto selezionato. In genere, per individuare e selezionare l'oggetto desiderato, l'utente seleziona il nodo **Tutti i miei oggetti gestiti** ed esegue un'operazione **Find Now** (Trova ora).

Gestione dei task delle caselle postali nella console Web

Quando si utilizza la console Web, si eseguono i task delle caselle postali applicabili riportati di seguito disponibili nella scheda **Gestione** > **Ricerca**. In genere, viene eseguita un'operazione di ricerca per individuare e selezionare l'oggetto della casella postale richiesta. Una volta selezionato uno o più oggetti dall'elenco, la barra delle applicazioni diventa attiva. Fare clic sulle opzioni per visualizzarne le funzioni.

Consultare i seguenti argomenti:

Gestione di task delle caselle postali dell'utente

È possibile gestire le caselle postali di Microsoft Exchange per gli account utente nel dominio o nel sottoalbero gestito. Ogni aspetto della gestione delle caselle postali di Microsoft Exchange richiede poteri differenti. I poteri di cui si dispone consentono di controllare le proprietà delle caselle postali che è possibile modificare oppure definiscono se è possibile creare, clonare, visualizzare o cancellare le caselle postali di Microsoft Exchange. È inoltre possibile gestire i diritti e le autorizzazioni sulle

caselle postali associate a un account utente per controllare la sicurezza dei propri ambienti Microsoft Exchange. Se non si dispone dei poteri necessari per modificare una scheda o un campo per la casella postale selezionata, DRA disabilita le schede e i campi che non è possibile modificare.

Oltre ai task definiti di seguito, l'amministratore di DRA può abilitare opzioni nelle proprietà dell'oggetto consentendo agli account utente di configurare le impostazioni di Skype e Skype Online. È possibile configurare Skype dagli account utente sia nella Console di delega e configurazione che nella console Web. Skype Online può essere configurato solo dalla console Web di.

Creazione di una casella postale

È possibile creare una casella postale di Microsoft Exchange per un account utente esistente. È inoltre possibile modificare le proprietà della nuova casella postale.

Nota: Quando si crea una casella postale, Exchange genera le necessarie stringhe dell'utente incaricato in base alle impostazioni delle policy di Exchange. Microsoft Exchange genera, inoltre, le stringhe dell'utente incaricato di default. Di conseguenza, quando si visualizzano le proprietà della casella postale appena creata, sarà possibile vedere entrambi i tipi di stringhe dell'utente incaricato.

Clonazione di un account utente

Quando si clona un account utente, eventuali gruppi di cui l'utente è membro vengono aggiunti automaticamente al nuovo account utente durante la configurazione. È possibile aggiungere o rimuovere gruppi dal nuovo account, abilitare l'e-mail ed eseguire eventuali altre configurazioni delle proprietà come si farebbe con qualsiasi altro nuovo account.

Nota: Quando si clona un oggetto InetOrgPerson, si crea un account utente.

Spostamento di una casella postale

È possibile spostare una casella postale di Microsoft Exchange di un account utente nella casella postale di un altro archivio o server Microsoft Exchange.

Modifica delle proprietà delle caselle postali

È possibile modificare le proprietà delle caselle postali di Exchange di Microsoft, mentre si gestiscono gli account utente associati. Le competenze di cui si dispone determinano quali proprietà delle caselle postali è possibile modificare.

Nota: Non è possibile modificare le proprietà delle caselle postali di account utente gestiti sui server dei membri.

Configurazione delle autorizzazioni di sicurezza della casella postale

È possibile specificare a quali account utente, gruppi o computer si desidera concedere o negare la possibilità di inviare e ricevere e-mail utilizzando una specifica casella postale di Microsoft Exchange. Queste impostazioni consentono di proteggere con maggiore efficacia il proprio ambiente Exchange. Non è possibile modificare le autorizzazioni di sicurezza ereditate.

Nota: Quando si gestisce la sicurezza delle casella postale, le autorizzazioni disabilitate possono indicare le autorizzazioni ereditate.

Rimozione delle autorizzazioni di sicurezza delle caselle postali

È possibile rimuovere le autorizzazioni di sicurezza di una casella postale da un account utente, da un gruppo o da un computer associato a una casella postale di Microsoft Exchange. La rimozione delle autorizzazioni di sicurezza di una casella postale impedisce all'account utente, al gruppo o all'account del computer di inviare e ricevere messaggi e-mail attraverso la casella postale specificata. Non è possibile rimuovere le autorizzazioni di sicurezza ereditate.

Configurazione dei diritti delle caselle postali

È possibile concedere o negare altri diritti su account utente, gruppi o computer per una specifica casella postale di Microsoft Exchange. Queste impostazioni consentono di proteggere il proprio ambiente Exchange con maggiore efficacia. Non è possibile modificare i diritti delle caselle postali ereditate.

Nota: Quando si gestiscono i diritti delle caselle postali, le autorizzazioni disabilitate possono indicare le autorizzazioni ereditate.

Rimozione dei diritti delle caselle postali

È possibile rimuovere i diritti delle caselle postali da account utente, gruppi o computer associati a una specifica casella postale di Microsoft Exchange. La rimozione dei diritti di una casella postale impedisce all'account utente, al gruppo o all'account del computer di utilizzare la casella postale specificata. Non è possibile rimuovere i diritti delle caselle postali ereditate.

Cancellazione di una casella postale

È possibile cancellare una casella postale associata a un account utente nel dominio o nel sottoalbero gestito. La cancellazione di una casella postale determina anche la cancellazione di tutti i messaggi che essa contiene.

Aggiunta o modifica di un indirizzo e-mail

È possibile specificare indirizzi e-mail per le caselle postali associate agli account utente nel dominio o nel sottoalbero gestito. È anche possibile assegnare indirizzi e-mail agli account utente che non dispongono di caselle postali. Quando si gestiscono caselle postali di Microsoft Exchange, è possibile aggiungere solo i tipi di indirizzi e-mail definiti dalle policy di generazione di utenti incaricati.

Specifica di un indirizzo di risposta

È possibile impostare gli indirizzi di risposta per una casella postale associata a un account utente nel dominio o nel sottoalbero gestito. Per una casella postale è possibile impostare più indirizzi di risposta. Tuttavia, non è possibile impostare come indirizzo di risposta più tipi di indirizzi e-mail. Ad esempio, non è possibile specificare più indirizzi Internet come indirizzo di risposta.

Cancellazione di un indirizzo e-mail

È possibile cancellare un indirizzo e-mail rimuovendo l'indirizzo dalla casella postale.

Specifica delle opzioni di consegna

È possibile specificare quali caselle postali l'utente può utilizzare per inviare i messaggi, impostare opzioni di inoltro e specificare i limiti del destinatario.

Specifica delle restrizioni di consegna

Impostando le restrizioni di consegna, è possibile limitare la dimensione dei messaggi in entrata e in uscita e l'accettazione dei messaggi in entrata per una specifica casella postale.

Specifica dei limiti di archiviazione

È possibile specificare i limiti di archiviazione, ad esempio per gli avvisi, in base alla dimensione di una casella postale. È inoltre possibile specificare il periodo di conservazione sul disco degli elementi cancellati.

Controllo dello stato di spostamento della casella postale

È possibile controllare lo stato di spostamento della casella postale e intraprendere azioni su di esso, ad esempio eliminare lo stato e annullare uno spostamento in corso e riprendere uno spostamento che è stato interrotto.

Gestione dei task delle caselle postali di Office 365

Questa sezione contiene informazioni su come gestire le caselle postali di Microsoft Office 365 nella Console di delega e configurazione tramite nodo Account and Resource Management (Gestione account e risorse) e nella console Web. Con i poteri appropriati è possibile eseguire diversi task di gestione degli account utente, ad esempio impostare i blocchi per controversia legale e configurare l'inoltro delle e-mail e così via.

Importante: DRA gestisce le caselle postali degli utenti Office 365 e le caselle postali condivise, le caselle postali sala e le caselle postali apparecchiatura migrate. Per consentire a DRA di gestire le caselle postali, è necessario che siano associate a un utente locale o un utente Azure gestito da DRA. Le proprietà della casella postale saranno disponibili tramite le pagine delle proprietà per gli utenti associati.

Impostazione di un blocco per controversia legale

È possibile impostare un blocco per controversia legale su una casella postale per conservarne tutto il contenuto, compresi gli elementi cancellati e le versioni originali degli elementi modificati. Inoltre, impostando un blocco per controversia legale sulla casella postale di un utente, sarà possibile conservare il contenuto, se esistente, nella casella postale di archiviazione dell'utente. Il blocco può durare per un periodo specificato o finché non viene rimosso dalla casella postale.

Per impostare un blocco per controversia legale, è necessario disporre della licenza appropriata per Exchange Online. Questa funzione può essere configurata tramite la scheda **Litigation Hold** (Blocco per controversia legale) nelle proprietà dell'oggetto utente.

Delega delle autorizzazioni della casella postale

È possibile delegare le autorizzazioni della casella postale Office 365 tramite la scheda Delega casella postale nelle proprietà dell'oggetto dell'utente. Sono disponibili tre tipi di autorizzazioni che è possibile delegare: Invia come, Invia per conto di e Accesso completo. I tipi di autorizzazione che è possibile delegare dipendono dal tipo di oggetto ricevente.

Visualizzazione dello stato della casella postale di archiviazione

È possibile visualizzare lo stato della casella postale di archiviazione per un utente e le statistiche relative alla casella postale di archiviazione, ad esempio il limite di memorizzazione e il limite di avviso. Quando la casella postale di archiviazione supera il limite di avviso di archiviazione, l'utente riceve una notifica.

Visualizzazione delle statistiche sull'utilizzo della casella postale

È possibile visualizzare la quantità della quota totale della casella postale utilizzata.

Configurazione delle restrizioni di consegna dei messaggi

Impostando le restrizioni di consegna, è possibile limitare la dimensione dei messaggi in entrata e in uscita e l'accettazione o il rifiuto dei messaggi in entrata per un utente specifico.

Specifica delle opzioni di consegna

È possibile configurare le opzioni di inoltro dei messaggi e specificare il numero massimo di destinatari ai quali un utente può inviare un messaggio.

Aggiunta o rimozione di un indirizzo e-mail

È possibile configurare più indirizzi e-mail per una casella postale utente e specificare l'indirizzo e-mail principale. È anche possibile assegnare indirizzi e-mail agli account utente che non dispongono di caselle postali.

Occultamento dell'indirizzo e-mail

È possibile specificare se si desidera che l'indirizzo e-mail non venga visualizzato nell'elenco.

Aggiunta di avviso messaggio

È possibile aggiungere testo informativo che si desidera visualizzare quando viene inviata un'e-mail all'utente.

Assegnazione di policy per la casella postale

È possibile assegnare una policy di condivisione, di conservazione e-mail, di assegnazione del ruolo o di rubrica per la casella postale.

Gestione dei task delle caselle postali risorse

La funzione di casella postale risorsa di Microsoft Exchange consente di creare una casella postale che rappresenta una risorsa, ad esempio una sala conferenze, affinché sia possibile prenotarla inviandogli un invito alla riunione, come se fosse una persona. DRA contiene un gruppo di ruoli, poteri e policy che consentono di gestire in modo efficiente le caselle postali risorsa.

Include inoltre il supporto per l'estensione dell'interfaccia per le caselle postali risorsa e il supporto per la generazione di rapporti revisione o interfaccia utente. In DRA è anche integrato il supporto degli script ADSI.

Creazione di una casella postale risorsa

È possibile creare caselle postali risorsa nel dominio o nel sottoalbero gestito.

Spostamento di una casella postale risorsa in un altro container

È possibile spostare una casella postale risorsa in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Spostamento di una casella postale risorsa nell'archivio di un'altra casella postale o nel server Exchange

È possibile spostare una casella postale risorsa nell'archivio di un'altra casella postale o nel server Microsoft Exchange.

Clonazione di una casella postale risorsa

Clonando una casella postale risorsa, è possibile creare rapidamente altre caselle postali risorsa con proprietà simili. Quando si clona una casella postale risorsa, DRA popola i campi della procedura guidata Clone Resource Mailbox (Clona casella postale risorsa) con i valori della risorsa selezionata.

Ridenominazione di una casella postale risorsa

È possibile rinominare le caselle postali risorsa nel dominio o nel sottoalbero gestito. Anche la modifica del nome di login dell'utente modifica il nome della casella postale associata all'account utente.

Aggiunta di una casella postale risorsa a un gruppo

È possibile aggiungere le caselle postali risorsa a un gruppo specifico nel dominio o nel sottoalbero gestito.

Cancellazione di una casella postale risorsa

È possibile cancellare una casella postale risorsa nel dominio o nel sottoalbero gestito. La cancellazione di una casella postale di risorsa comporta anche l'eliminazione di tutti i messaggi della casella postale e degli oggetti utente disabilitati associati alla casella postale della risorsa. Se lo si desidera, è possibile ignorare la cancellazione degli oggetti utente disabilitati quando si cancella la casella postale. Se si cancella un oggetto utente associato a una casella postale risorsa, viene cancellata anche la casella postale risorsa.

Ripristino di una casella postale risorsa cancellata

È possibile ripristinare una casella postale risorsa che è stata cancellata se nel dominio è abilitato il Cestino.

Modifica delle proprietà della casella postale risorsa

È possibile gestire le proprietà delle caselle postali risorsa nel dominio o nel sottoalbero gestito. I poteri di cui si dispone determinano quali proprietà è possibile modificare.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Gestione dei task delle caselle postali condivise

Le caselle postali condivise sono utili per gli amministratori e il personale del supporto tecnico, in quanto tutte le risposte possono essere configurate per essere inserite in una singola casella postale a cui possono accedere più utenti. La casella postale deve trovarsi in un dominio DRA gestito in cui siano abilitate le policy di Exchange e sul quale l'utente deve disporre di poteri delegati per la gestione delle caselle postali condivise.

Quando si crea una casella postale condivisa, sono disponibili due tipi di autorizzazioni che è possibile delegare agli utenti: Invia come e Accesso completo. Invia come fornisce l'autorizzazione di lettura e invio delle e-mail. È possibile delegare le autorizzazioni sia agli oggetti utente che gruppo. È inoltre possibile specificare le restrizioni e le opzioni di consegna, i limiti di archiviazione, le autorizzazioni sulla cartella e altre opzioni nelle proprietà dell'oggetto.

Nota: È possibile eseguire i task di gestione per le caselle postali condivise solo tramite la console Web.

Creazione di una casella postale condivisa

È possibile creare caselle postali condivise nel dominio o nel sottoalbero gestito.

Spostamento di una casella postale condivisa in un altro container

È possibile spostare una casella postale condivisa in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Spostamento di una casella postale condivisa nell'archivio di un'altra casella postale

È possibile spostare una casella postale condivisa nell'archivio di un'altra casella postale.

Clonazione di una casella postale condivisa

Clonando una casella postale condivisa, è possibile creare rapidamente altre caselle postali condivise con proprietà simili.

Ridenominazione di una casella postale condivisa

È possibile rinominare condivise caselle postali nel dominio o nel sottoalbero gestito. Anche la modifica del nome di login dell'utente modifica il nome della casella postale associata all'account utente.

Cancellazione di una casella postale condivisa

È possibile cancellare una casella postale condivisa nel dominio o nel sottoalbero gestito. Se il Cestino è disabilitato per tale dominio, l'eliminazione di una casella postale condivisa ne determina la rimozione definitiva da Active Directory. Se invece il Cestino è abilitato per il dominio, l'eliminazione di una casella postale condivisa ne determina lo spostamento nel Cestino.

La cancellazione di una casella postale condivisa comporta anche l'eliminazione di tutti i messaggi della casella postale e degli oggetti utente disabilitati associati alla casella postale condivisa. Se si cancella un oggetto utente associato a una casella postale condivisa, viene cancellata anche la casella postale condivisa.

Ripristino di una casella postale condivisa cancellata

È possibile ripristinare una casella postale condivisa che è stata cancellata se nel dominio è abilitato il Cestino.

Creazione di una casella postale condivisa di archiviazione

È possibile creare caselle postali condivise archiviate nel dominio o nel sottoalbero gestito.

Cancellazione di una casella postale condivisa di archiviazione

È possibile cancellare le caselle postali condivise archiviate nel dominio o nel sottoalbero gestito.

Modifica delle proprietà delle caselle postali condivise

È possibile modificare le proprietà delle caselle postali condivise nel dominio o nel sottoalbero gestito. I poteri di cui si dispone determinano quali proprietà è possibile modificare.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Gestione dei task delle caselle postali collegate

Le caselle postali collegate sono utili quando si eseguono modifiche organizzative di vasta portata, ad esempio nel caso di fusioni, acquisizioni e divisioni aziendali, in cui la migrazione delle caselle postali è una prassi comune. Questa funzione consente di collegare le caselle postali di foreste Exchange differenti per impedire l'interruzione delle attività e-mail dell'utente. Le caselle postali devono trovarsi in un dominio DRA gestito in cui siano abilitate le policy di Exchange e sul quale l'utente deve disporre di poteri delegati per la gestione delle caselle postali collegate. Quando si crea una casella postale collegata, alle proprietà dell'oggetto viene aggiunta una scheda **Casella postale collegata**.

La gestione delle caselle postali collegate è supportata solo nella console Web. Una casella postale collegata può essere creata dalla barra degli strumenti di un account utente selezionato. Questa opzione è abilitata solo quando il dominio dell'utente selezionato dispone di una relazione di attendibilità per la foresta esterna con altri domini gestiti in DRA. Quando si ricercano account utente per il collegamento a un altro dominio DRA gestito verranno elencati solo gli account utente disabilitati.

Creazione di una casella postale collegata

È possibile creare una casella postale collegata da due account utente selezionati in diverse foreste Exchange gestite.

Cancellazione di una casella postale collegata

È possibile cancellare una casella postale collegata dalla barra degli strumenti di un utente selezionato contenente una casella postale collegata.

Modifica delle proprietà della casella postale collegata

È possibile modificare le proprietà di una casella postale collegata dalla scheda **Casella postale collegata** nella finestra delle proprietà dell'utente selezionato.

Creazione di una casella postale di archiviazione collegata

È possibile creare una casella postale di archiviazione collegata da un utente selezionato che possiede una casella postale collegata.

Cancellazione di una casella postale di archiviazione collegata

È possibile cancellare una casella postale di archiviazione collegata dalla barra degli strumenti di un utente selezionato che possiede una casella postale di archiviazione collegata.

Ripristino di una casella postale collegata cancellata

È possibile ripristinare una casella postale collegata che è stata cancellata se nel dominio è abilitato il Cestino.

Gestione dei task delle cartelle pubbliche

Se l'amministratore DRA ha creato foreste di cartelle pubbliche nell'azienda gestita con DRA e ha concesso all'utente poteri di gestione delle cartelle pubbliche nel programma, sarà possibile creare cartelle pubbliche, modificarne le proprietà e generare rapporti della cronologia modifiche. La creazione e la modifica delle cartelle pubbliche possono essere eseguite solo nella console Web. È possibile utilizzare l'opzione di ricerca per cercare le cartelle pubbliche. Per ulteriori informazioni, vedere *"Ricerca" a pagina 41*.

I task delle cartelle pubbliche vengono eseguite dalla scheda **Gestione** > **Cartelle pubbliche**.

Creazione di una cartella pubblica

È possibile creare nuove cartelle pubbliche nelle caselle postali tramite la console Web, in domini, sottoalberi e caselle postali di cartelle pubbliche. È possibile utilizzare la casella postale di default per il dominio selezionato oppure sceglierne una.

Abilitazione dell'e-mail per una cartella pubblica

È possibile abilitare l'e-mail per una cartella pubblica mediante l'opzione **Abilita posta** sulla barra degli strumenti dell'elenco. Questo consente di associare gli indirizzi e-mail con la cartella pubblica e modificare le proprietà della cartella.

Disabilitazione dell'e-mail per una cartella pubblica

È possibile disabilitare l'e-mail per una cartella pubblica utilizzando l'opzione **Disabilita posta** sulla barra degli strumenti dell'elenco.

Modifica delle proprietà delle cartelle pubbliche

Dopo aver abilitato la posta su una cartella pubblica esistente, è possibile visualizzare le statistiche della cartella e modificare le proprietà della stessa. In queste proprietà è possibile specificare le opzioni di consegna e le restrizioni dell'utente, i limiti delle dimensioni e gli avvisi sulla quota, le proprietà della posta, i limiti della durata dell'archiviazione, l'inserimento di moderatori per approvare la posta e gli attributi personalizzati.

Nota: È inoltre possibile aggiornare alcune proprietà per più cartelle pubbliche, quando sono selezionate più opzioni, ad esempio le quote di archiviazione.

Cancellazione di una cartella pubblica

È possibile cancellare le cartelle pubbliche se non includono sottocartelle e l'opzione relativa all'e-mail è disabilitata.

7 Gestione delle risorse

DRA consente di gestire le risorse inclusi computer, stampanti e altri dispositivi, nonché i processi associati. Se, ad esempio, è necessario avviare un servizio specifico in un computer gestito, si potrebbe ricercare tale oggetto computer in DRA, accedere ai relativi servizi mediante le proprietà dell'oggetto, quindi riavviare un servizio specifico da DRA su tale computer senza doversi connettere a quest'ultimo da remoto.

Gestione delle unità organizzative (UO)

In questa sezione viene illustrato come amministrare le unità organizzative nella Console di delega e configurazione tramite il nodo Account and Resource Management (Gestione account e risorse). Con i poteri appropriati è possibile eseguire diversi task di gestione delle unità organizzative, ad esempio spostare un'unità organizzativa in un altro container.

Nota: È possibile gestire le unità organizzative solo tramite la Console di delega e configurazione.

Modifica delle proprietà delle UO

È possibile modificare le proprietà delle UO. I poteri di cui si dispone determinano le proprietà di una UO che è possibile modificare nel dominio o nel sottoalbero gestito.

Creazione di una UO

È possibile creare una UO nel dominio o nel sottoalbero gestito. È, inoltre, possibile modificare le proprietà generali della UO come, ad esempio, la descrizione.

Clonazione di una UO

È possibile creare una nuova UO clonando una UO esistente dal dominio o dal sottoalbero gestito. È, inoltre, possibile modificare le proprietà generali dalla nuova UO come, ad esempio, la descrizione. La clonazione di una UO non determina la clonazione degli oggetti che essa contiene.

Apertura di un albero Active Directory in un'ubicazione dell'UO

È possibile aprire, in modo rapido e semplice, l'albero Active Directory nell'ubicazione di una UO specifica nel dominio o nel sottoalbero gestito.

Spostamento di una UO in un altro container

È possibile spostare una UO in un container differente nel dominio gestito. Quando si gestisce un sottoalbero di un dominio, è possibile spostare le UO all'interno della gerarchia di tale sottoalbero.

Nota

- Se lo spostamento di una UO in un altro container aumenta i poteri sulla UO, DRA non consentirà l'operazione.
- È inoltre possibile spostare una UO trascinandola nella nuova ubicazione.

Cancellazione di una UO

È possibile cancellare le UO dal dominio o dal sottoalbero gestito. È possibile cancellare solo le UO vuote. Se una UO contiene degli oggetti, la cancellazione non sarà consentita. Per poter cancellare una UO contenente degli oggetti, è prima necessario cancellare gli oggetti, quindi sarà possibile cancellare la UO.

Gestione di computer

DRA consente di amministrare computer nel dominio o nel sottoalbero gestito. Ad esempio, è possibile aggiungere o rimuovere gli account del computer in domini gestiti, gestendo, al contempo, le risorse presenti su ciascun computer. Quando si aggiunge un computer a un dominio, DRA crea un account nel dominio per il computer in uso. Sarà quindi possibile connettersi al computer in tale dominio e configurare il computer per l'utilizzo di quell'account. È inoltre possibile visualizzare e modificare le proprietà dell'account del computer. DRA consente infine di arrestare un computer e sincronizzare i controller del dominio in un dominio gestito.

Nota

- È possibile gestire i computer solo tramite la Console di delega e configurazione.
- Non è possibile gestire i controller di dominio nascosti. La cache del dominio non include controller del dominio nascosti. Di conseguenza, DRA non visualizza i computer nascosti del dominio in elenchi o finestre delle proprietà

Specifica dell'appartenenza ai gruppi per i computer

È possibile aggiungere o rimuovere i computer da un gruppo specifico nel dominio o nel sottoalbero gestito. È inoltre possibile visualizzare o modificare le proprietà dei gruppi esistenti a cui appartiene il computer.

Nota: DRA consente di esportare i risultati di **Membro di** come file CSV. Per esportare i risultati di **Membro di** dalla console Web, accedere a **Gestione** > **Ricerca** e fare clic su **Proprietà**. Passare alla scheda **Membro di** e fare clic sull'icona **Download**. Le modifiche non salvate non vengono esportate. Accertarsi di salvare le modifiche recenti in modo che siano disponibili nel file esportato.

Gestione delle proprietà dell'account del computer

È possibile gestire le proprietà dell'account del computer. I poteri di cui si dispone determinano le proprietà che è possibile modificare per un computer nel dominio o nel sottoalbero gestito.

Aggiunta di un computer a un dominio

È possibile aggiungere un computer a un dominio o a un sottoalbero gestito mediante la creazione di un nuovo account del computer.

Rimozione di un computer da un dominio

È possibile rimuovere un computer da un dominio o da un sottoalbero gestito eliminando l'account del computer.

Spostamento di un computer

È possibile spostare un computer in un altro container, ad esempio un'unità organizzativa, nel dominio o nel sottoalbero gestito.

Arresto o riavvio di un computer

È possibile arrestare un computer e riavviarlo immediatamente oppure a una data e a un'ora impostate.

Reimpostazione della password dell'account amministratore

Per reimpostare la password dell'account amministratore per un computer, l'utente deve disporre del potere Reset Password for Local Administrator (Reimposta password per l'amministratore locale) oppure deve essere associato a un ruolo contenente questo potere. È possibile reimpostare la password dell'amministratore per i server dei membri nel dominio o nel sottoalbero gestito. Non è possibile reimpostare la password dell'amministratore per un controller del dominio.

Reimpostazione dell'account del computer

È possibile reimpostare un account del computer per i server dei membri nel dominio o nel sottoalbero gestito. Non è possibile reimpostare l'account del computer per un controller del dominio.

Cancellazione di un account del computer

È possibile cancellare un account del computer dal dominio o dal sottoalbero gestito. Se si sta gestendo un dominio Microsoft Windows, è possibile cancellare gli account di computer contenenti altri oggetti, ad esempio, una risorsa condivisa. Abilitare l'opzione **Forza cancellazione** per eliminare gli oggetti computer da Active Directory. Verranno inoltre cancellati gli oggetti secondari, tra cui le stampanti e le cartelle condivise. I computer cancellati e i relativi oggetti associati vengono spostati nel Cestino di DRA. Se durante la cancellazione il Cestino è disabilitato, gli oggetti vengono cancellati in modo permanente.

Nota: È possibile cancellare gli account computer per i server dei membri nel dominio o nel sottoalbero gestito.

Disabilitazione di un account del computer

È possibile disabilitare un account del computer nel dominio o nel sottoalbero gestito. La disabilitazione di un account del computer impedisce agli utenti di tale computer di eseguire il login a qualsiasi dominio.

Abilitazione di un account del computer

È possibile abilitare un account del computer nel dominio o nel sottoalbero gestito. L'abilitazione di un account del computer consente agli utenti di tale computer di eseguire il login a qualsiasi dominio.

Gestione delle risorse del computer

Per ogni account del computer nel dominio o nel sottoalbero gestito, è possibile gestire le risorse associate, quali servizi, condivisioni, dispositivi, stampanti e lavori di stampa.

Gestione dei servizi

Un servizio è un tipo di applicazione che consente di ottenere un trattamento speciale da sistema operativo Windows. I servizi possono essere eseguiti anche se a un computer non è attualmente connesso alcun utente. Gli amministratori aggiunti con i poteri appropriati possono gestire i servizi in esecuzione sui computer nel dominio o nel sottoalbero gestito.

Gestione delle proprietà dei servizi

È possibile gestire le proprietà dei servizi in esecuzione sui computer nel dominio o nel sottoalbero gestito. È possibile gestire i servizi anche mentre si gestiscono altre risorse per tale computer.

Avvio di un servizio

È possibile avviare un servizio su un computer qualsiasi del dominio o del sottoalbero gestito.

Avvio di un servizio con parametri

Quando si avviano i servizi che accettano parametri, è possibile specificare i parametri all'avvio. È possibile avviare i servizi nei computer nel dominio o nel sottoalbero gestito.

Nota: È possibile avviare un servizio con parametri solo tramite la Console di delega e configurazione.

Specifica di un tipo di avvio del servizio

È possibile modificare il tipo di avvio di un servizio, richiedendo, ad esempio, un avvio manuale.

Specifica di un account di login al servizio

È possibile modificare l'account di login al servizio per un account diverso dall'attuale account di sistema. È possibile specificare l'account del sistema locale, un account utente specifico o un account gMSA (group Managed Service Account) come account di accesso al servizio.

Riavvio di un servizio

È possibile riavviare un servizio in esecuzione su un computer nel dominio o nel sottoalbero gestito.

Per riavviare un servizio, l'utente deve disporre di entrambi i poteri Stop a Service (Arresta un servizio) e Start a Service (Avvia un servizio) o deve essere associato a un ruolo che possiede tali poteri, come il ruolo Start Service (Avvia servizio) e Stop Service (Arresta servizio).

Arresto di un servizio

È possibile arrestare un servizio in esecuzione su un computer nel dominio o nel sottoalbero gestito.

Sospensione di un servizio

È possibile sospendere un servizio in esecuzione su un computer nel dominio o nel sottoalbero gestito. Se un servizio può essere sospeso o meno dipende dal tipo di servizio. Ad esempio, potrebbe non essere possibile sospendere un servizio che include servizi dipendenti.

Ripresa di un servizio sospeso

È possibile riprendere un servizio che è stato sospeso su un computer nel dominio o nel sottoalbero gestito.

Gestione di stampanti e di lavori di stampa

Per gestire le stampanti, è necessario gestire le code di stampa che alimentano tali stampanti. DRA consente di sospendere o riprendere, avviare, modificare, arrestare e visualizzare le stampanti risorsa e le stampanti pubblicate. DRA consente anche di modificare le proprietà e le priorità dei lavori di stampa. Per aggiungere o cancellare una stampante, è possibile utilizzare gli strumenti nativi di Windows.

Un server di stampa è un computer su cui sono installate uno o più stampanti logiche. Una stampante logica è definita nel computer che possiede il driver del dispositivo di stampa. Una stampante logica include il driver di stampa, la coda di stampa e le porte di una stampante. Il server di stampa associa le stampanti logiche alle stampanti fisiche.

Una stampante connessa viene definita sui computer da cui vengono selezionati i documenti per la stampa. Una stampante connessa è una connessione a una condivisione di stampa sulla rete. Pertanto, è possibile gestire le stampanti e i lavori di stampa mediante i computer associati.

Una stampante pubblicata è un stampante pubblicata in Active Directory. Una stampante pubblicata può essere una stampante di rete che non è connessa direttamente a un server oppure che è ospitata dal server del cluster.

Nota: È possibile gestire le stampanti e i lavori di stampa solo tramite la Console di delega e configurazione.

Per ulteriori informazioni sulla gestione delle stampanti e dei task di stampa, vedere i seguenti argomenti:

- “Gestione dei task delle stampanti” a pagina 89
- “Gestione dei task dei lavori di stampa” a pagina 90
- “Gestione dei task delle stampanti pubblicate” a pagina 91
- “Gestione dei task dei lavori di stampa per le stampanti pubblicate” a pagina 92

Gestione dei task delle stampanti

È possibile gestire le stampanti associate ai computer nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse di tale computer.

In questa sezione viene illustrato come amministrare le stampanti nella Console di delega e configurazione tramite il nodo Account and Resource Management (Gestione account e risorse). Con i poteri appropriati è possibile eseguire diversi task di gestione delle stampanti come, ad esempio l'arresto di una stampante.

Gestione delle proprietà della stampante

È possibile gestire le proprietà per le stampanti nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse di tale computer.

Sospensione di una stampante

È possibile sospendere una stampante associata a un computer nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse di tale computer.

Ripristino di una stampante

È possibile ripristinare una stampante associata a un computer nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse di tale computer.

Gestione dei task dei lavori di stampa

È possibile gestire i lavori di stampa associati alle stampanti nel dominio o nel sottoalbero gestito. Poiché i lavori di stampa sono associati a una stampante, è possibile gestire i lavori di stampa mentre si gestisce la stampante.

In questa sezione viene illustrato come gestire i lavori di stampa nel nodo Account and Resource Management (Gestione account e risorse) della Console di delega e configurazione. Con i poteri appropriati è possibile eseguire diversi task di gestione dei lavori di stampa come, ad esempio l'annullamento.

Gestione delle proprietà dei lavori di stampa

È possibile modificare le proprietà dei lavori di stampa come parte del proprio workflow di gestione della stampante. Poiché i lavori di stampa sono associati alle stampanti, è possibile modificare il lavoro di stampa mentre si gestisce la stampante corrispondente. Le proprietà del lavoro di stampa che è possibile modificare dipendono dal tipo di potere di cui si dispone. Per modificare le proprietà del lavoro di stampa, è necessario poter accedere alla stampante e al computer corrispondenti.

Sospensione di un lavoro di stampa

È possibile sospendere un lavoro di stampa su una stampante del dominio o del sottoalbero gestito. Per sospendere un lavoro di stampa, è necessario poter accedere alla stampante e al computer corrispondente. La sospensione di un lavoro di stampa non ne determina la cancellazione dalla coda di stampa.

Ripresa di un lavoro di stampa

È possibile riprendere un lavoro di stampa che è stato sospeso. Per riprendere un lavoro di stampa, è necessario poter accedere alla stampante e al computer corrispondenti.

Riavvio di un lavoro di stampa

È possibile riavviare un lavoro di stampa che è stato arrestato. Per riavviare un lavoro di stampa, è necessario poter accedere alla stampante e al computer corrispondenti.

Annullamento di un lavoro di stampa

È possibile annullare un lavoro di stampa che si trova nella coda di stampa. Quando si annulla un lavoro di stampa, DRA lo cancella definitivamente dalla coda di stampa. Per annullare un lavoro di stampa, è necessario poter accedere alla stampante e al computer corrispondenti.

Gestione dei task delle stampanti pubblicate

È possibile gestire le stampanti pubblicate nel dominio o nel sottoalbero gestito. È possibile aggiungere o ricercare qualsiasi stampante pubblicata in Active Directory oppure le stampanti ospitate nel server del cluster.

In questa sezione vengono fornite informazioni sull'amministrazione delle stampanti pubblicate nel nodo Account and Resource Management (Gestione account e risorse). Con i poteri appropriati è possibile eseguire diversi task di gestione delle stampanti come, ad esempio, l'arresto di una stampante.

Gestione delle proprietà delle stampanti pubblicate

È possibile gestire le proprietà delle stampanti pubblicate nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse.

Aggiornamento delle informazioni sulle stampanti pubblicate

È possibile aggiornare le informazioni sulle stampanti pubblicate nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti pubblicate mentre si gestiscono altre risorse.

Sospensione di una stampante pubblicata

È possibile sospendere una stampante pubblicata nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti mentre si gestiscono altre risorse.

Ripristino di una stampante pubblicata

È possibile ripristinare una stampante pubblicata, che è stata sospesa nel dominio o nel sottoalbero gestito. DRA consente di gestire le stampanti pubblicate mentre si gestiscono altre risorse.

Spostamento di una stampante pubblicata

È possibile spostare una stampante pubblicata disponibile in un container del dominio gestito in un altro container dello stesso dominio. DRA consente di gestire le stampanti pubblicate mentre si gestiscono altre risorse.

Ridenominazione di una stampante pubblicata

È possibile rinominare una stampante pubblicata condivisa in Active Directory. DRA consente di gestire le stampanti pubblicate mentre si gestiscono altre risorse.

Nota: La ridenominazione di una stampante pubblicata in Active Directory non modifica il nome della condivisione della stampante risorsa né propaga la modifica del nome alla stampante risorsa che si desidera gestire. Se, ad esempio, il nome della stampante risorsa è Emerald e si rinomina la stampante Ruby in Active Directory, gli altri utenti vedranno Ruby come nome della stampante, ma il nome della stampante risorsa continuerà a essere Emerald.

Gestione dei task dei lavori di stampa per le stampanti pubblicate

È possibile gestire i lavori di stampa associati a stampanti pubblicate nel dominio o nel sottoalbero gestito. Poiché i lavori di stampa sono associati a una stampante, sarà possibile gestirli durante la gestione della stampante stessa.

In questa sezione vengono fornite informazioni sull'amministrazione delle stampanti pubblicate nel nodo Account and Resource Management (Gestione account e risorse). Con i poteri appropriati è possibile eseguire diversi task di gestione dei lavori di stampa come, ad esempio l'annullamento.

Gestione delle proprietà dei lavori di stampa

È possibile modificare le proprietà dei lavori di stampa come parte del workflow di gestione delle stampanti pubblicate. Poiché i lavori di stampa sono associati alle stampanti, è possibile modificare il lavoro di stampa durante la gestione della stampante pubblicata corrispondente. Le proprietà del lavoro di stampa che è possibile modificare dipendono dal tipo di poteri di cui si dispone. Per modificare le proprietà dei lavori di stampa, è necessario poter accedere alla stampante pubblicata corrispondente.

Sospensione di un lavoro di stampa

È possibile sospendere un lavoro di stampa in una stampante pubblicata in un dominio o in un sottoalbero gestito. Per sospendere un lavoro di stampa, è necessario poter accedere alla stampante pubblicata corrispondente. La sospensione di un lavoro di stampa non determina la cancellazione del lavoro di stampa dalla coda di stampa.

Ripresa di un lavoro di stampa

È possibile riprendere un lavoro di stampa che è stato sospeso in un dominio o in un sottoalbero gestito. Per riprendere un lavoro di stampa, è necessario poter accedere alla stampante pubblicata corrispondente.

Riavvio di un lavoro di stampa

È possibile riavviare un lavoro di stampa che è stato interrotto in un dominio o in un sottoalbero gestito. Per riavviare un lavoro di stampa, è necessario poter accedere alla stampante pubblicata corrispondente.

Annullamento di un lavoro di stampa

È possibile annullare un lavoro di stampa nella coda di stampa di un dominio o di un sottoalbero gestito. Quando si annulla un lavoro di stampa, DRA lo cancella definitivamente dalla coda di stampa. Per annullare un lavoro di stampa, è necessario poter accedere alla stampante pubblicata corrispondente.

Gestione delle condivisioni

Una condivisione è un metodo per rendere le risorse, ad esempio file o stampanti, disponibili ad altri utenti sulla rete. Ogni condivisione ha un nome che fa riferimento a una cartella condivisa sul server. DRA gestisce le condivisioni solo nei computer che si trovano in domini gestiti. Per gestire correttamente le condivisioni, l'account di accesso deve disporre delle autorizzazioni di amministrazione (ad esempio può essere un membro del gruppo di amministratori locale) su tutti i

computer in cui si desidera gestire le risorse. Per assegnare queste autorizzazioni, è necessario aggiungere l'account di accesso del gruppo di amministratori del dominio nativo al dominio del computer.

Nota: È possibile gestire le condivisioni solo tramite la Console di delega e configurazione.

Gestione delle proprietà delle condivisioni

È possibile gestire le proprietà delle condivisioni nel dominio o nel sottoalbero gestito. DRA consente di gestire le condivisioni mentre si gestiscono altre risorse di tale computer.

Creazione di una condivisione

È possibile creare una condivisione per un computer nel dominio o nel sottoalbero gestito. È anche possibile modificare le proprietà della condivisione.

Clonazione di una condivisione

È possibile clonare una condivisione per un computer nel dominio o nel sottoalbero gestito. Per clonare una condivisione, è possibile creare rapidamente condivisioni in base alle altre condivisioni con proprietà simili. Questa flessibilità consente di applicare impostazioni coerenti per tutte le condivisioni create in un determinato dominio.

Quando si clona una condivisione, DRA popola i campi della procedura guidata Clone Share (Clona condivisione) con i valori della condivisione selezionata. È anche possibile modificare le proprietà della nuova condivisione.

Cancellazione di una condivisione

È possibile cancellare le condivisioni da computer che si trovano nel dominio o nel sottoalbero gestito.

Gestione degli utenti connessi

Ogni volta che un utente si connette a una particolare risorsa su un computer remoto viene avviata una sessione. Un utente connesso è un utente che si è connesso a una risorsa condivisa sulla rete.

DRA gestisce gli utenti connessi solo sui computer che si trovano nei domini gestiti. L'account di accesso deve disporre delle autorizzazioni di amministrazione (ad esempio può essere membro del gruppo di amministratori locale) su tutti i computer in cui si desidera gestire gli utenti connessi. Per assegnare queste autorizzazioni, è necessario aggiungere l'account di accesso del gruppo di amministratori di dominio nativo al dominio del computer.

Disconnessione di un utente

È possibile disconnettere un utente connesso da un computer che si trova nel dominio o nel sottoalbero gestito. L'utente deve poter accedere al computer e deve essere avviata una sessione. La disconnessione di un utente connesso termina la sessione aperta.

Aggiornamento dell'elenco degli utenti connessi

Per essere certi di visualizzare le informazioni aggiornate sulle sessioni aperte in un computer, è necessario aggiornare manualmente l'elenco degli utenti connessi. L'utente deve poter accedere al computer e deve essere avviata una sessione.

Gestione dei dispositivi

Un dispositivo è qualsiasi un'apparecchiatura collegata a una rete, ad esempio un computer, una stampante, un modem o qualsiasi altro apparecchio esterno.

Anche se un dispositivo può essere installato nel computer utilizzato, Windows non è in grado di riconoscerlo fino a quando non si installa e si configura il driver appropriato. Il driver di un dispositivo consente la comunicazione di una parte specifica dell'hardware con il sistema operativo.

DRA consente di configurare e gestire i dispositivi solo sui computer che si trovano in domini gestiti. L'account di accesso deve disporre delle autorizzazioni di amministrazione (ad esempio può essere membro del gruppo di amministratori locale) su tutti i computer in cui si desidera gestire gli utenti connessi. Per assegnare le autorizzazioni, è necessario aggiungere l'account di accesso del gruppo di amministratori del dominio nativo al dominio del computer.

Gestione delle proprietà dei dispositivi

È possibile modificare le proprietà di un dispositivo su un computer specifico. La modifica delle proprietà del dispositivo per un dispositivo consente di modificare il tipo di avvio per un dispositivo.

Avvio di un dispositivo

È possibile avviare un dispositivo su un computer specifico nel dominio o nel sottoalbero gestito.

Arresto di un dispositivo

È possibile arrestare un dispositivo su un computer specifico nel dominio o nel sottoalbero gestito.

Gestione dei log degli eventi

Un evento è un'occorrenza importante del sistema o dell'applicazione. Il sistema operativo Windows registra le informazioni sugli eventi nel file di log degli eventi. Potrebbero essere presenti diversi log degli eventi memorizzati in ciascun computer. Utilizzare il Visualizzatore eventi di Windows nativo per visualizzare i log degli eventi. DRA gestisce i log degli eventi solo sui computer che si trovano in domini gestiti.

Registra inoltre le operazioni di iniziate dall'utente nell'archivio di log, il quale è un archivio sicuro. È possibile far sì che DRA oltre a registrare le informazioni nell'archivio dei log, registri anche le operazioni iniziate dall'utente nel registro eventi di Windows. Per ulteriori informazioni, vedere la sezione Informazioni su data e ora.

Tipi di log degli eventi

I computer che eseguono Microsoft Windows registrano ulteriori informazioni in log differenti. Di seguito viene fornita una breve descrizione dei log:

Tipo di log	Descrizione
ADAM	Registra gli eventi registrati dall'archivio ADAM.

Tipo di log	Descrizione
Applicazione	Registra gli eventi registrati da un'applicazione del computer, ad esempio un errore o un avvio di un servizio. Ad esempio, DRA archivia gli eventi nel log dell'applicazione.
Servizio directory	Registra gli eventi relativi ai controller del dominio gestendo il database della sicurezza.
Servizio di replica dei file	Registra gli eventi correlati ai servizi di replica dei file forniti dal sistema operativo.
Sicurezza	Registra gli eventi che includono tentativi di login, accesso a file e directory nonché modifiche delle policy di sicurezza basate sulle opzioni di policy di revisione.
Sistema	Registra gli eventi registrati dai componenti di sistema di Windows, ad esempio la mancata applicazione di un driver o l'avvio e l'arresto dei servizi.

Task di gestione del log degli eventi

Quando si installa DRA, di default, gli eventi di revisione non vengono registrati nel log degli eventi di Windows. È possibile abilitare questo tipo di registrazione, modificando la chiave del registro.

Avviso: Fare attenzione quando si modifica il Registro di Windows. Se si verifica un errore nel Registro di sistema, il computer potrebbe non funzionare più correttamente. Se si verifica un errore, è possibile ripristinare il Registro di sistema allo stato in cui si trovava all'ultimo avvio corretto del computer. Per ulteriori informazioni, vedere la Guida relativa all'editor del Registro di Windows.

È possibile specificare la dimensione massima di un file del log degli eventi e l'azione che deve essere eseguita quando il log è pieno. La finestra delle proprietà visualizza anche il nome del log, il percorso e il nome del file del log, quando il log è stato creato, nonché la data dell'ultima modifica e l'ultimo accesso. Se si sceglie di eseguire il backup del file di log, DRA consente di salvare il log degli eventi con un nome di file univoco in un'ubicazione standard del computer selezionato.

DRA consente di gestire i log degli eventi mentre si gestiscono altre risorse di tale computer. Con i poteri appropriati è possibile eseguire diversi task, ad esempio la modifica delle proprietà del log degli eventi.

Gestione delle proprietà dei log degli eventi

È possibile modificare le proprietà dei log degli eventi per un computer specifico.

Visualizzazione delle voci del log degli eventi

È possibile visualizzare le voci di un log degli eventi specifico per un computer nel dominio o nel sottoalbero gestito. Nella Console di delega e configurazione è possibile visualizzare il file di log degli eventi nel Visualizzatore eventi di Windows nativo.

Eliminazione del log degli eventi

È possibile eliminare le voci in un log degli eventi specifico per un computer che si trova in un dominio o in sottoalbero gestito. È inoltre possibile salvare le voci del log degli eventi prima di eliminare il log.

Gestione dei file aperti

Un file aperto è una connessione a risorse condivise, ad esempio file o pipe. Una pipe è un meccanismo di comunicazione tra processi che permette a un processo di comunicare con un altro processo locale o remoto.

DRA consente di gestire i file aperti solo su computer che si trovano nel dominio e nel sottoalbero gestito. Poiché i file aperti sono associati a un computer, è possibile gestire tali file mentre si gestiscono altre risorse per tale computer. Ad esempio, è possibile chiudere i file aperti quando si arresta un sistema o si installa un nuovo dispositivo o un servizio. È inoltre possibile monitorare i file a cui gli utenti eseguono più frequentemente l'accesso, consentendo di valutare meglio la sicurezza dei file.

Nota: È possibile gestire i file aperti solo tramite la Console di delega e configurazione.

Chiusura di un file

È possibile chiudere file aperti dalle risorse della rete. Se si intende chiudere i file aperti, si consiglia di informare gli utenti. Potrebbero aver bisogno di tempo per salvare i dati. Per chiudere un file aperto, è necessario poter accedere al computer corrispondente.

Aggiornamento dell'elenco di file aperti

Per essere certi di visualizzare informazioni aggiornate sulle sessioni aperte in un computer, è necessario aggiornare manualmente l'elenco degli utenti connessi. Per aggiornare l'elenco di file aperti, è necessario poter accedere al computer corrispondente.

8 Gestione del Cestino

Il Cestino fornisce una rete di sicurezza, consentendo di cancellare temporaneamente account utente, gruppi, contatti e account del computer. È possibile ripristinare tali oggetti intatti al loro stato originario con tutti i relativi dati, ad esempio SID, ACL (elenchi di controllo di accesso) e appartenenze ai gruppi o cancellarli definitivamente. Questa flessibilità fornisce un metodo più sicuro per gestire gli account utente, i gruppi, i contatti e gli account del computer. È possibile utilizzare l'opzione di ricerca per cercare gli oggetti richiesti. Per ulteriori informazioni, vedere *Ricerca degli oggetti*.

Ripristino di un oggetto dal Cestino

È possibile ripristinare gli oggetti cancellati nel container da cui sono stati cancellati. DRA ripristina questi oggetti al loro stato originario con tutti i dati intatti, ad esempio SID, ACL e appartenenze. Un oggetto può essere un account utente, un gruppo, un contatto, un gruppo dinamico, un casella postale risorsa, un gruppo di distribuzione dinamico o un account del computer.

Ripristino di tutti gli oggetti

È possibile ripristinare tutti gli oggetti dal Cestino di un dominio gestito. È possibile ripristinare gli oggetti dal Cestino per un dominio specifico o per tutti i domini gestiti. Per ripristinare gli oggetti dal Cestino per un dominio specifico, è necessario attivare il Cestino per tale dominio.

Cancellazione di un oggetto dal Cestino

È possibile cancellare definitivamente gli oggetti dal Cestino per un dominio gestito. Dopo aver cancellato un oggetto dal Cestino, non sarà più possibile ripristinarlo. Un oggetto può essere un account utente, un gruppo, un contatto, un gruppo dinamico, un casella postale risorsa, un gruppo di distribuzione dinamico o un account del computer.

Svuotamento del Cestino

È possibile svuotare il Cestino per un dominio gestito. Lo svuotamento del Cestino cancella definitivamente tutti gli oggetti attualmente presenti nel Cestino. È possibile svuotare il Cestino per un dominio specifico o per tutti i domini gestiti. Per svuotare un Cestino per un dominio specifico, è necessario abilitare il Cestino per tale dominio. Una volta svuotato il Cestino, non sarà più possibile ripristinare gli oggetti cancellati.