NetIQ Directory and Resource Administrator 10.2

Guida all'amministrazione

Maggio 2022

Note legali

Sommario

Informazioni su questa guida

La *Guida all'amministrazione* fornisce informazioni concettuali sul prodotto Directory and Resource Administrator (DRA), definisce la terminologia e illustra vari concetti correlati. Fornisce inoltre istruzioni dettagliate per l'esecuzione di molti task di configurazione e operativi.

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 DRA.

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/.

Introduzione

Prima di installare e configurare tutti i componenti di Directory and Resource Administrator™ (DRA) è necessario comprendere ciò che DRA è in grado di fare per l'azienda e il ruolo che svolgono i suoi componenti nell'architettura del prodotto.

1 Che cos'è Directory and Resource Administrator

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. Tutte queste funzionalità contribuiscono a proteggere gli ambienti AD ed Exchange dei clienti dal rischio di escalation dei privilegi, errori, attività dannose e non conformità alle norme, riducendo al contempo il carico di lavoro degli amministratori tramite funzionalità 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 Microsoft Active Directory, Windows, 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 e di Exchange 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.

2 Caratteristiche dei componenti di Directory and Resource Administrator

I componenti di DRA che si utilizzano regolarmente per gestire l'accesso con privilegi comprendono i server primario e secondario, le console di amministrazione, i componenti di generazione di rapporti e il motore di Workflow Automation per l'automazione dei 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	Configurazione di DRA Reporting Center (NRC) PowerShell *(facoltativo)* Interfaccia della riga di comando *(facoltativo)* Provider ADSI di DRA *(facoltativo)*	Qualsiasi server DRA
Amministratore occasionale dell'help desk	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.

Console di delega e configurazione

La Console di delega e configurazione è un'interfaccia utente installabile che fornisce agli amministratori di sistema l'accesso alle funzioni di configurazione e amministrazione di DRA.

- **Gestione della delega:** consente di specificare e assegnare in modo differenziato l'accesso a risorse gestite e task ad amministratori aggiunti.
- **Gestione di policy e automazione:** consente di definire e applicare policy per garantire la conformità a standard e convenzioni dell'ambiente.
- **Gestione della configurazione:** consente di aggiornare le impostazioni di sistema e le opzioni di DRA, aggiungere personalizzazioni e configurare servizi gestiti (Active Directory, Exchange, Azure Active Directory e così via).
- **Gestione account e risorse:** Consente agli amministratori aggiunti DRA di visualizzare e gestire gli oggetti delegati dei domini e dei servizi connessi dalla Console di delega e configurazione.

Console Web

La Console Web è un'interfaccia utente basata sul Web che fornisce un accesso rapido e semplice agli amministratori aggiunti, 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.

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:

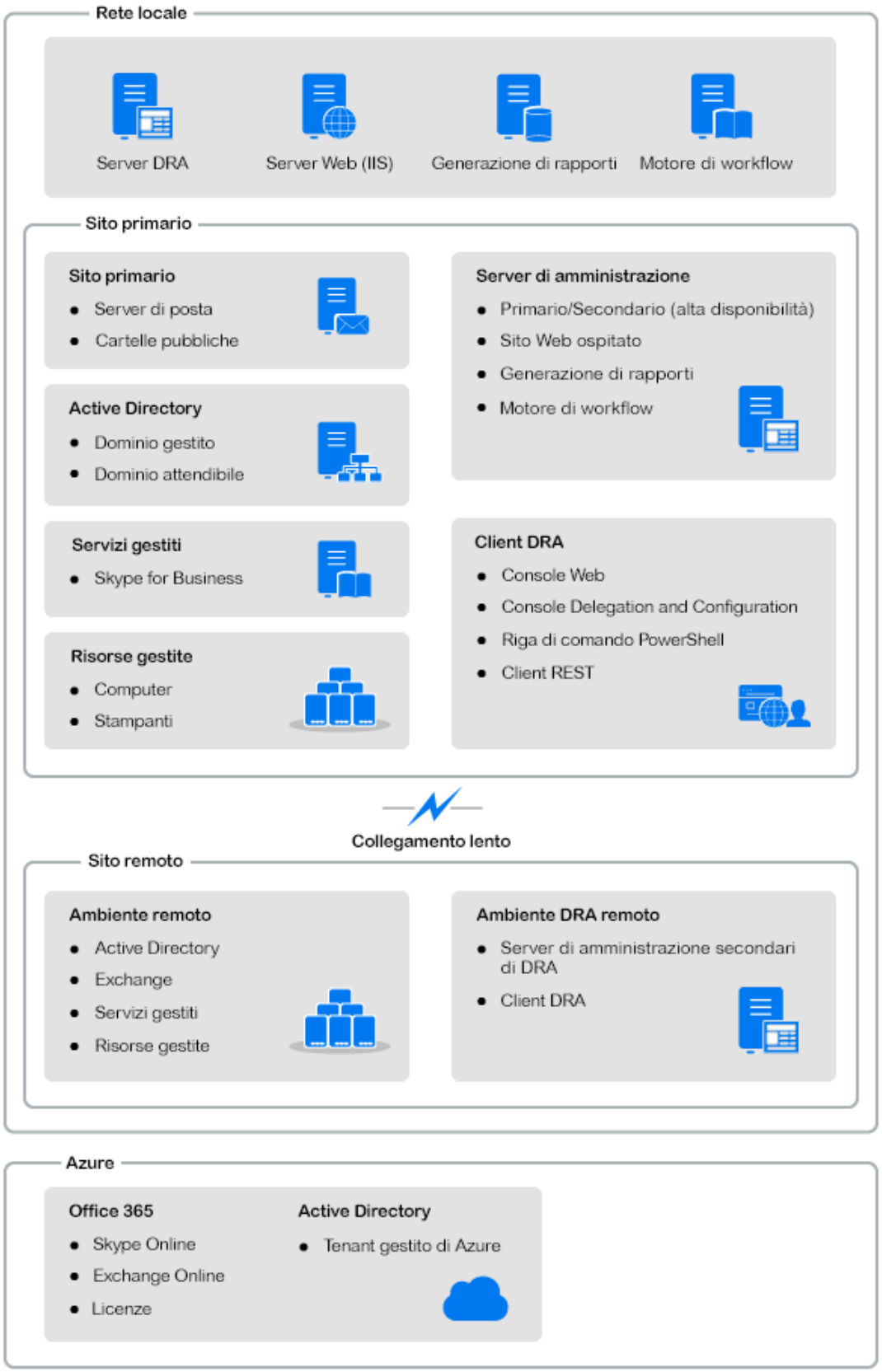
- Rapporti risorse per gli oggetti Active Directory
- Rapporti sui dati oggetto di Active Directory
- Rapporti di riepilogo di Active Directory
- Rapporti di configurazione di DRA
- Rapporti di configurazione di Exchange
- Rapporti di Exchange Online di Office 365
- Rapporti dettagliati sulle tendenze 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 Automation

DRA si integra con il motore di Workflow Automation 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 Automation, vedere il sito della documentazione di DRA.

Architettura del prodotto



II Installazione e upgrade del prodotto

In questo capitolo vengono illustrati i requisiti hardware, software e di account consigliati per Directory and Resource Administrator. Vengono quindi fornite istruzioni dettagliate per l'installazione tramite un elenco di controllo per l'installazione di ciascun componente.

3 Pianificazione dell'installazione

Per pianificare l'installazione di Directory and Resource Administrator, utilizzare questa sezione per valutare la compatibilità dell'ambiente hardware e software e prendere nota delle porte e i protocolli necessari che dovranno essere configurati per l'installazione.

Suggerimenti relativi a risorse provate

In questa sezione si forniscono informazioni sulle dimensioni delle risorse di base consigliate. I risultati potrebbero variare a seconda dell'hardware disponibile, dell'ambiente in uso, del tipo specifico di dati elaborati e di altri fattori. È possibile che esistano configurazioni hardware più grandi e potenti, capaci di gestire un carico superiore. Per eventuali domande, rivolgersi a Servizi NetIQ Consulting.

Esecuzione in un ambiente con circa un milione di oggetti Active Directory:

Componente	CPU	Memoria	Spazio
Server di amministrazione DRA	8 CPU/core 2.0 GHz	16 GB	120 GB
Console Web di DRA	2 CPU/core 2.0 GHz	8 GB	100 GB
DRA Reporting	4 CPU/core 2.0 GHz	16 GB	100 GB
Server di workflow DRA	4 CPU/core 2.0 GHz	16 GB	120 GB

Provisioning delle risorse per gli ambienti virtuali

DRA mantiene attivi segmenti di memoria di grandi dimensioni per lunghi periodo di tempo. Quando si esegue il provisioning delle risorse per un ambiente virtuale, considerare i suggerimenti seguenti:

- Allocare lo spazio come "Thick Provisioned"
- Impostare la memoria su Reserve All Guest Memory (All Locked)
- Verificare che il file di paginazione sia di dimensioni sufficienti per l'eventuale riallocazione del ballooning della memoria a livello virtuale

Porte e protocolli necessari

In questa sezione sono indicati i protocolli e le porte per la comunicazione di DRA.

- Le porte configurabili sono indicate con un asterisco (*)
- Le porte che necessitano di un certificato sono indicate con due asterischi (**)

Tabelle dei componenti:

- "Server di amministrazione DRA" a pagina 24
- "Server REST di DRA" a pagina 26
- "Console Web (IIS)" a pagina 26
- "Console di delega e amministrazione di DRA" a pagina 26
- "Server di workflow" a pagina 27

Server di amministrazione DRA

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 135	Bidirezionale	Server di amministrazione DRA	Mapper di endpoint, ovvero un requisito di base per la comunicazione di DRA. Consente ai server di amministrazione d'individuarsi reciprocamente in un MMS
TCP 445	Bidirezionale	Server di amministrazione DRA	Replica del modello di delega; replica dei file durante la sincronizzazione di un MMS (SMB)
Intervallo di porte TCP dinamiche*	Bidirezionale	Controller di dominio Microsoft Active Directory	Per default, DRA assegna dinamicamente le porte nell'intervallo di porte TCP da 1024 a 65535. Tuttavia, è possibile configurare l'intervallo utilizzando Servizi componenti. Per ulteriori informazioni, vedere *Using Distributed COM with Firewalls* (Utilizzo di Distributed COM con firewall).
TCP 50000 *	Bidirezionale	Server di amministrazione DRA	Replica dell'attributo e comunicazione server DRA-AD LDS. (LDAP)
TCP 50001 *	Bidirezionale	Server di amministrazione DRA	Replica dell'attributo SSL (AD LDS)
TCP/UDP 389	In uscita	Controller di dominio Microsoft Active Directory	Gestione degli oggetti Active Directory (LDAP)
	In uscita	Microsoft Exchange Server	Gestione delle caselle postali (LDAP)
TCP/UDP 53	In uscita	Controller di dominio Microsoft Active Directory	Risoluzione dei nomi

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP/UDP 88	In uscita	Controller di dominio Microsoft Active Directory	Consente l'autenticazione dal server DRA ai controller di dominio (Kerberos)
TCP 80	In uscita	Microsoft Exchange Server	Necessaria per tutte le installazioni locali di Exchange Server 2013 e versioni successive (HTTP)
	In uscita	Microsoft Office 365	Accesso remoto a PowerShell (HTTP)
TCP 443	In uscita	Microsoft Office 365, Change Guardian	Accesso ad API Graph e integrazione con Change Guardian (HTTPS)
TCP 443, 5986, 5985	In uscita	Microsoft PowerShell	Cmdlet PowerShell nativi (HTTPS) e comunicazione remota di PowerShell
TCP 5984	Localhost	Server di amministrazione DRA	Accesso di IIS al Servizio Replica per fornire supporto alle assegnazioni temporanee al gruppo
TCP 8092 * **	In uscita	Server di workflow	Stato e attivazione dei workflow (HTTPS)
TCP 50101 *	In entrata	Client DRA	Fare clic con il pulsante destro del mouse su Cronologia delle modifiche per il rapporto di revisione delle interfacce utente. Configurabili durante l'installazione.
TCP 8989	Localhost	Servizio di archivio log	Comunicazione con l'archivio log (non è necessaria l'apertura tramite il firewall)
TCP 50102	Bidirezionale	Servizio DRA Core	Servizio di archivio log
TCP 50103	Localhost	Servizio DB cache di DRA	Comunicazione con il servizio cache nel server DRA (non è necessaria l'apertura tramite il firewall)
TCP 1433	In uscita	Microsoft SQL Server	Raccolta dati per la generazione di rapporti
UDP 1434	In uscita	Microsoft SQL Server	Il servizio browser di SQL Server utilizza questa porta per identificare la porta per l'istanza con nome.
TCP 8443	Bidirezionale	Server Change Guardian	Cronologia modifiche unificata
TCP 8898	Bidirezionale	Server di amministrazione DRA	Comunicazione del Servizio Replica di DRA tra server DRA per le assegnazioni temporanee al gruppo
TCP 636	In uscita	Controller di dominio Microsoft Active Directory	Gestione degli oggetti Active Directory (SSL LDAP).

Server REST di DRA

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 8755 * **	In entrata	Server IIS, cmdlet PowerShell di DRA	Esecuzione delle attività di workflow basate su REST di DRA (ActivityBroker)
TCP 135	In uscita	Controller di dominio Microsoft Active Directory	Rilevamento automatico mediante punto di connessione del servizio (SCP)
TCP 443	In uscita	Controller di dominio Microsoft AD	Rilevamento automatico mediante punto di connessione del servizio (SCP)

Console Web (IIS)

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 8755 * **	In uscita	Servizio REST di DRA	Per la comunicazione tra la console Web di DRA e PowerShell di DRA
TCP 443	In entrata	Browser client	Apertura di un sito Web DRA
TCP 443 **	In uscita	Server di Advanced Authentication	Advanced Authentication

Console di delega e amministrazione di DRA

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 135	In uscita	Controller di dominio Microsoft Active Directory	Rilevamento automatico mediante SCP
Intervallo di porte TCP dinamiche*	In uscita	Server di amministrazione DRA	Attività di workflow dell'adattatore di DRA. Per default, DCOM assegna dinamicamente le porte nell'intervallo di porte TCP da 1024 a 65535. Tuttavia, è possibile configurare l'intervallo utilizzando Servizi componenti. Per ulteriori informazioni, vedere *Using Distributed COM with Firewalls* (Utilizzo di Distributed COM con firewall) (DCOM)
TCP 50102	In uscita	Servizio DRA Core	Generazione di rapporti sulla cronologia delle modifiche

Server di workflow

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 8755	In uscita	Server di amministrazione DRA	Esecuzione delle attività di workflow basate su REST di DRA (ActivityBroker)
Intervallo di porte TCP dinamiche*	In uscita	Server di amministrazione DRA	Attività di workflow dell'adattatore di DRA. Per default, DCOM assegna dinamicamente le porte nell'intervallo di porte TCP da 1024 a 65535. Tuttavia, è possibile configurare l'intervallo utilizzando Servizi componenti. Per ulteriori informazioni, vedere *Using Distributed COM with Firewalls* (Utilizzo di Distributed COM con firewall) (DCOM)
TCP 1433	In uscita	Microsoft SQL Server	Archiviazione dei dati di workflow
TCP 8091	In entrata	Operations Console (Console delle operazioni) e Configuration Console (Console di configurazione)	Workflow API BSL (TCP)
TCP 8092 **	In entrata	Server di amministrazione DRA	Workflow API BSL (HTTP) e (HTTPS)
TCP 2219	Localhost	Provider dello spazio dei nomi	Utilizzati dal provider dello spazio dei nomi per eseguire gli adattatori
TCP 9900	Localhost	Motore di correlazione	Utilizzati dal Motore di correlazione per comunicare con il motore di Workflow Automation e il Provider dello spazio dei nomi
TCP 10117	Localhost	Provider dello spazio dei nomi per la gestione delle risorse	Utilizzati dal provider dello spazio dei nomi per la gestione delle risorse

Piattaforme supportate

Per informazioni aggiornate sulle piattaforme software supportate, vedere la pagina del prodotto Directory and Resource Administrator.

Sistema gestito	Prerequisiti
Azure Active Directory	Per abilitare l'amministrazione di Azure, è necessario installare i seguenti moduli PowerShell: ◆ Azure Active Directory V2 (AzureAD) versione 2.0.2.4 o successiva ◆ AzureRM.Profile versione 5.8.2 o successiva ◆ PowerShell per Exchange Online V2.0.3 o versione successiva Per installare i nuovi moduli Azure PowerShell è richiesto PowerShell 5.1 o il modulo più recente.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Server 2022 ◆ Azure Active Directory
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online O365
Skype for Business	◆ Microsoft Skype for Business 2015
Cronologia modifiche	◆ Change Guardian 6.0 o versione successiva
Database	◆ Microsoft SQL Server 2016
Browser Web	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019 ◆ Microsoft Server 2022

Requisiti del server di amministrazione DRA e della console Web

I componenti DRA richiedono i seguenti software e account:

- “Requisiti software” a pagina 29
- “Dominio server” a pagina 30
- “Requisiti degli account” a pagina 30
- “Account di accesso DRA con minimo privilegio” a pagina 32

Requisiti software

Componente	Prerequisiti
Destinazione di installazione	**Sistema operativo del server di amministrazione NetIQ:**
Sistema operativo	◆ Microsoft Windows Server 2012 R2, 2016, 2019, 2022 **Nota:** il server deve anche essere un membro di un dominio Active Directory locale di Microsoft supportato. **Interfacce DRA:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019, 2022 ◆ Microsoft Windows 10, 11
Programma di installazione	◆ Microsoft .NET Framework 4.8 e versioni successive
Server di amministrazione	**Directory and Resource Administrator:** ◆ Microsoft .NET Framework 4.8 e versioni successive ◆ Pacchetti Microsoft Visual C++ 2015-2019 Redistributable (x64 e x86) ◆ Accodamento messaggi Microsoft ◆ Ruoli di Microsoft Active Directory Lightweight Directory Services ◆ Servizio Registro di sistema remoto avviato ◆ Microsoft Internet Information Services ◆ URL Rewrite Module for IIS ◆ Estensione Application Request Routing di Microsoft Internet Information Services **Nota:** NetIQ DRA REST Service viene installato con il server di amministrazione. **Amministrazione di Microsoft Office 365/Exchange Online:** ◆ Modulo di Windows Azure Active Directory per Windows PowerShell ◆ Modulo Windows PowerShell ◆ PowerShell per Exchange Online V2.0.3 o versione successiva ◆ Abilitare WinRM per l'autenticazione di base sul lato client per i task di Exchange Online. Per ulteriori informazioni, vedere Piattaforme supportate.
Interfaccia utente	**Interfacce DRA:** ◆ Microsoft .NET Framework 4.8 ◆ Pacchetti Microsoft Visual C++ 2015-2019 Redistributable (x64 e x86)
Estensioni PowerShell	◆ Microsoft .NET Framework 4.8 ◆ PowerShell 5.1 o versione successiva

Componente	Prerequisiti
Console Web di DRA	**Server Web:** ◆ Microsoft .Net Framework 4.x > Servizi WCF > Attivazione HTTP ◆ Microsoft Internet Information Server 8.5, 10 ◆ URL Rewrite Module for IIS ◆ Estensione Application Request Routing di Microsoft Internet Information Services **Componenti del server Web (IIS):** ◆ Server Web > Protezione > Autorizzazione URL

Dominio server

Componente	Sistemi operativi
Server DRA	◆ Microsoft Windows Server 2022 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

Requisiti degli account

Account	Descrizione	Autorizzazioni
Gruppo AD LDS	Per accedere ad AD LDS è necessario aggiungere a questo gruppo l'account del servizio DRA	◆ Gruppo di sicurezza locale di dominio

Account	Descrizione	Autorizzazioni

Account del servizio DRA	Autorizzazioni necessarie per eseguire il servizio di amministrazione NetIQ	◆ Per autorizzazioni "Distributed COM Users"
		◆ Membro del gruppo Amministratori di AD LDS
		◆ Gruppo operatore di account
		◆ Gruppi log archivio (OnePointOp ConfgAdms e OnePointOp)
		◆ Nella scheda Account è necessario selezionare una delle seguenti **opzioni Account** per l'utente account del servizio DRA se si installa DRA su un server mediante la metodologia STIG:
		  ◆ Kerberos AES 128 bits encryption (Cifratura Kerberos AES a 128 bit)
		  ◆ Kerberos AES 256 bits encryption (Cifratura Kerberos AES a 256 bit)
		Nota
		◆ Per ulteriori informazioni sulla configurazione di account con accesso al dominio con privilegi minimi, vedere Account di accesso DRA con minimo privilegio.
		◆ Per ulteriori informazioni sulla configurazione di un account del servizio gestito del gruppo per DRA, vedere "Configurazione dei servizi DRA per un account del servizio gestito del gruppo" nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Amministratore di DRA	Account utente o gruppo di cui viene eseguito il provisioning nel ruolo integrato degli amministratori di DRA	◆ Gruppo di sicurezza locale di dominio o account utente di dominio ◆ Membro del dominio gestito o di un dominio attendibile ◆ Se si specifica un account da un dominio attendibile, accertarsi che il computer del server di amministrazione possa autenticare tale account.

Account	Descrizione	Autorizzazioni
Account amministratori aggiunti di DRA	Account a cui vengono delegati poteri attraverso DRA	◆ Aggiungere tutti gli account amministratore aggiunto di DRA al gruppo "Distributed COM Users" affinché possano eseguire la connessione al server DRA da client remoti. È necessario solo se si utilizza un thick client o la Console di delega e configurazione. **Nota:** DRA può essere configurato affinché durante l'installazione gestisca questa configurazione.

Account di accesso DRA con minimo privilegio

Di seguito sono indicati privilegi e autorizzazioni necessari per gli account specificati e i comandi di configurazione che è necessario eseguire.

Account di accesso ai domini: l'uso di ADSI Edit concede all'account di accesso al dominio le seguenti autorizzazioni di Active Directory a livello più alto del dominio per i seguenti tipi di oggetto discendenti:

- Controllo COMPLETO sugli oggetti builtInDomain
- Controllo COMPLETO sugli oggetti Computer
- Controllo COMPLETO degli oggetti Punto di connessione
- Controllo COMPLETO sugli oggetti Contatto
- Controllo COMPLETO sugli oggetti Container
- Controllo COMPLETO sugli oggetti Gruppo
- Controllo COMPLETO sugli oggetti InetOrgPerson
- Controllo COMPLETO sugli oggetti MsExchDynamicDistributionList
- Controllo COMPLETO sugli oggetti MsExchSystemObjectsContainer
- Controllo COMPLETO sugli oggetti msDS-GroupManagedServiceAccount
- Controllo COMPLETO sugli oggetti Unità organizzativa
- Controllo COMPLETO sugli oggetti Stampante
- Controllo COMPLETO sugli oggetti publicFolder
- Controllo COMPLETO sugli oggetti Cartella condivisa
- Controllo COMPLETO sugli oggetti Utente

Nota: Se lo schema Active Directory del dominio gestito non è esteso per Exchange Online, i seguenti oggetti non verranno elencati:

- Oggetti MsExchDynamicDistributionList
- Oggetti MsExchSystemObjectsContainer
- Oggetti publicFolder

Concedere all'account di accesso al dominio le seguenti autorizzazioni di Active Directory a livello più alto del dominio a questo oggetto e a tutti gli oggetti discendenti:

- Allow create Computer objects (Consenti di creare oggetti Computer)
- Allow create Contact objects (Consenti di creare oggetti Contatto)
- Allow create Container objects (Consenti di creare oggetti Container)
- Allow create Group objects (Consenti di creare oggetti Gruppo)
- Allow create MsExchDynamicDistributionList objects (Consenti di creare oggetti MsExchDynamicDistributionList)
- Allow create msDS-GroupManagedServiceAccount objects (Consenti di creare oggetti msDS-GroupManagedServiceAccount)
- Allow create Organizational Unit objects (Consenti di creare oggetti Unità organizzativa)
- Allow create publicFolders objects (Consenti di creare oggetti publicFolders)
- Allow create Shared Folder objects (Consenti di creare oggetti Cartella condivisa)
- Allow create User objects (Consenti di creare oggetti Utente)
- Allow create Printer objects (Consenti di creare oggetti Stampante)
- Allow delete Computer objects (Consenti di eliminare oggetti Computer)
- Allow delete Contact objects (Consenti di eliminare oggetti Contatto)
- Allow delete Container (Consenti di eliminare oggetti Container)
- Allow delete Group objects (Consenti di eliminare oggetti Gruppo)
- Allow delete InetOrgPerson objects (Consenti di eliminare oggetti InetOrgPerson)
- Allow delete MsExchDynamicDistributionList objects (Consenti di eliminare oggetti MsExchDynamicDistributionList)
- Allow delete msDS-GroupManagedServiceAccount objects (Consenti di eliminare oggetti msDS-GroupManagedServiceAccount)
- Allow delete Organizational Unit objects (Consenti di eliminare oggetti Unità organizzativa)
- Allow delete publicFolders objects (Consenti di eliminare oggetti publicFolders)
- Allow delete Shared Folder objects (Consenti di eliminare oggetti Cartella condivisa)
- Allow delete User objects (Consenti di eliminare oggetti Utente)
- Allow delete Printer objects (Consenti di eliminare oggetti Stampante)

Nota

- Di default, alcuni oggetti Container integrati in Active Directory non ereditano le autorizzazioni dal livello più alto del dominio. Per questo motivo, per tali oggetti sarà necessario abilitare l'ereditarietà oppure impostare autorizzazioni esplicite.
- Se si utilizza l'account con meno privilegi come account di accesso, assicurarsi che a tale account in Active Directory sia assegnata l'autorizzazione "Reset Password" (Reimpostazione password), affinché la reimpostazione della password venga eseguita correttamente in DRA.

Account di accesso a Exchange: per gestire gli oggetti dell'installazione locale di Microsoft Exchange, assegnare il ruolo di gestione organizzativa all'account di accesso a Exchange e l'account di accesso a Exchange al gruppo Account Operators.

Account di accesso a Skype: verificare che l'account sia un utente abilitato a Skype e che sia un membro di almeno uno dei seguenti ruoli:

- Ruolo CSAdministrator
- Ruoli CSUserAdministrator e CSArchiving

Account di accesso alle cartelle pubbliche: assegnare le seguenti autorizzazioni di Active Directory all'account di accesso alle cartelle pubbliche:

- Gestione cartelle pubbliche
- Cartelle pubbliche abilitate per la posta

Tenant di Azure: L'autenticazione di base richiede le autorizzazioni di Azure Active Directory sia per l'account di accesso tenant di Azure che per l'applicazione Azure. L'autenticazione basata su certificato richiede le autorizzazioni di Azure Active Directory per l'applicazione Azure. Di default, DRA crea automaticamente un certificato autofirmato richiesto per l'autenticazione.

Applicazione Azure: l'applicazione Azure richiede i ruoli e le autorizzazioni seguenti:

Ruoli:

- Amministratore utente
- Amministratore di Exchange

Autorizzazioni:

- Lettura e scrittura dei profili completi di tutti gli utenti
- Lettura e scrittura di tutti i gruppi
- Lettura dei dati della directory
- Gestione di Exchange Online come applicazione per l'accesso alle risorse di Exchange Online
- Lettura e scrittura di tutte le applicazioni
- Amministratore destinatari di Exchange

Account di accesso tenant di Azure: l'account di accesso tenant di Azure richiede le autorizzazioni seguenti:

- Gruppi di distribuzione
- Destinatari di posta
- Creazione destinatari di posta
- Creazione e appartenenza a gruppi di sicurezza
- (Facoltativo) Amministratore Skype for Business

  Per gestire Skype for Business Online, assegnare il potere Amministratore Skype for Business all'account di accesso tenant di Azure.
- Amministratore utente
- Amministratore dell'autenticazione con privilegi

Autorizzazioni account di NetIQ Administration Service (Servizio di amministrazione NetIQ):

- Amministratori locali

- Concedere all'account prioritario di minimo privilegio le "Autorizzazioni complete" sulle cartelle condivise o DFS in cui viene eseguito il provisioning delle directory Home.
- **Gestione delle risorse**: per gestire le risorse pubblicate all'interno di un dominio Active Directory gestito, è necessario concedere le autorizzazioni di amministrazione locale per tali risorse all'account con accesso al dominio.

Dopo l'installazione di DRA: Prima di gestire i domini richiesti è necessario eseguire i seguenti comandi:

- Per delegare l'autorizzazione al container "Oggetti eliminati" dalla cartella di installazione di DRA (si noti che il comando deve essere eseguito da un amministratore di dominio):

  `DraDelObjsUtil.exe /domain:<NomeDominioNetbios> /delegate:<Nome account>`
- Per delegare l'autorizzazione a "NetIQReceyleBin OU" dalla cartella di installazione di DRA:

  `DraRecycleBinUtil.exe /domain:<NomeDominioNetbios> / delegate:<NomeAccount>`

Accesso remoto a SAM: Assegnare i controller di dominio o i server membri gestiti da DRA per abilitare gli account elencati nell'impostazione GPO (Group Policy Object, Oggetto Criteri di Gruppo) seguente, in modo da poter effettuare query remote sul database SAM (Security Account Manager). La configurazione deve includere l'account del servizio DRA.

Accesso alla rete: limita i client a cui è consentito effettuare chiamate remote a SAM

Per accedere a questa impostazione, effettuare le seguenti operazioni:

1. Aprire la console Gestione Criteri di gruppo sul controller di dominio.
2. Espandere **Domains** (Domini) > **[controller di dominio]** > **Group Policy Objects** (Oggetti Criteri di gruppo) nell'albero dei nodi.
3. Fare clic con il pulsante destro del mouse su **Default Domain Controllers Policy** (Criterio controller di dominio predefiniti) e selezionare **Edit** (Modifica) per aprire l'editor GPO per questa policy.
4. Espandere **Computer Configuration** (Configurazione computer) > **Policies** (Criteri) > **Windows Settings** (Impostazioni di Windows) > **Security Settings** (Impostazioni di sicurezza) > **Local Policies** (Criteri locali) nell'albero dei nodi dell'editor GPO.
5. Fare doppio clic su **Network access: Restrict clients allowed to make remote calls to SAM** (Accesso alla rete: limita i client a cui è consentito effettuare chiamate remote a SAM) nel riquadro dei criteri, quindi selezionare **Define this policy setting** (Definisci le impostazioni relative al criterio).
6. Fare clic su **Edit Security** (Modifica protezione) e abilitare **Allow** (Consenti) per Remote Access (Accesso remoto). Se non è già stato incluso, aggiungere l'account del servizio DRA come utente o membro del gruppo di amministratori.
7. Applicare le modifiche. In tal modo verrà aggiunto il descrittore di sicurezza `O:BAG:BAD:(A;;RC;;;BA)` alle impostazioni della policy.

Per ulteriori informazioni, vedere l'articolo 7023292 della knowledgebase.

Requisiti per la generazione di rapporti

Di seguito sono riportati i requisiti per DRA Reporting.

Requisiti software

Componente	Prerequisiti
Destinazione di installazione	**Sistema operativo:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019, 2022
NetIQ Reporting Center (ver. 3.3)	**Database:** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ L'amministratore di dominio che gestisce i lavori dell'agente SQL richiede le autorizzazioni di sicurezza per SQL Server Integration Services di Microsoft, altrimenti è possibile che alcuni rapporti NRC non vengano elaborati. **Server Web:** ◆ Microsoft Internet Information Server 8.5, 10 ◆ Componenti di Microsoft IIS: ◆◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Necessario per l'esecuzione del programma di installazione NRC ◆ Necessario anche sul server primario DRA per la configurazione di DRA Reporting **Nota:** Quando si installa NetIQ Reporting Center (NRC) in un computer con SQL Server, potrebbe essere necessario eseguire l'installazione manuale di .NET Framework 3.5 prima di installare NRC. **Protocollo di sicurezza della comunicazione:** ◆ SQL Server deve supportare TLS 1.2. Per ulteriori informazioni, vedere Supporto di TLS 1.2 per Microsoft SQL Server. ◆ SQL Server deve disporre in un driver supportato da TLS aggiornato e installato sul server DRA. Il driver suggerito è l'ultima versione di Microsoft® SQL Server® 2012 Native Client - QFE ◆ I sistemi operativi sia del server SQL Server che del server di amministrazione DRA devono supportare la stessa versione del protocollo TLS. Ad esempio, è stato abilitato solo TLS 1.2.
DRA Reporting	**Database:** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Requisiti relativi alle licenze

La licenza determina quali prodotti e funzionalità è possibile utilizzare. Per DRA è necessario installare una chiave di licenza insieme al server di amministrazione.

Una volta installato il server di amministrazione, è possibile utilizzare l'utility Health Check per installare la licenza acquistata. Nel pacchetto di installazione è inoltre inclusa una chiave di licenza di valutazione (TrialLicense.lic) che consente di gestire un numero illimitato di account utente e di caselle postali per 30 giorni. Per ulteriori informazioni sulle licenze di DRA, vedere Installazione e upgrade delle licenze.

Per ulteriori informazioni sulla definizione della licenza e le restrizioni, fare riferimento al contratto di licenza con l'utente finale (EULA) del prodotto.

4 Installazione del prodotto

In questo capitolo vengono fornite istruzioni dettagliate per l'installazione di Directory and Resource Administrator. Per ulteriori informazioni sulla pianificazione dell'installazione o dell'upgrade, vedere Pianificazione dell'installazione.

Installazione del server di amministrazione DRA

È possibile installare il server di amministrazione DRA nell'ambiente in uso come nodo primario o secondario. I requisiti per i server di amministrazione primario e secondario sono i medesimi, ma in tutte le installazioni di DRA deve essere presente un server di amministrazione primario.

Il pacchetto server DRA dispone delle seguenti caratteristiche:

- **Server di amministrazione:** memorizza i dati di configurazione (ambiente, accesso delegato e policy), consente di eseguire i task relativi a operatori e automazione ed esegue la revisione delle attività del sistema. Dispone delle seguenti funzionalità:
  - **Resource Kit di archivio log:** consente di visualizzare le informazioni di revisione.
  - **SDK DRA:** fornisce gli script di esempio ADSI e fornisce supporto alla creazione di script personalizzati.
  - **Assegnazioni temporanee al gruppo:** Fornisce i componenti per abilitare la sincronizzazione delle Assegnazioni temporanee al gruppo.
- **Interfacce utente:** interfaccia Web client utilizzata principalmente dagli amministratori aggiunti e che include anche opzioni di personalizzazione.
  - **Provider ADSI:** consente di creare script delle policy personalizzate.
  - **Interfaccia della riga di comando:** consente di eseguire le operazioni DRA.
  - **Delega e configurazione:** consente agli amministratori di sistema di accedere alle funzioni di configurazione e amministrazione DRA. Consente inoltre di specificare e assegnare in modo differenziato l'accesso a risorse gestite e task ad amministratori aggiunti.
  - **Estensioni PowerShell:** forniscono un modulo PowerShell che consente ai client non DRA di richiedere operazioni DRA mediante cmdlet PowerShell.
  - **Console Web:** interfaccia Web client utilizzata principalmente dagli amministratori aggiunti e che include anche opzioni di personalizzazione.

Per informazioni sull'installazione di console DRA specifiche e di client da riga di comando su più computer, vedere Installazione dei client DRA.

Elenco di controllo per l'installazione interattiva:

Passaggio	Dettagli
Accesso al server di destinazione	Accedere al server di destinazione Microsoft Windows per eseguire l'installazione con un account che disponga di privilegi di amministratore locale.
Copia ed esecuzione di Admin Installation Kit	Eseguire il kit di installazione di DRA (NetIQAdminInstallationKit.msi) per estrarre il supporto di installazione di DRA nel file system locale. **Nota:** il kit di installazione installerà .NET Framework nel server di destinazione, se necessario.
Installazione di DRA	Fare clic su **Install DRA** (Installa DRA) e su **Next** (Avanti) per visualizzare le opzioni di installazione. **Nota:** per eseguire il programma di installazione in un secondo momento, spostarsi nell'ubicazione in cui è stato estratto il supporto di installazione (vedere il kit di installazione) ed eseguire `Setup.exe`.
Installazione di default	Scegliere i componenti da installare e accettare l'ubicazione di installazione di default `C:\Program Files (x86)\NetIQ\DRA` o specificare un'ubicazione alternativa per l'installazione. Opzioni dei componenti: **Server di amministrazione** ◆ Resource Kit di archivio log (Facoltativo) ◆ SDK DRA ◆ Assegnazioni temporanee al gruppo **Interfacce utente** ◆ Provider ADSI (Facoltativo) ◆ Interfaccia della riga di comando (facoltativa) ◆ Delega e configurazione ◆ Estensioni PowerShell ◆ Console Web
Verifica dei prerequisiti	Nella finestra di dialogo **Prerequisites List** (Elenco dei prerequisiti) verrà visualizzato l'elenco del software necessario in base ai componenti selezionati per l'installazione. Il programma di installazione guida l'utente nell'installazione di eventuali prerequisiti mancanti che sono necessari per eseguire correttamente l'installazione.
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale.
Selezione dell'ubicazione dei log	Specificare un'ubicazione in cui DRA deve memorizzare tutti i file di log. **Nota:** i log della Console di delega e configurazione e i log ADSI sono memorizzati nella cartella del profilo utente.

Passaggio	Dettagli
Selezione della modalità operativa dei server	Selezionare **Primary Administration Server** (Server di amministrazione primario) per installare il primo server di amministrazione DRA di un set multimaster (nell'installazione vi sarà un solo primario) o **Secondary Administration Server** (Server di amministrazione secondario) per unire un nuovo server di amministrazione DRA a un set multimaster esistente. Per informazioni sul set multimaster, vedere “Configurazione del set multimaster” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).
Immissione degli account e delle credenziali di installazione	◆ Account del servizio DRA ◆ Gruppo AD LDS ◆ Amministratore di DRA Account Per ulteriori informazioni, vedere Requisiti del server di amministrazione DRA e della console Web.
Configurazione delle autorizzazioni DCOM	Abilitare DRA per configurare l'accesso “Distributed COM” agli utenti autenticati.
Configurazione delle porte	Per ulteriori informazioni sulle porte di default, vedere Porte e protocolli necessari.
Immissione dell'ubicazione di archiviazione	Specificare l'ubicazione del file locale che DRA utilizza per archiviare i dati di revisione e cache.
Immissione dell'ubicazione del database di replica DRA	◆ Specificare l'ubicazione del file per il database di replica DRA e la porta del servizio di replica. ◆ Specificare il certificato SSL che si desidera utilizzare per le comunicazioni sicure con il database mediante IIS e la porta di replica IIS. **Nota:** Nel campo **IIS Replication Web Site SSL Certificate** (Certificato SSL del sito Web di replica IIS) sono elencati i certificati provenienti sia dall'archivio WebHosting (Hosting Web) che dall'archivio Personal (Personale).
Immissione del certificato SSL del servizio REST	Selezionare il certificato SSL che verrà utilizzato per il servizio REST e specificare la porta del servizio REST. **Nota:** Nel campo **REST Service SSL Certificate** (Certificato SSL del servizio REST) sono elencati i certificati provenienti sia dall'archivio WebHosting (Hosting Web) che dall'archivio Personal (Personale).
Immissione del certificato SSL della Console Web	Specificare il certificato SSL che verrà utilizzato per il binding HTTPS.
Verifica della configurazione di installazione	È possibile verificare la configurazione nella pagina di riepilogo dell'installazione prima di fare clic su **Installa** e procedere con l'installazione.
Verifica post-installazione	Una volta completata l'installazione, viene eseguita l'utility Health Checker per verificare l'installazione e aggiornare la licenza del prodotto. Per ulteriori informazioni, vedere "Utility Health Check" nella *DRA Administrator Guide* (Guida all'amministrazione DRA).

Installazione dei client DRA

È possibile installare console e client da riga di comando specifici di DRA eseguendo DRAInstaller.msi con il pacchetto .mst corrispondente nella destinazione di installazione:

NetIQDRACLI.mst	Consente di installare l'interfaccia della riga di comando
NetIQDRAADSI.mst	Consente di installare il provider ADSI di DRA
NetIQDRAClients.mst	Consente di installare tutte le interfacce utente di DRA

Per installare client DRA specifici in più computer all'interno dell'azienda, configurare un oggetto Criteri di gruppo per installare il pacchetto .MST specifico.

1. Avviare Utenti e computer di Active Directory e creare un oggetto Criteri di gruppo.
2. Aggiungere il pacchetto DRAInstaller.msi all'oggetto Criteri di gruppo.
3. Verificare che l'oggetto Criteri di gruppo abbia una delle seguenti proprietà:
   - Ciascun account utente del gruppo dispone delle autorizzazioni Power User per il computer appropriato.
   - Abilitare l'impostazione dei criteri Installa sempre con privilegi elevati.
4. Aggiungere il file .mst dell'interfaccia utente all'oggetto Criteri di gruppo.
5. Distribuire i criteri di gruppo.

Nota: per ulteriori informazioni sui criteri di gruppo, vedere la Guida di Microsoft Windows. Per provare e installare facilmente e in modo sicuro i criteri di gruppo in tutta l'azienda, utilizzare *Amministratore Criteri di gruppo*.

Installazione di Workflow Automation e configurazione delle impostazioni

Per gestire le richieste di Workflow Automation in DRA, è necessario eseguire le seguenti operazioni:

- Installare e configurare Workflow Automation e l'adattatore DRA.

  Per informazioni, vedere la *Guida all'amministrazione di Workflow Automation* workflow) e il *Workflow Automation Adapter Reference for DRA* (Riferimento per l'adattatore di Workflow Automation per DRA).
- Configurare l'integrazione di Workflow Automation con DRA.

  Per informazioni, vedere “Configurazione del server di Workflow Automation” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).
- Delegare i poteri di Workflow Automation in DRA.

  Per informazioni, vedere “Delega dei poteri di configurazione del server di Workflow Automation” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

I documenti indicati in precedenza sono disponibili nel sito della documentazione di DRA.

Installazione di DRA Reporting

DRA Reporting richiede l'installazione del file DRAReportingSetup.exe dal kit di installazione di NetIQ DRA.

Passaggi	Dettagli
Accesso al server di destinazione	Accedere al server di destinazione Microsoft Windows per eseguire l'installazione con un account che disponga di privilegi di amministratore locale. Verificare che l'account disponga di privilegi di amministratore locale e di dominio, come anche di privilegi di amministratore di sistema in SQL Server.
Copia ed esecuzione di NetIQ Admin Installation Kit	Copiare il kit di installazione di DRA NetIQAdminINstallationKit.msi nel server di destinazione ed eseguirlo facendo doppio clic sul file o richiamandolo dalla riga di comando. Il kit di installazione estrarrà il supporto di installazione di DRA nel file system locale in un'ubicazione personalizzabile. Inoltre, il kit di installazione installerà .NET Framework nel server di destinazione, se è necessario per soddisfare i prerequisiti del programma di installazione di DRA.
Esecuzione dell'installazione di DRA Reporting	Passare all'ubicazione in cui è stato estratto il supporto d'installazione ed eseguire DRA`ReportingSetup.exe` per installare il componente di gestione per l'integrazione con DRA Reporting.
Verifica e installazione dei prerequisiti	Nella finestra di dialogo **Prerequisites** (Prerequisiti) verrà visualizzato l'elenco del software necessario in base ai componenti selezionati per l'installazione. Il programma di installazione guida l'utente nell'installazione di eventuali prerequisiti mancanti che sono necessari per eseguire correttamente l'installazione. Per informazioni su NetIQ Reporting Center, vedere la *Reporting Center Guide* (Guida di Reporting Center) sul sito Web della documentazione.
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale per completare la procedura di installazione.

5 Upgrade del prodotto

In questo capitolo viene descritta una procedura utile per eseguire in fasi controllate l'upgrade o la migrazione di un ambiente distribuito.

Si presuppone che l'ambiente includa più server di amministrazione, alcuni dei quali ubicati in siti remoti. Questa configurazione è denominata set multimaster (MMS). Un MMS è costituito da un server di amministrazione primario e uno o più server di amministrazione secondari associati. Per ulteriori informazioni sul funzionamento di un MMS, vedere “Configurazione del set multimaster” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Pianificazione dell'upgrade di DRA

Eseguire `NetIQAdminInstallationKit.msi` per estrarre il supporto di installazione di DRA, quindi installare ed eseguire l'utility Health Check.

Prima di iniziare la procedura di upgrade, verificare di aver pianificato l'installazione di DRA. Per la pianificazione dell'installazione, considerare le linee guida seguenti:

- Provare la procedura di upgrade in un ambiente lab prima di eseguire l'upgrade nell'ambiente di produzione. Questa prova consente d'individuare e risolvere eventuali problemi imprevisti senza ripercussioni sulle responsabilità quotidiane di amministrazione.
- Riesaminare la sezione Porte e protocolli necessari.
- Stabilire quanti amministratori aggiunti utilizzeranno ciascun MMS. Se la maggior parte degli amministratori aggiunti utilizza server o set di server specifici, eseguire prima l'upgrade di tali server nelle ore non di punta.
- Determinare quali amministratori aggiunti necessitano della Console di delega e configurazione. È possibile ottenere queste informazioni in uno dei modi seguenti:
  - Verificare quali amministratori aggiunti sono associati ai gruppi di amministratori aggiunti integrati.
  - Verificare quali amministratori aggiunti sono associati alle viste ActiveView integrate.
  - Utilizzare Directory and Resource Administrator Reporting per generare rapporti sul modello di sicurezza, come ad esempio i rapporti ActiveView Assistant Admin Details (Dettagli amministratori aggiunti) e Assistant Admin Groups (Gruppi amministratori aggiunti).

  Notificare a tali amministratori aggiunti i piani di upgrade per le interfacce utente.

- Stabilire quali amministratori aggiunti necessitano di eseguire la connessione al server di amministrazione primario. Tali amministratori aggiunti devono eseguire l'upgrade dei loro computer client una volta completato l'upgrade del server di amministrazione primario.

  Notificare a questi amministratori aggiunti i piani di upgrade dei server di amministrazione e delle interfacce utente.
- Stabilire se è necessario implementare modifiche di delega, configurazione o policy prima di iniziare la procedura di upgrade. A seconda dell'ambiente, questa decisione potrebbe variare da sito a sito.
- Coordinare l'upgrade dei computer client e dei server di amministrazione in modo da ridurre al minimo i tempi di fermo. Tenere presente che DRA non supporta l'esecuzione di versioni precedenti insieme alla versione attuale di DRA nello stesso server di amministrazione o computer client.

Task da eseguire prima dell'upgrade

Prima di iniziare le installazioni di upgrade, seguire i passaggi preliminari riportati di seguito per preparare ciascun server per l'upgrade.

Passaggi	Dettagli
Backup dell'istanza di AD LDS	Aprire l'Utility Health Check ed eseguire il controllo **AD LDS Instance Backup** (Backup istanza AD LDS) per creare una copia di backup dell'istanza attuale.
Definizione di un piano di installazione	Creare un piano di installazione per eseguire l'upgrade dei server di amministrazione e delle interfacce utente (computer client degli amministratori aggiunti). Per ulteriori informazioni, vedere Pianificazione dell'upgrade di DRA.
Riserva di un server secondario per l'esecuzione di una versione precedente di DRA	*Facoltativo:* riservare un server di amministrazione secondario per l'esecuzione di una versione precedente di DRA mentre si esegue l'upgrade di un sito.
Esecuzione delle modifiche necessarie per l'MMS	Apportare le modifiche necessarie alle impostazioni di delega, configurazione o policy per l'MMS. Per modificare tali impostazioni, utilizzare il server di amministrazione primario.
Sincronizzazione dell'MMS	Sincronizzare i set di server in modo che le impostazioni di configurazione e sicurezza di ogni server di amministrazione siano aggiornate.
Backup del registro del server primario	Eseguire il backup del registro dal server di amministrazione primario. Una copia di backup delle impostazioni precedenti del registro consente di ripristinare facilmente la configurazione e le impostazioni di sicurezza precedenti..
Convertire gli account gMSA in account utente DRA	*Facoltativo:* se si utilizza un account del servizio gestito del gruppo (gMSA, group Managed Service Account) per l'account del servizio DRA, modificare l'account gMSA in un account utente DRA prima di eseguire l'upgrade. Dopo l'upgrade è necessario modificare l'account nuovamente in gMSA.

Nota: Se è necessario ripristinare l'istanza di AD LDS, effettuare le operazioni seguenti:

1. Interrompere l'istanza attuale di AD LDS in Gestione computer > Servizi. Il titolo sarà: `NetIQDRASecureStoragexxxxx`.
2. Sostituire il file `adamnts.dit` **attuale** con il file `adamnts.dit` di **backup** come indicato di seguito:
   - Ubicazione del file attuale: `%ProgramData%/NetIQ/DRA/<NomeIstanzaDRA>/data/`
   - Ubicazione del file di backup: `%ProgramData%/NetIQ/ADLDS/`
3. Riavviare l'istanza di AD LDS.

Argomenti preliminari all'upgrade:

- "Server di amministrazione locale per l'esecuzione di una versione precedente di DRA" a pagina 47
- "Sincronizzazione del set di server di una versione precedente di DRA" a pagina 48
- "Backup del registro del server di amministrazione" a pagina 49

Server di amministrazione locale per l'esecuzione di una versione precedente di DRA

Per ridurre al minimo i tempi di fermo e le costose connessioni a siti remoti, è possibile riservare presso un sito uno o più server di amministrazione secondari che eseguano una versione precedente di DRA durante l'upgrade. Questo passaggio è facoltativo e consente agli amministratori aggiunti di utilizzare una versione precedente di DRA durante tutta la procedura di upgrade, fino al corretto completamento dell'installazione.

Valutare questa opzione in caso di una o più delle esigenze di upgrade seguenti:

- Tempi di fermo minimi o nulli.
- Necessità di supportare un numero elevato di amministratori aggiunti e impossibilità di eseguire immediatamente l'upgrade di tutti i computer client.
- Necessità di continuare a supportare l'accesso a una versione precedente di DRA dopo l'upgrade del server di amministrazione primario.
- Presenza nell'ambiente di un MMS che si estende in più siti.

È possibile installare un nuovo server di amministrazione secondario o designare un server secondario esistente che esegua una versione precedente di DRA. Se si intende eseguire l'upgrade di tale server, esso deve essere l'ultimo della procedura. In caso contrario, disinstallare completamente DRA dal server dopo aver completato l'upgrade.

Installazione di un nuovo server secondario

L'installazione di un nuovo server di amministrazione secondario in un sito locale consente di evitare costose connessioni a siti remoti e permette agli amministratori aggiunti di continuare a utilizzare una versione precedente di DRA senza interruzioni. Se nell'ambiente è presente un MMS che si estende in più siti, è opportuno prendere in considerazione questa opzione. Ad esempio, se l'MMS in uso è costituito da un server di amministrazione primario presso il sito di Londra e un server di

amministrazione secondario presso il sito di Tokyo, si consideri di installare un server secondario presso il sito di Londra e di aggiungerlo all'MMS corrispondente. Questo server aggiuntivo consente agli amministratori aggiunti del sito di Londra di utilizzare una versione precedente di DRA fino al completamento dell'upgrade.

Utilizzo di un server secondario esistente

È possibile utilizzare un server di amministrazione secondario esistente come server riservato a una versione precedente di DRA. Se si prevede di non eseguire l'upgrade di un server di amministrazione secondario in un sito specifico, è opportuno prendere in considerazione questa opzione. Se non è possibile riservare un server secondario esistente, valutare se installare un nuovo server di amministrazione per questo scopo. Riservare uno o più server secondari per l'esecuzione di una versione precedente di DRA consente agli amministratori aggiunti di continuare a utilizzare una versione precedente di DRA senza interruzioni fino al completamento dell'upgrade. Questa opzione assicura i risultati migliori in ambienti di grandi dimensioni che utilizzano un modello di amministrazione centralizzato.

Sincronizzazione del set di server di una versione precedente di DRA

Prima di eseguire il backup del registro della versione precedente di DRA o iniziare la procedura di upgrade, assicurarsi di sincronizzare i set di server in modo che le impostazioni di configurazione e sicurezza di ciascun server di amministrazione siano aggiornate.

Nota: accertarsi di aver apportato tutte le modifiche necessarie alle impostazioni di delega, configurazione o policy per l'MMS. Per modificare tali impostazioni, utilizzare il server di amministrazione primario. Una volta eseguito l'upgrade del server di amministrazione primario, non è possibile sincronizzare le impostazioni di delega, configurazione o policy in alcun server di amministrazione che esegue una versione precedente di DRA.

Per sincronizzare il set di server esistente:

1. Eseguire l'accesso al server di amministrazione primario con l'account predefinito Administrator.
2. Aprire la Console di delega e configurazione ed espandere **Configuration Management** (Gestione configurazione).
3. Fare clic su **Server di amministrazione**.
4. Nel riquadro destro, selezionare il server di amministrazione primario appropriato per questo set di server.
5. Fare clic su **Proprietà**.
6. Nella scheda Pianificazione della sincronizzazione, fare clic su **Aggiorna ora**.
7. Verificare che la sincronizzazione sia stata eseguita e che tutti i server di amministrazione secondari siano disponibili.

Backup del registro del server di amministrazione

Eseguendo il backup del registro del server di amministrazione è possibile tornare alle configurazioni precedenti. Ad esempio, se è necessario disinstallare completamente la versione attuale di DRA e utilizzare la versione precedente, con una copia di backup delle impostazioni precedenti del registro è possibile recuperare facilmente le impostazioni di configurazione e sicurezza.

Tuttavia, prestare attenzione quando si apportano modifiche al registro. In caso di errore nel registro, il server di amministrazione potrebbe non funzionare come previsto. Se si verifica un errore durante la procedura di upgrade, è possibile utilizzare la copia di backup delle impostazioni del registro per eseguire il ripristino. Per ulteriori informazioni, vedere la *Guida dell'Editor del Registro di sistema*.

Importante: quando si esegue il ripristino del registro, la versione del server DRA, il nome del sistema operativo Windows e la configurazione dei domini gestiti deve essere esattamente la stessa.

Importante: prima dell'upgrade, eseguire il backup del sistema operativo Windows del computer in cui risiede DRA o creare un'immagine snapshot del computer come macchina virtuale.

Per eseguire il backup del registro del server di amministrazione:

1. Eseguire `regedit.exe`.
2. Fare clic con il pulsante destro del mouse sul nodo `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` e selezionare **Esporta**.
3. Specificare il nome e l'ubicazione del file per salvare la chiave di registro e fare clic su **Salva**.

Upgrade del server di amministrazione DRA

L'elenco di controllo seguente funge da guida per tutta la procedura di upgrade. Per eseguire l'upgrade di ciascun set di server dell'ambiente, utilizzare questa procedura. Se l'operazione non è ancora stata eseguita, creare una copia di backup dell'istanza attuale di AD LDS mediante l'utility Health Check.

Avviso: eseguire l'upgrade dei server di amministrazione secondari solo dopo aver eseguito l'upgrade del server di amministrazione primario del relativo MMS.

È possibile suddividere la procedura in svariate fasi, eseguendo l'upgrade di un MMS alla volta. Tale procedura di upgrade consente anche di includere temporaneamente server secondari che eseguono una versione precedente di DRA e server secondari che eseguono la versione attuale di DRA nel medesimo MMS. DRA supporta la sincronizzazione tra server di amministrazione che eseguono una versione precedente e server che eseguono la versione attuale di DRA. Tuttavia, tenere presente che DRA non supporta l'esecuzione di versioni precedenti insieme alla versione attuale di DRA nello stesso server di amministrazione o computer client.

Importante: Per la corretta replica delle assegnazioni temporanee al gruppo nel server secondario, eseguire manualmente la **Pianificazione della sincronizzazione multimaster** o attendere l'esecuzione pianificata.

Passaggi	Dettagli
Esecuzione dell'utility Health Check	Installare l'utility Health Check di DRA autonomo ed eseguirla utilizzando un account del servizio. Risolvere eventuali problemi.
Esecuzione di un upgrade di prova	Eseguire un upgrade di prova nell'ambiente lab per individuare potenziali problemi e ridurre al minimo i tempi di fermo della produzione.
Definizione dell'ordine di upgrade	Stabilire l'ordine in cui si desidera eseguire l'upgrade dei set di server.
Preparazione degli MMS per l'upgrade	Preparare ciascun MMS per l'upgrade. Per ulteriori informazioni, vedere Task da eseguire prima dell'upgrade.
Esecuzione dell'upgrade del server primario	Eseguire l'upgrade del server di amministrazione primario nell'MMS appropriato. Per ulteriori informazioni, vedere Upgrade del server di amministrazione primario.
Installazione di un nuovo server secondario	*(Facoltativo)* Per ridurre al minimo i tempi di fermo presso i siti remoti, installare un server di amministrazione secondario locale che esegua la versione più recente di DRA. Per ulteriori informazioni, vedere Installazione di un server di amministrazione secondario locale per la versione corrente di DRA.
Installazione delle interfacce utente	Installare le interfacce utente per gli amministratori aggiunti. Per ulteriori informazioni, vedere Installazione delle interfacce utente di DRA
Upgrade dei server secondari	Eseguire l'upgrade dei server di amministrazione secondari nell'MMS. Per ulteriori informazioni, vedere Upgrade dei server di amministrazione secondari.
Upgrade di DRA Reporting	Eseguire l'upgrade di DRA Reporting. Per ulteriori informazioni, vedere Upgrade della generazione di rapporti.
Esecuzione dell'utility Health Check	Eseguire l'utility Health Check installata durante l'upgrade. Risolvere eventuali problemi.
Aggiungere i tenant di Azure *(dopo l'upgrade)*	*(Facoltativo, dopo l'upgrade)* Se precedentemente all'upgrade venivano gestiti tenant di Azure, durante l'upgrade essi vengono rimossi. Sarà necessario aggiungere nuovamente i tenant ed eseguire un aggiornamento della cache degli account completo dalla Console di delega e configurazione. Per ulteriori informazioni, vedere "Configurazione dei tenant di Azure" nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).
Aggiornamento della configurazione della console Web *(dopo l'upgrade)*	*(Condizionale, dopo l'upgrade)* Se prima dell'upgrade si dispone di una delle configurazioni della console Web riportate di seguito, sarà necessario aggiornarle al termine dell'installazione dell'upgrade: ◆ Connessioni server di default abilitate ◆ File di configurazione modificati Per ulteriori informazioni, vedere Aggiornamento della configurazione della console Web - Dopo l'installazione.

Argomenti dell'upgrade del server:

Upgrade del server di amministrazione primario

Dopo aver correttamente preparato l'MMS, eseguire l'upgrade del server di amministrazione primario. Eseguire l'upgrade delle interfacce utente nei computer client solo dopo aver completato l'upgrade del server di amministrazione primario. Per ulteriori informazioni, vedere Installazione delle interfacce utente di DRA.

Nota: per ulteriori considerazioni e istruzioni sull'upgrade, vedere le *Directory and Resource Administrator Release Notes* (Note di rilascio di Directory and Resource Administrator).

Prima di eseguire l'upgrade, notificare agli amministratori aggiunti quando si prevede di avviare la procedura. Se è stato riservato un server di amministrazione secondario per l'esecuzione di una versione precedente di DRA, indicare inoltre tale server affinché gli amministratori aggiunti possano continuare a utilizzare la versione precedente di DRA durante l'upgrade.

Nota: una volta eseguito l'upgrade del server di amministrazione primario, non è possibile sincronizzare le impostazioni di delega, configurazione o policy da tale server ai server di amministrazione secondari che eseguono una versione precedente di DRA.

Installazione di un server di amministrazione secondario locale per la versione corrente di DRA

L'installazione di un nuovo server di amministrazione secondario per eseguire la versione attuale di DRA presso un sito locale può essere utile per ridurre al minimo le costose connessioni a siti remoti, diminuendo al contempo i tempi di fermo complessivi e consentendo un'installazione più rapida delle interfacce utente. Questo passaggio è facoltativo e permette agli amministratori aggiunti di utilizzare sia la versione attuale che quella precedente di DRA durante tutta la procedura di upgrade, fino al corretto completamento dell'installazione.

Valutare questa opzione in caso di una o più delle esigenze di upgrade seguenti:

- Tempi di fermo minimi o nulli.
- Necessità di supportare un numero elevato di amministratori aggiunti e impossibilità di eseguire immediatamente l'upgrade di tutti i computer client.
- Necessità di continuare a supportare l'accesso a una versione precedente di DRA dopo l'upgrade del server di amministrazione primario.
- Presenza nell'ambiente di un MMS che si estende in più siti.

Ad esempio, se l'MMS in uso è costituito da un server di amministrazione primario presso il sito di Londra e un server di amministrazione secondario presso il sito di Tokyo, si consideri di installare un server secondario presso il sito di Tokyo e di aggiungerlo all'MMS corrispondente. Questo server aggiuntivo esegue un miglior bilanciamento del carico amministrativo quotidiano presso il sito di Tokyo e consente agli amministratori aggiunti di entrambi i siti di utilizzare una versione precedente di DRA come anche la versione attuale fino al completamento dell'upgrade. Inoltre si eviteranno tempi morti per gli amministratori aggiunti, poiché è possibile installare immediatamente le interfacce utente della versione attuale di DRA. Per ulteriori informazioni sull'upgrade delle interfacce utente, vedere Installazione delle interfacce utente di DRA.

Installazione delle interfacce utente di DRA

In genere, le interfacce utente della versione attuale di DRA si installano dopo aver eseguito l'upgrade del server di amministrazione primario e di un server di amministrazione secondario. Tuttavia, per gli amministratori aggiunti che devono utilizzare il server di amministrazione primario, verificare di avere precedentemente eseguito l'upgrade dei rispettivi computer client installando la Console di delega e configurazione. Per ulteriori informazioni, vedere Pianificazione dell'upgrade di DRA.

Se si eseguono spesso elaborazioni batch tramite l'interfaccia della riga di comando, il provider ADSI, PowerShell o se si generano frequentemente rapporti, valutare l'installazione di tali interfacce utente in un server di amministrazione secondario dedicato per mantenere un bilanciamento del carico appropriato nell'MMS.

È possibile consentire agli amministratori aggiunti di installare le interfacce utente di DRA oppure installarle tramite criteri di gruppo. È inoltre possibile installare facilmente e rapidamente la Console Web per più amministratori aggiunti.

Nota: l'esecuzione side-by-side di più versioni di componenti di DRA nello stesso server DRA non è consentita. Se si prevede di eseguire gradualmente l'upgrade dei computer client degli amministratori aggiunti, valutare l'installazione della Console Web per consentire l'accesso immediato a un server di amministrazione che esegue la versione attuale di DRA.

Upgrade dei server di amministrazione secondari

Quando si esegue l'upgrade dei server di amministrazione secondari, è possibile procedere secondo necessità, in base alle esigenze di amministrazione. Considerare inoltre come si prevede di eseguire l'upgrade e l'installazione delle interfacce utente di DRA. Per ulteriori informazioni, vedere Installazione delle interfacce utente di DRA.

Ad esempio, un percorso di upgrade tipico può includere i passaggi seguenti:

1. Upgrade di un server di amministrazione secondario.
2. Comunicare agli amministratori aggiunti che utilizzano questo server di installare le interfacce utente appropriate, ad esempio la Console Web.
3. Ripetizione dei passaggi 1 e 2 fino a completare l'upgrade dell'MMS.

Prima di eseguire l'upgrade, notificare agli amministratori aggiunti quando si prevede di avviare la procedura. Se è stato riservato un server di amministrazione secondario per l'esecuzione di una versione precedente di DRA, indicare inoltre tale server affinché gli amministratori aggiunti possano

continuare a utilizzare la versione precedente di DRA durante l'upgrade. Al termine della procedura di upgrade dell'MMS e quando tutti i computer client degli amministratori aggiunti eseguono interfacce utente di cui è stato eseguito l'upgrade, mettere offline eventuali altri server che eseguono versioni precedenti di DRA.

Aggiornamento della configurazione della console Web - Dopo l'installazione

Eseguire una o entrambe le azioni riportate di seguito, dopo l'installazione dell'upgrade, se applicabili all'ambiente DRA:

Connessione al server DRA di default

Il componente Servizio REST di DRA viene consolidato con il server DRA a partire da DRA 10.1. Se è stata configurata la connessione al server DRA di default prima dell'upgrade da una versione DRA 10.0.x o precedente, è necessario rivedere tali impostazioni dopo l'upgrade poiché ora è disponibile una sola configurazione di connessione, la Connessione server DRA. È possibile accedere a questa configurazione nella console Web in **Amministrazione** > **Configurazione** > **Connessione server DRA**.

È inoltre possibile aggiornare queste impostazioni dopo l'upgrade nel file `web.config` in `C:\inetpub\wwwroot\DRAClient\rest` sul server della console Web di DRA, come indicato di seguito:

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Configurazione del login alla console Web

Quando si esegue l'upgrade da DRA 10.0.x o versioni precedenti, se il servizio REST di DRA è installato senza il server DRA, la disinstallazione del servizio REST di DRA è un prerequisito per l'upgrade. Viene creata una copia dei file modificati prima dell'upgrade in `C:\ProgramData\NetIQ\DRA\Backup\` sul server. È possibile utilizzare questi file come riferimento per aggiornare quelli pertinenti dopo l'upgrade.

Upgrade di Workflow Automation

Per eseguire un upgrade sul posto su ambienti non cluster a 64 bit, è sufficiente eseguire il programma di installazione di Workflow Automation sui computer di Workflow Automation esistenti. Non è necessario arrestare i servizi di Workflow Automation in esecuzione.

Tutti gli adattatori di Workflow Automation non incorporati nel programma di installazione di Workflow Automation devono essere disinstallati e reinstallati dopo l'upgrade.

Per informazioni più dettagliate sull'upgrade di Workflow Automation, vedere “Upgrade da una versione precedente” nella *Workflow Automation Administrator Guide* (Guida all'amministrazione di Workflow Automation).

Upgrade della generazione di rapporti

Prima di eseguire l'upgrade di DRA Reporting, accertarsi che l'ambiente soddisfi i requisiti minimi di NRC 3.3. Per ulteriori informazioni sui requisiti di installazione e considerazioni sull'upgrade, vedere la *NetIQ Reporting Center Reporting Guide* (Guida alla generazione di rapporti di NetIQ Reporting Center).

Passaggi	Dettagli
Disabilitazione del supporto per DRA Reporting	Affinché i servizi di raccolta per la generazione di rapporti non vengano eseguiti durante la procedura di upgrade, disabilitare il supporto per DRA Reporting nella finestra Reporting Service Configuration (Configurazione del servizio di generazione rapporti) nella Console di delega e configurazione.
Esecuzione dell'accesso al server dell'istanza SQL con credenziali applicabili	Accedere con un account amministratore al server Microsoft Windows in cui è installata l'istanza di SQL per i database di generazione dei rapporti. Verificare che l'account disponga di privilegi di amministratore locale come anche di privilegi di amministratore di sistema in SQL Server.
Esecuzione del programma di installazione di DRA Reporting	Eseguire DRA`ReportingSetup.exe`. dal kit di installazione e seguire le istruzioni della procedura guidata di installazione.
Abilitazione del supporto per DRA Reporting	Nel server di amministrazione primario, abilitare la generazione di rapporti nella Console di delega e configurazione.

Se nell'ambiente si utilizza l'integrazione SSRS, sarà necessario ripetere l'installazione dei rapporti. Per ulteriori informazioni sulla reinstallazione dei rapporti, vedere la *Reporting Center Guide* (Guida di Reporting Center) sul sito Web della documentazione.

III Modello di delega

Grazie a DRA gli amministratori possono implementare uno schema di autorizzazioni di "minimo privilegio" basato su un set di controlli flessibile, per concedere in modo differenziato i poteri sugli oggetti gestiti dell'azienda. Queste deleghe consentono agli amministratori di avere la certezza che le autorizzazioni concesse agli amministratori aggiunti sono quelle strettamente necessarie per svolgere i loro ruoli e adempiere alle loro responsabilità specifiche.

6 Caratteristiche del modello di delega dinamico

Con DRA è possibile gestire l'accesso amministrativo all'azienda nell'ambito di un modello di delega. Il modello di delega consente di configurare l'accesso di "minimo privilegio" per gli amministratori aggiunti attraverso un set di controlli dinamico che può essere adattato ai cambiamenti e alle evoluzioni aziendali. Mediante il modello di delega è possibile ottenere il controllo dell'accesso amministrativo che meglio risponde alle modalità operative dell'azienda:

- Grazie a regole con ambiti flessibili, gli amministratori possono definire autorizzazioni mirate per oggetti gestiti specifici in funzione delle esigenze anziché della struttura aziendale.
- La delega basata sui ruoli assicura che le autorizzazioni vengano concesse in modo coerente e semplifica il provisioning.
- È possibile amministrare l'assegnazione dei privilegi su domini, tenant cloud e applicazioni gestite da un'unica ubicazione.
- I poteri differenziati permettono di adattare l'accesso specifico concesso agli amministratori aggiunti.

Controlli del modello di delega

Per il provisioning dell'accesso mediante il modello di delega, gli amministratori possono utilizzare i controlli seguenti:

- **Delega:** il provisioning dell'accesso a utenti e gruppi viene eseguito dagli amministratori assegnando un ruolo, che dispone di autorizzazioni specifiche nel contesto di una vista ActiveView che determina l'ambito.
- **Viste ActiveView:** una vista ActiveView rappresenta un ambito specifico di oggetti gestiti che sono definiti da una o più regole. Gli oggetti gestiti identificati da ciascuna regola in una vista ActiveView sono raggruppati in un ambito unificato.
- **Regola ActiveView:** le regole sono definite mediante espressioni che corrispondono a un set di oggetti gestiti in base a varie condizioni, quali tipo di oggetto, ubicazione, nome e così via.
- **Ruoli:** un ruolo è un set specifico di poteri (autorizzazioni) necessario per eseguire una funzione amministrativa specifica. In DRA sono disponibili alcuni ruoli integrati per le comuni funzioni aziendali ed è possibile definire ruoli personalizzati che soddisfino al meglio le esigenze dell'organizzazione.
- **Poteri:** un potere definisce un'autorizzazione specifica per i task supportati dall'oggetto gestito, vale a dire visualizzazione, modifica, creazione, eliminazione e così via. Le autorizzazioni relative alla modifica di un oggetto gestito possono essere ulteriormente suddivise in base alle proprietà specifiche che possono essere modificate. In DRA è disponibile un'ampia gamma di poteri integrati per gli oggetti gestiti supportati ed è possibile definire poteri personalizzati per estendere il provisioning che è possibile fornire mediante il modello di delega.

Elaborazione delle richieste in DRA

Quando il server di amministrazione riceve una richiesta relativa a un'azione, come la modifica di una password utente, utilizza il processo seguente:

1. Vengono cercate le viste Activeview configurate per gestire l'oggetto di destinazione dell'operazione.
2. Viene eseguita la convalida dei poteri assegnati all'account che richiede l'azione.
    a. Vengono valutate tutte le assegnazioni alla vista ActiveView che contiene l'amministratore aggiunto che richiede l'operazione.
    b. Una volta stilato l'elenco, viene creato un altro elenco di tutte le viste ActiveView che contengono sia l'oggetto di destinazione sia l'amministratore aggiunto.
    c. Vengono poi confrontati i poteri con quelli necessari per eseguire l'operazione richiesta.
3. *Se l'account dispone del potere appropriato*, il server di amministrazione consente l'esecuzione dell'azione.

    Se invece i poteri dell'account non sono appropriati, il server di amministrazione restituisce un errore.
4. Active Directory viene aggiornato.

Esempi di elaborazione delle assegnazioni di delega in DRA

Gli esempi seguenti descrivono gli scenari più comuni che si verificano nella valutazione del modello di delega quando viene elaborata una richiesta:

Esempio 1: modifica della password di un utente

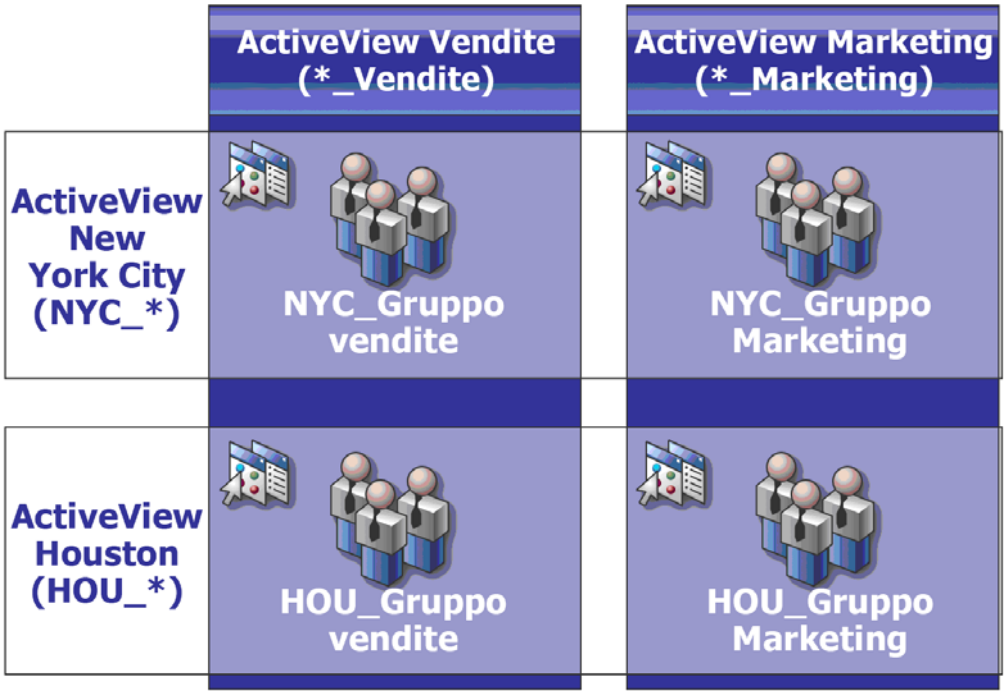
Quando un amministratore aggiunto tenta di impostare una nuova password per l'account utente MRossi, il server di amministrazione cerca tutte le viste ActiveView che includono MRossi. Più precisamente vengono cercate tutte le eventuali viste ActiveView in cui MRossi è specificato in modo diretto, tramite una regola con caratteri jolly o attraverso l'appartenenza a un gruppo. Se una vista ActiveView include altre viste ActiveView, il server di amministrazione esegue la ricerca anche in tali viste aggiuntive. Il server di amministrazione determina quindi se l'amministratore aggiunto dispone del potere *Reset User Account Password* (Reimposta password account utente) in una o più di tali viste ActiveView. Se l'amministratore aggiunto dispone del potere *Reset User Account Password* (Reimposta password account utente), il server di amministrazione reimposta la password di MRossi. Se invece non dispone di tale potere, il server di amministrazione rifiuta la richiesta.

Esempio 2: viste ActiveView sovrapposte

Un potere definisce le proprietà di un oggetto che un amministratore aggiunto può visualizzare, modificare o creare nel dominio o sottoalbero gestito. Lo stesso oggetto può far parte di più viste ActiveView. Questa configurazione è detta **viste ActiveView sovrapposte**.

Quando le viste ActiveView si sovrappongono, è possibile che sugli stessi oggetti si accumulino poteri diversi. Ad esempio, se una vista ActiveView consente di aggiungere un account utente a un dominio e un'altra vista ActiveView consente di eliminare un account utente dal medesimo dominio, sarà possibile aggiungere o eliminare gli account utente in tale dominio. Di conseguenza, i poteri di cui si dispone su un determinato oggetto sono cumulativi.

È importante comprendere in quale modo le viste ActiveView possono sovrapporsi e come sia possibile disporre di poteri maggiori su oggetti inclusi in nelle ActiveView. Si consideri la configurazione di ActiveView illustrata nella figura seguente.



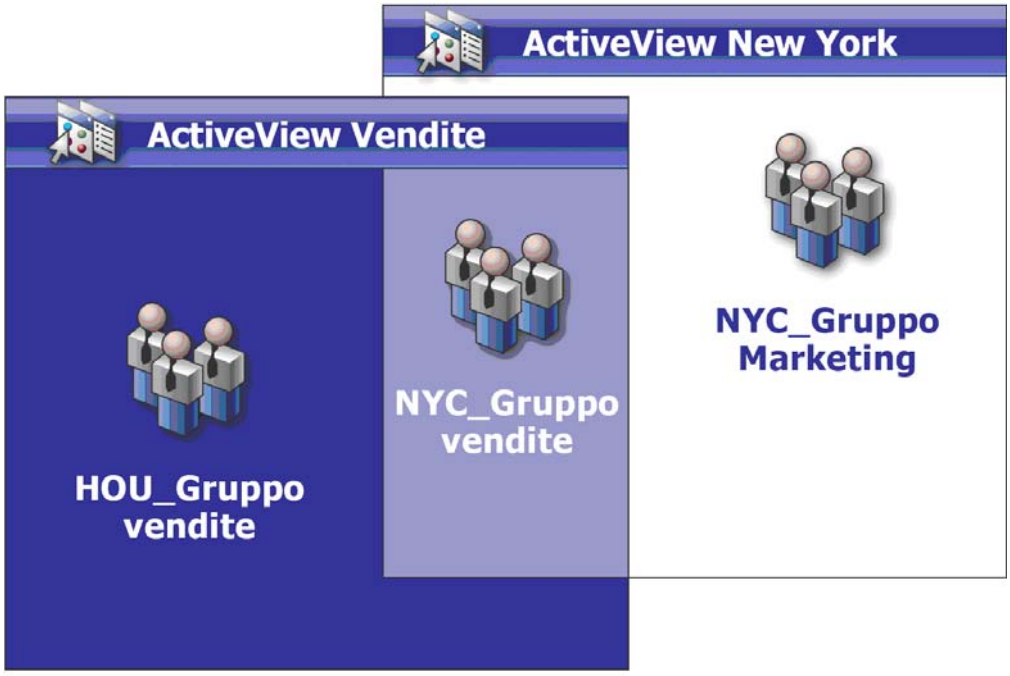
Le schede bianche identificano le viste ActiveView per ubicazione, cioè *New York City* e *Houston*. Le schede nere identificano le viste ActiveView per funzione organizzativa, ovvero *Vendite* e *Marketing*. Le celle mostrano i gruppi inclusi in ciascuna vista ActiveView.

NYC_Gruppo vendite e HOU_Gruppo vendite sono entrambi rappresentati nella vista ActiveView Vendite. Se si dispone di un potere nella vista ActiveView Vendite, è possibile gestire qualsiasi membro di NYC_Gruppo vendite e HOU_Gruppo vendite. Se si dispone di poteri anche nella vista ActiveView New York City, tali poteri aggiuntivi si applicano a NYC_Gruppo Marketing. Di conseguenza, i poteri si accumulano dato che le viste ActiveView si sovrappongono.

Le viste ActiveView sovrapposte possono fornire un modello di delega potente e flessibile. Tuttavia, questa funzione può avere anche conseguenze impreviste. È consigliabile pianificare le viste ActiveView per essere certi che ogni amministratore aggiunto disponga solo dei poteri che si intende concedere per ciascun account utente, gruppo, unità organizzativa, contatto o risorsa.

Gruppi in più viste ActiveView

In questo esempio, NYC_Gruppo vendite è rappresentato in più viste ActiveView. I membri di NYC_Gruppo vendite sono rappresentati nella vista ActiveView New York City perché il nome del gruppo soddisfa la regola ActiveView NYC_*. Il gruppo fa parte anche della vista ActiveView Vendite perché il nome soddisfa la regola ActiveView *_Vendite. Includendo lo stesso gruppo in più viste ActiveView, è possibile consentire a diversi amministratori aggiunti di gestire gli stessi oggetti in modo diverso.

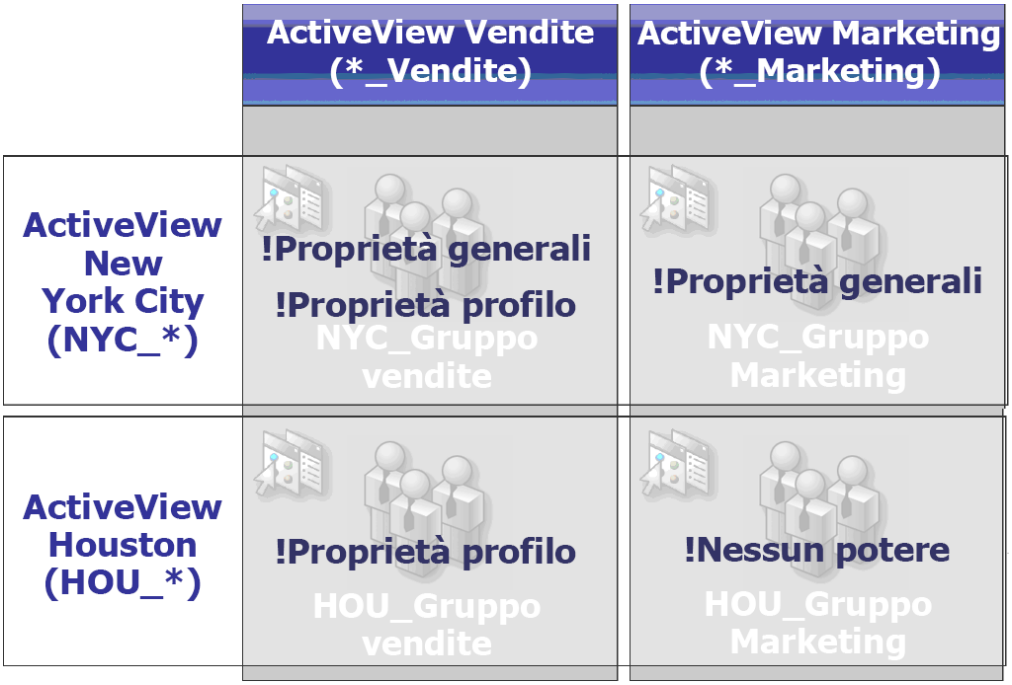


Utilizzo dei poteri in più viste ActiveView

Si supponga che un amministratore aggiunto, MRossi, disponga del potere *Modify General User Properties* (Modifica proprietà utente generali) nella vista ActiveView New York City. Il primo potere consente a MRossi di modificare tutte le proprietà nella scheda Generale della finestra delle

proprietà di un utente. Mrossi dispone del potere *Modify User Profile Properties* (Modifica proprietà del profilo utente) nella vista ActiveView Vendite. Il secondo potere consente a MRossi di modificare tutte le proprietà nella scheda Profilo della finestra delle proprietà di un utente.

Nella figura seguente sono illustrati i poteri di cui MRossi dispone per ciascun gruppo.



Mrossi dispone dei poteri seguenti:

- Proprietà generali nella vista ActiveView NYC_*
- Proprietà del profilo nella vista ActiveView *_Vendite

La delega dei poteri in queste viste ActiveView sovrapposte consente a MRossi di modificare le proprietà nelle schede Generale e Profilo di NYC_Gruppo vendite. Ciò significa che MRossi dispone di tutti i poteri concessi in tutte le viste ActiveView che rappresentano NYC_Gruppo vendite.

7 Viste ActiveView

Le viste ActiveView consentono di implementare un modello di delega che:

- È indipendente dalla struttura di Active Directory
- Consente di assegnare poteri e definire policy correlate ai workflow esistenti
- Consente l'automazione per facilitare un'ulteriore integrazione e personalizzazione dell'azienda
- Risponde in modo dinamico ai cambiamenti

Una vista ActiveView rappresenta un set di oggetti all'interno di uno o più domini gestiti. È possibile includere un oggetto in più viste ActiveView. È inoltre possibile includere numerosi oggetti da più domini o unità organizzative.

Viste ActiveView integrate

Le viste ActiveView integrate sono quelle disponibili di default in DRA e rappresentano tutti gli oggetti e le impostazioni di sicurezza correnti. Pertanto, le viste ActiveView integrate forniscono accesso immediato a tutti gli oggetti e le impostazioni, nonché al modello di delega di default. È possibile utilizzarle per gestire oggetti, quali account utente e risorse, o per applicare il modello di delega di default alla configurazione attuale dell'azienda.

In DRA sono disponibili numerose viste ActiveView integrate che possono rappresentare il modello di delega. Il nodo ActiveView integrato contiene le viste ActiveView seguenti:

All Objects (Tutti gli oggetti)

Include tutti gli oggetti di tutti i domini gestiti. Mediante questa vista ActiveView è possibile gestire qualsiasi aspetto aziendale. Deve essere assegnata all'amministratore o a un amministratore aggiunto che necessita di poteri di revisione su tutta l'azienda.

Objects Current User Manages as Windows Administrator (Oggetti che l'utente attuale gestisce come amministratore di Windows)

Include gli oggetti provenienti dal dominio gestito attuale. Mediante questa vista ActiveView è possibile gestire account utente, gruppi, contatti, unità organizzative e risorse. Deve essere assegnata ad amministratori nativi responsabili degli oggetti Account e Risorsa nel dominio gestito.

Administration Servers and Managed Domains (Server di amministrazione e domini gestiti)

Include i computer del server di amministrazione e i domini gestiti. Mediante questa vista ActiveView è possibile gestire la manutenzione quotidiana dei server di amministrazione. Deve essere assegnata agli amministratori aggiunti i cui compiti comprendono il monitoraggio dello stato di sincronizzazione o l'esecuzione di aggiornamenti della cache.

DRA Policies and Automation Triggers (Policy e trigger di automazione di DRA)

Include tutti gli oggetti connessi a policy e trigger di automazione in tutti i domini gestiti. Mediante questa vista ActiveView è possibile gestire proprietà e ambito delle policy, nonché le proprietà dei trigger di automazione. Deve essere assegnata agli amministratori aggiunti responsabili della creazione e della manutenzione delle policy aziendali.

DRA Security Objects (Oggetti di sicurezza di DRA)

Include tutti gli oggetti di sicurezza. Mediante questa vista ActiveView è possibile gestire viste ActiveView, gruppi di amministratori aggiunti e ruoli. Deve essere assegnata agli amministratori aggiunti responsabili della creazione e della manutenzione del modello di sicurezza.

SPA Users from All Managed and Trusted Domains (Utenti SPA in tutti i domini gestiti e attendibili)

Include tutti gli account utente dei domini gestiti e attendibili. Mediante questa vista ActiveView è possibile gestire le password degli utenti tramite Secure Password Administrator (SPA).

Accesso alle viste ActiveView integrate

Accedendo alle viste ActiveView integrate è possibile eseguire la revisione del modello di delega di default o gestire le proprie impostazioni di sicurezza.

Per accedere alle viste ActiveView integrate:

1. Passare a **Delegation Management** (Gestione delega) > **Manage ActiveViews** (Gestisci viste ActiveView).
2. Verificare che il campo di ricerca sia vuoto e fare clic su **Find Now** (Trova ora) nel riquadro **List items that match my criteria** (Elenca elementi corrispondenti ai miei criteri).
3. Selezionare la vista ActiveView appropriata.

Utilizzo delle viste ActiveView integrate

Non è possibile eliminare, clonare o modificare le viste ActiveView integrate. Tuttavia, è possibile incorporarle nel proprio modello di delega esistente o utilizzarle per progettare un proprio modello.

È possibile utilizzare le viste ActiveView integrate nei modi seguenti:

- Assegnando le singole viste ActiveView integrate ai gruppi di amministratori aggiunti appropriati. Questa associazione consente ai membri di un gruppo di amministratori aggiunti di gestire il set di oggetti corrispondente con i poteri appropriati.
- Facendo riferimento alle regole delle viste ActiveView integrate come linee guida per la progettazione e l'implementazione del modello di delega.

Per ulteriori informazioni sulla progettazione di un modello di delega dinamico, vedere Caratteristiche del modello di delega dinamico.

Implementazione di una vista ActiveView personalizzata

Una vista ActiveView fornisce l'accesso in tempo reale a oggetti specifici all'interno di uno o più domini o unità organizzative. È possibile aggiungere o rimuovere oggetti da una vista ActiveView, senza modificare il dominio sottostante o la struttura dell'unità organizzativa.

Una vista ActiveView può essere considerata come un dominio o una OU virtuale, oppure come il risultato di un'istruzione di selezione o una vista di database per un database relazionale. Le viste ActiveView possono includere o escludere un qualsiasi set di oggetti, contenere altre viste ActiveView e avere contenuti sovrapposti. Possono anche contenere oggetti di domini, alberi e foreste diversi. È possibile configurare le viste ActiveView affinché rispondano alle più svariate esigenze di gestione aziendale.

Nelle viste ActiveView è possibile includere i seguenti tipi di oggetti:

Account:

- Utenti
- Gruppi
- Computer
- Contatti
- Gruppi di distribuzione dinamici
- Account del servizio gestito del gruppo
- Stampanti pubblicate
- Lavori di stampa di stampanti pubblicate
- Caselle postali di risorse
- Caselle postali condivise
- Cartelle pubbliche

Oggetti Directory:

- Unità organizzative
- Domini
- Server membri

Oggetti di delega:

- Viste ActiveView
- Auto amministrazione
- Dipendenti
- Gruppi gestiti

Risorse:

- Utenti connessi
- Dispositivi
- Log degli eventi
- File aperti

- Stampanti
- Lavori di stampa
- Servizi
- Condivisioni

Oggetti Azure:

- Utente Azure
- Utente guest Azure
- Gruppo Azure
- Tenant di Azure
- Contatto Azure

Seguendo i cambiamenti e la crescita dell'azienda, le viste ActiveView cambiano includendo o escludendo i nuovi oggetti. Perciò, è possibile utilizzare le viste ActiveView per ridurre la complessità del modello, fornire la sicurezza necessaria e ottenere una flessibilità nettamente superiore a quella offerta da altri strumenti organizzativi.

Regole delle viste ActiveView

Una vista ActiveView può essere costituita da regole che includono o escludono oggetti quali account utente, gruppi, unità organizzative, contatti, risorse, computer, caselle postali di risorse, caselle postali condivise, gruppi di distribuzione dinamici, account del servizio gestito del gruppo viste ActiveView e oggetti Azure quali utenti Azure, gruppi Azure e contatti Azure. Tale flessibilità rende dinamiche le viste ActiveView.

Le corrispondenze sono denominate **caratteri jolly**. Ad esempio, è possibile definire una regola per includere tutti i computer con nomi corrispondenti a `DOM*`. Quando si specifica questo carattere jolly, vengono cercati gli account computer il cui nome inizia con la stringa di caratteri DOM. I caratteri jolly rendono dinamica l'amministrazione, poiché quando gli account soddisfano la regola vengono inclusi automaticamente. Perciò, quando si utilizzano i caratteri jolly, non è necessario riconfigurare le viste ActiveView in caso di cambiamenti organizzativi.

Un'altra possibilità consiste nel definire le viste ActiveView in base all'appartenenza a gruppi. È possibile definire una regola che include tutti i membri dei gruppi che iniziano con le lettere NYC. In questo modo, quando vengono aggiunti membri a un gruppo che soddisfa questa regola, essi vengono automaticamente inclusi nella vista ActiveView. Seguendo i cambiamenti e la crescita dell'azienda, DRA applica nuovamente le regole in modo da escludere o includere i nuovi oggetti nelle viste ActiveView appropriate.

8 Ruoli

In questa sezione si elencano e si descrivono i ruoli integrati di DRA, illustrando anche come utilizzarli, e si forniscono informazioni sulla creazione e la gestione di ruoli personalizzati.

Per una descrizione generale dei ruoli e del loro utilizzo, vedere Controlli del modello di delega.

Ruoli integrati

I ruoli integrati degli amministratori aggiunti forniscono accesso immediato a un set di poteri utilizzati di frequente. È possibile estendere la configurazione di sicurezza attuale utilizzando i ruoli di default per delegare poteri ad account utente specifici o ad altri gruppi.

Questi ruoli contengono i poteri necessari per eseguire task di amministrazione comuni. Ad esempio, il ruolo DRA Administration (Amministrazione DRA) include tutti i poteri necessari per gestire gli oggetti. Tuttavia, per utilizzare questi poteri, il ruolo deve essere associato a un account utente o a un gruppo di amministratori aggiunti e alla vista ActiveView gestita.

Poiché i ruoli integrati sono parte del modello di delega di default, è possibile utilizzarli per delegare rapidamente il potere e implementare la sicurezza. I ruoli integrati gestiscono i task comuni che è possibile eseguire mediante le interfacce utente di DRA. Nelle sezioni seguenti vengono descritti i singoli ruoli integrati, con una sintesi dei poteri associati ai ruoli.

Azure Active Directory Management (Gestione di Azure Active Directory)

Azure Contact Administration (Amministrazione contatto Azure):

Fornisce tutti i poteri necessari per creare, modificare, eliminare e visualizzare le proprietà di un contatto Azure. È possibile assegnare il ruolo a tutti gli amministratori aggiunti responsabili della gestione dei contatti Azure.

Azure Group Administration (Amministrazione gruppo Azure)

Fornisce tutti i poteri necessari per gestire i gruppi Azure e l'appartenenza ad Azure.

Azure User Administration (Amministrazione utente Azure)

Fornisce tutti i poteri necessari per creare, modificare, eliminare, abilitare, disabilitare, nonché per visualizzare le proprietà di un utente Azure. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dell'utente Azure.

Azure Guest User Administration (Amministrazione utente guest Azure)

Fornisce tutti i poteri necessari per gestire un utente guest Azure. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dell'utente guest Azure.

Amministrazione

Contact Administration (Amministrazione contatti)

Fornisce tutti i poteri necessari per creare un nuovo contatto, modificare le proprietà del contatto o eliminare un contatto. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei contatti.

DRA Administration (Amministrazione DRA)

Fornisce tutti i poteri a un amministratore aggiunto. Questo ruolo concede a un utente le autorizzazioni per eseguire tutti i task amministrativi in DRA. È equivalente alle autorizzazioni di un amministratore. Un amministratore aggiunto associato al ruolo di amministrazione di DRA può accedere a tutti i nodi di Directory and Resource Administrator.

gMSA Administration (Amministrazione gMSA)

Fornisce i poteri necessari per creare, modificare, eliminare e visualizzare le proprietà di un account del servizio gestito del gruppo (gMSA). È possibile assegnare il ruolo a tutti gli amministratori aggiunti responsabili della gestione di un account gMSA.

Manage and Execute Custom Tools (Gestisci ed esegui strumenti personalizzati)

Fornisce tutti i poteri necessari per creare, gestire ed eseguire strumenti personalizzati. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di strumenti personalizzati.

Manage Clone Exceptions (Gestisci eccezioni di clonazione)

Fornisce tutti i poteri necessari per creare e gestire eccezioni di clonazione.

Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione)

Fornisce tutti i poteri necessari per definire policy e trigger di automazione. Assegnare il ruolo agli amministratori aggiunti responsabili della manutenzione delle policy aziendali e dell'automazione dei workflow.

Manage Security Model (Gestisci modello di sicurezza)

Fornisce tutti i poteri necessari per definire le regole di amministrazione, quali viste ActiveView, amministratori aggiunti e ruoli. Assegnare il ruolo agli amministratori aggiunti responsabili dell'implementazione e della gestione del modello di sicurezza.

Manage Virtual Attributes (Gestisci attributi virtuali)

Fornisce tutti i poteri necessari per creare e gestire attributi virtuali. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli attributi virtuali.

OU Administration (Amministrazione OU)

Fornisce tutti i poteri necessari per gestire le unità organizzative. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione della struttura di Active Directory.

Public Folder Administration (Amministrazione cartelle pubbliche)

Fornisce i poteri di creazione, modifica, eliminazione, abilitazione o disabilitazione della posta, nonché di visualizzazione delle proprietà della cartella pubblica dell'utente. È possibile assegnare il ruolo a tutti gli amministratori aggiunti responsabili della gestione della cartella pubblica.

Replicate Files (Replica file)

Fornisce tutti i poteri necessari per effettuare l'upload, eliminare e modificare informazioni sui file. Assegnare il ruolo agli amministratori aggiunti responsabili della replica dei file dal server di amministrazione primario ad altri server di amministrazione dell'MMS e a computer client DRA.

Reset Local Administrator Password (Reimposta password amministratore locale)

Fornisce tutti i poteri necessari per reimpostare la password dell'account dell'amministratore locale e visualizzare il nome dell'amministratore del computer. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account amministratore.

Self Administration (Auto amministrazione)

Fornisce tutti i poteri necessari per modificare le proprietà di base, ad esempio i numeri di telefono, del proprio account utente. Assegnare il ruolo agli amministratori aggiunti che devono gestire le proprie informazioni personali.

Gestione avanzata delle query

Execute Advanced Queries (Esegui query avanzate)

Fornisce tutti i poteri necessari per eseguire query avanzate precedentemente salvate. Assegnare il ruolo agli amministratori aggiunti responsabili dell'esecuzione di query avanzate.

Manage Advanced Queries (Gestisci query avanzate)

Fornisce tutti i poteri necessari per creare, gestire ed eseguire query avanzate. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di query avanzate.

Gestione revisione

Audit All Objects (Revisiona tutti gli oggetti)

Fornisce tutti i poteri necessari per visualizzare le proprietà di oggetti, policy e configurazioni di tutta l'azienda. Questo ruolo non consente agli amministratori aggiunti di modificare le proprietà. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione delle azioni all'interno dell'azienda. Consente agli amministratori aggiunti di visualizzare tutti i nodi ad eccezione del nodo Custom Tools (Strumenti personalizzati).

Audit Limited Account and Resource Properties (Revisiona proprietà limitate di account e risorse)

Fornisce i poteri per tutte le proprietà degli oggetti.

Audit Resources (Revisiona risorse)

Fornisce tutti i poteri necessari per visualizzare le proprietà di risorse gestite. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione degli oggetti Risorsa.

Audit Users and Groups (Revisiona utenti e gruppi)

Fornisce tutti i poteri necessari per visualizzare le proprietà di account utente e gruppi, ma nessun potere di modifica di tali proprietà. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione delle proprietà degli account.

Gestione computer

Computer Administration (Amministrazione computer)

Fornisce tutti i poteri necessari per modificare le proprietà dei computer. Questo ruolo consente agli amministratori aggiunti di aggiungere, eliminare e spegnere i computer, nonché di sincronizzare i controller di dominio. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei computer nella vista ActiveView.

Create and Delete Computer Accounts (Crea ed elimina account computer)

Fornisce tutti i poteri necessari per creare ed eliminare un account computer. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei computer.

Manage Computer Properties (Gestisci proprietà computer)

Fornisce tutti i poteri necessari per gestire tutte le proprietà di un account computer. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei computer.

View All Computer Properties (Visualizza tutte le proprietà di un computer)

Fornisce tutti i poteri necessari per visualizzare le proprietà di un account computer. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione dei computer.

Gestione di Exchange

Clone User with Mailbox (Clona utente con casella postale)

Fornisce tutti i poteri necessari per clonare un account utente esistente insieme alla relativa casella postale. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente.

Nota: per consentire all'amministratore aggiunto di aggiungere il nuovo account utente a un gruppo durante il task di clonazione, assegnare anche il ruolo Manage Group Memberships (Gestisci appartenenze a gruppi).

Create and Delete Resource Mailbox (Crea ed elimina casella postale risorsa)

Fornisce tutti i poteri necessari per creare ed eliminare una casella postale. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle caselle postali.

Mailbox Administration (Amministrazione caselle postali)

Fornisce tutti i poteri necessari per gestire le proprietà delle caselle postali di Microsoft Exchange. Se si utilizza Microsoft Exchange, assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle caselle postali di Microsoft Exchange.

Manage Exchange Mailbox Rights (Gestisci diritti caselle postali di Exchange)

Fornisce tutti i poteri necessari per gestire la sicurezza e i diritti delle caselle postali di Microsoft Exchange. Se si utilizza Microsoft Exchange, assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle autorizzazioni delle caselle postali di Microsoft Exchange.

Manage Group Email (Gestisci e-mail gruppo)

Fornisce tutti i poteri necessari per visualizzare, abilitare o disabilitare l'indirizzo e-mail di un gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di gruppi o indirizzi e-mail per gli oggetti Account.

Manage Mailbox Move Requests (Gestisci richieste di spostamento caselle postali)

Fornisce tutti i poteri necessari per gestire le richieste di spostamento delle caselle postali.

Manage Resource Mailbox Properties (Gestisci proprietà delle caselle postali delle risorse)

Fornisce tutti i poteri necessari per gestire tutte le proprietà di una casella postale. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle caselle postali.

Manage User Email (Gestisci e-mail utente)

Fornisce tutti i poteri necessari per visualizzare, abilitare o disabilitare l'indirizzo e-mail di un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di account utente o indirizzi e-mail per gli oggetti Account.

Reset Unified Messaging PIN Properties (Reimposta proprietà PIN di Messaggistica unificata)

Fornisce tutti i poteri necessari per reimpostare il PIN di Messaggistica unificata per gli account utente.

Resource Mailbox Administration (Amministrazione caselle postali delle risorse)

Fornisce tutti i poteri necessari per gestire le caselle postali delle risorse.

Shared Mailbox Administration (Amministrazione caselle postali condivise)

Fornisce tutti i poteri necessari per creare, modificare, eliminare e visualizzare le proprietà delle caselle postali condivise. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle caselle postali condivise.

View All Resource Mailbox Properties (Visualizza tutte le proprietà di una casella postale risorsa)

Fornisce tutti i poteri necessari per visualizzare le proprietà di una casella postale risorsa. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione delle caselle postali risorse.

Gestione gruppo

Create and Delete Groups (Crea ed elimina gruppi)

Fornisce tutti i poteri necessari per creare ed eliminare un gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei gruppi.

Dynamic Group Administration (Amministrazione gruppi dinamici)

Fornisce tutti i poteri necessari per gestire i gruppi dinamici di Active Directory.

Group Administration (Amministrazione gruppi)

Fornisce tutti i poteri necessari per gestire i gruppi e le relative appartenenze, nonché per visualizzare le proprietà degli utenti corrispondenti. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di gruppi o account e di oggetti Risorsa gestiti mediante gruppi.

Manage Dynamic Distribution Groups (Gestisci gruppi di distribuzione dinamici)

Fornisce tutti i poteri necessari per gestire gruppi di distribuzione dinamici Microsoft Exchange.

Manage Group Membership Security (Gestisci sicurezza appartenenze a gruppi)

Fornisce tutti i poteri necessari per designare chi può visualizzare e modificare le appartenenze ai gruppi Microsoft Windows tramite Microsoft Outlook.

Manage Group Memberships (Gestisci appartenenze a gruppi)

Fornisce tutti i poteri necessari per aggiungere e rimuovere account utente o gruppi da un gruppo esistente, oltre che per visualizzare il gruppo primario di un account utente o computer. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di gruppi o account utente.

Manage Group Properties (Gestisci proprietà gruppi)

Fornisce tutti i poteri necessari per gestire tutte le proprietà di un gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei gruppi.

Manage Temporary Group Assignments (Gestisci assegnazioni temporanee al gruppo)

Fornisce tutti i poteri necessari per creare e gestire assegnazioni temporanee al gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei gruppi.

Rename Group and Modify Description (Rinomina gruppo e modifica descrizione)

Fornisce tutti i poteri necessari per modificare il nome e la descrizione di un gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei gruppi.

View All Group Properties (Visualizza tutte le proprietà di un gruppo)

Fornisce tutti i poteri necessari per visualizzare le proprietà di un gruppo. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione dei gruppi.

Gestione rapporti

Manage Active Directory Collectors, DRA Collectors, and Management Reporting Collectors (Gestisci servizi di raccolta Active Directory, DRA e generazione di rapporti di gestione)

Fornisce tutti i poteri necessari per gestire i servizi di raccolta di Active Directory, di DRA e di generazione dei rapporti di gestione per la raccolta dati. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione della configurazione del di generazione di rapporti.

Manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration (Gestisci servizi di raccolta Active Directory, DRA, generazione di rapporti di gestione e configurazione database)

Fornisce tutti i poteri necessari per la gestione dei servizi di raccolta di Active Directory, di DRA, di generazione dei rapporti di gestione e della configurazione del database per la raccolta dati. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione della configurazione per la generazione di rapporti e per il database.

Manage UI Reporting (Gestisci generazione di rapporti interfaccia utente)

Fornisce tutti i poteri necessari per generare ed esportare rapporti di dettaglio delle attività per utenti, gruppi, contatti, computer, unità organizzative, poteri, ruoli, viste ActiveView, container, stampanti pubblicate e amministratori aggiunti. Assegnare il ruolo agli amministratori aggiunti responsabili della generazione dei rapporti.

Manage Database Configuration (Gestisci configurazione database)

Fornisce tutti i poteri necessari per gestire la configurazione del database per i rapporti di gestione. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione della configurazione del database di generazione di rapporti.

View Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration Information (Visualizza servizi di raccolta Active Directory, DRA, generazione di rapporti di gestione e le informazioni di configurazione database)

Fornisce tutti i poteri necessari per visualizzare i servizi di raccolta di AD, di DRA e di la generazione di rapporti di gestione, nonché per le informazioni di configurazione del database.

Resource Management

Create and Delete Resources (Crea ed elimina risorse)

Fornisce tutti i poteri necessari per creare ed eliminare condivisioni e account computer, oltre che per eliminare log degli eventi. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione di oggetti Risorsa e di log degli eventi.

Manage Printers and Print Jobs (Gestisci stampanti e lavori di stampa)

Fornisce tutti i poteri necessari per gestire stampanti, code di stampa e lavori di stampa. Per gestire i lavori di stampa associati a un account utente, il lavoro di stampa e l'account utente devono essere inclusi nella stessa vista ActiveView. Assegnare il ruolo agli amministratori aggiunti responsabili della manutenzione delle stampanti e della gestione dei lavori di stampa.

Manage Resources for Managed Users (Gestisci risorse per utenti gestiti)

Fornisce tutti i poteri necessari per gestire le risorse associate ad account utente specifici. L'amministratore aggiunto e gli account utente devono essere inclusi nella stessa vista ActiveView. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli oggetti Risorsa.

Manage Services (Gestisci servizi)

Fornisce tutti i poteri necessari per gestire i servizi. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dei servizi.

Manage Shared Folders (Gestisci cartelle condivise)

Fornisce tutti i poteri necessari per gestire le cartelle condivise. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle cartelle condivise.

Resource Administration (Amministrazione risorse)

Fornisce tutti i poteri necessari per modificare le proprietà delle risorse gestite, incluse quelle associate a un qualsiasi account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli oggetti Risorsa.

Start and Stop Resources (Avvia e interrompi risorse)

Fornisce tutti i poteri necessari per sospendere, avviare, riprendere o interrompere un servizio, avviare o interrompere un dispositivo o una stampante, spegnere un computer oppure sincronizzare i controller di dominio. Fornisce anche tutti i poteri necessari per sospendere, riprendere e avviare i servizi, interrompere i dispositivi o le code di stampa e spegnere i computer. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli oggetti Risorsa.

Gestione server

Built-in Scheduler (Pianificazione integrata) - Solo per uso interno

Fornisce i poteri per pianificare l'aggiornamento della cache in DRA.

Application Servers Administration (Amministrazione dei server per applicazioni)

Fornisce i poteri necessari per configurare, visualizzare ed eliminare le configurazioni dei server per applicazioni.

Configure Servers and Domains (Configura server e domini)

Fornisce tutti i poteri necessari per modificare le opzioni del server di amministrazione e i domini gestiti. Fornisce inoltre i poteri necessari per configurare e gestire i tenant di Azure. Assegnare il ruolo agli amministratori aggiunti responsabili del controllo e della manutenzione dei server amministrativi e della gestione dei tenant di Azure.

Unified Change History Server Administration (Amministrazione server Cronologia modifiche unificata)

Fornisce i poteri necessari per configurare, visualizzare ed eliminare le configurazioni del server di Cronologia modifiche unificata.

Workflow Automation Server Administration (Amministrazione server di Workflow Automation)

Fornisce i poteri necessari per configurare, visualizzare ed eliminare le configurazioni del server di Workflow Automation.

Gestione account utente

Create and Delete User Accounts (Crea ed elimina account utente)

Fornisce tutti i poteri necessari per creare ed eliminare un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente.

Help Desk Administration (Amministrazione help desk)

Fornisce tutti i poteri necessari per visualizzare le proprietà degli account utente e per modificare le password e le relative proprietà. Questo ruolo consente inoltre agli amministratori aggiunti di disabilitare, abilitare e sbloccare gli account utente. Assegnare il ruolo agli amministratori aggiunti responsabili di compiti di help desk connessi alla verifica dell'accesso appropriato degli utenti ai loro account.

Manage User Dial in Properties (Gestisci proprietà di accesso telefonico utente)

Fornisce tutti i poteri necessari per modificare le proprietà di accesso telefonico degli account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente che dispongono di accesso remoto all'azienda.

Manage User Password and Unlock Account (Gestisci password utente e sblocca account)

Fornisce tutti i poteri necessari per reimpostare la password, specificare le impostazioni della password e sbloccare un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dell'accesso per gli account utente.

Manage User Properties (Gestisci proprietà utente)

Fornisce tutti i poteri necessari per gestire tutte le proprietà di un account utente, incluse le proprietà delle caselle postali di Microsoft Exchange. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente.

Rename User and Modify Description (Rinomina utente e modifica descrizione)

Fornisce tutti i poteri necessari per modificare il nome e la descrizione di un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente.

Reset Password (Reimposta password)

Fornisce tutti i poteri necessari per reimpostare e modificare le password. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle password.

Reset Password and Unlock Account Using SPA (Reimposta password e sblocca account tramite SPA)

Fornisce tutti i poteri necessari per utilizzare Secure Password Administrator al fine di reimpostare le password e sbloccare gli account utente.

Transform a User (Trasforma un utente)

Fornisce tutti i poteri necessari per aggiungere o rimuovere un utente dai gruppi inclusi in un account modello, oltre alla possibilità di modificare le proprietà dell'utente durante la trasformazione.

User Administration (Amministrazione utenti)

Fornisce tutti i poteri necessari per gestire gli account utente, le caselle postali Microsoft Exchange associate e le appartenenze a gruppi. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione degli account utente.

View All User Properties (Visualizza tutte le proprietà di un utente)

Fornisce tutti i poteri necessari per visualizzare le proprietà di un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della revisione degli account utente.

WTS Administration (Amministrazione WTS)

Manage WTS Environment Properties (Gestisci proprietà ambiente WTS)

Fornisce tutti i poteri necessari per modificare le proprietà dell'ambiente WTS per un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dell'ambiente WTS o degli account utente.

Manage WTS Remote Control Properties (Gestisci proprietà di controllo remoto WTS)

Fornisce tutti i poteri necessari per modificare le proprietà di controllo remoto WTS per un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione dell'accesso WTS o degli account utente.

Manage WTS Session Properties (Gestisci proprietà sessione WTS)

Fornisce tutti i poteri necessari per modificare le proprietà della sessione WTS per un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle sessioni WTS o degli account utente.

Manage WTS Terminal Properties (Gestisci proprietà terminale WTS)

Fornisce tutti i poteri necessari per modificare le proprietà del terminale WTS per un account utente. Assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle proprietà dei terminali WTS o degli account utente.

WTS Administration (Amministrazione WTS)

Fornisce tutti i poteri necessari per gestire le proprietà di Windows Terminal Server (WTS) per gli account utente nella vista ActiveView. Se si utilizza WTS, assegnare il ruolo agli amministratori aggiunti responsabili della gestione delle proprietà WTS degli account utente.

Accesso ai ruoli integrati

Accedendo ai ruoli integrati è possibile eseguire la revisione del modello di delega di default o gestire le proprie impostazioni di sicurezza.

Per accedere ai ruoli integrati:

1. Passare a **Delegation Management** (Gestione delega) > **Manage Roles** (Gestisci ruoli).
2. Verificare che il campo di ricerca sia vuoto e fare clic su **Find Now** (Trova ora) nel riquadro **List items that match my criteria** (Elenca elementi corrispondenti ai miei criteri).
3. Selezionare il ruolo appropriato.

Utilizzo dei ruoli integrati

Non è possibile eliminare né modificare i ruoli integrati. Tuttavia, i ruoli integrati possono essere incorporati nel modello di delega esistente o utilizzati per progettare e implementare il proprio modello.

È possibile utilizzare i ruoli integrati nei modi seguenti:

- Associando un ruolo integrato a un account utente o a gruppo di amministratori aggiunti. Questa associazione fornisce all'utente o ai membri del gruppo di amministratori aggiunti i poteri appropriati per il task.
- Clonando un ruolo integrato e utilizzare il clone come base per un ruolo personalizzato. È possibile aggiungere altri ruoli o poteri al nuovo ruolo e rimuovere poteri originariamente inclusi nel ruolo integrato.

Per ulteriori informazioni sulla progettazione di un modello di delega dinamico, vedere Caratteristiche del modello di delega dinamico.

Creazione di ruoli personalizzati

Mediante la creazione di un ruolo, è possibile delegare in modo rapido e semplice un set di poteri che rappresenta un task o un workflow amministrativo. Per creare e gestire i ruoli, utilizzare il nodo **Delegation Management** (Gestione delega) > **Roles** (Ruoli) nella Console di delega e configurazione. In questo nodo è possibile eseguire le operazioni seguenti:

- Creare nuovi ruoli

- Clonare ruoli esistenti
- Modificare le proprietà dei ruoli
- Eliminare i ruoli
- Gestire le assegnazioni dei ruoli
  - Delegare una nuova assegnazione
  - Rimuovere un'assegnazione esistente
  - Visualizzare le proprietà di un amministratore aggiunto assegnato
  - Visualizzare le proprietà di una vista ActiveView assegnata
- Gestire i ruoli e i poteri di un ruolo (i ruoli possono essere nidificati)
- Generare rapporti sulle modifiche dei ruoli

Il workflow generale per eseguire una delle azioni menzionate in questa sezione inizia con la selezione del nodo **Ruoli** e continua con una delle operazioni seguenti:

- Utilizzare il menu **Task** o il menu di scelta rapida per aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione desiderata.
- Individuare l'oggetto Ruolo nel riquadro **List items that match my criteria** (Elenca elementi corrispondenti ai miei criteri) e utilizzare il menu **Task** o il menu di scelta rapida per selezionare e aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione necessaria.

Per eseguire una delle azioni precedenti, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo Manage Security Model (Gestisci modello di sicurezza).

9 Poteri

I poteri sono le fondamenta dell'amministrazione basata sul "minimo privilegio". Assegnando poteri agli utenti si implementa e si gestisce il modello di sicurezza dinamico. Queste procedure si eseguono nella Console di delega e configurazione.

Poteri integrati

Sono disponibili oltre 390 poteri integrati per la gestione di oggetti e l'esecuzione di task amministrativi comuni ed è possibile utilizzarli per definire ruoli e assegnare deleghe. I poteri integrati non possono essere eliminati, ma è possibile clonarli per creare poteri personalizzati. Di seguito sono riportati alcuni esempi di poteri integrati:

Create Group and Modify All Properties (Crea gruppo e modifica tutte le proprietà)

Concede il potere di creare gruppi e specificare tutte le proprietà durante la creazione.

Delete User Account (Elimina account utente)

Se il Cestino è abilitato, concede il potere di spostare gli account utente nel Cestino. Se il Cestino è disabilitato, concede il potere di eliminare definitivamente gli account utente.

Modify All Computer Properties (Modifica tutte le proprietà dei computer)

Concede il potere di modificare tutte le proprietà degli account computer.

Poteri di Azure

Utilizzare i seguenti poteri per delegare la creazione e la gestione di utenti, gruppi e contatti Azure.

Poteri dell'account utente Azure:

- Create Azure User and Modify All Properties (Crea utente Azure e modifica tutte le proprietà)
- Delete Azure User Account Permanently (Elimina definitivamente account utente Azure)
- Manage Sign-In for Azure Users (Gestisci login per utenti Azure)
- Manage Sign-In for Azure Users Synced to Azure Tenant (Gestisci login per utenti Azure sincronizzati con il tenant di Azure)
- Modify All Azure User Properties (Modifica tutte le proprietà dell'utente Azure)
- Reset Azure User Account Password (Reimposta password dell'account utente Azure)
- View All Azure User Properties (Visualizza tutte le proprietà dell'utente Azure)

Poteri del gruppo Azure:

- Add Object to Azure Group (Aggiungi oggetto a gruppo Azure)
- Create Azure Group and Modify All Properties (Crea gruppo Azure e modifica tutte le proprietà)
- Delete Azure Group Account (Elimina account gruppo Azure)
- Modify All Azure Group Properties (Modifica tutte le proprietà del gruppo Azure)

- Remove Object from Azure Group (Rimuovi oggetto da gruppo Azure)
- View All Azure Group Properties (Visualizza tutte le proprietà del gruppo Azure)

Poteri del contatto Azure:

- Create Azure Contact and Modify All Properties (Crea contatto Azure e modifica tutte le proprietà)
- Delete Azure Contact Account (Elimina account contatto Azure)
- Modify All Azure Contact Properties (Modifica tutte le proprietà del contatto Azure)
- View All Azure Contact Properties (Visualizza tutte le proprietà del contatto Azure)

Potere dell'account utente guest Azure:

- Invite Azure Guest User (Invita utente guest Azure)

I poteri elencati per gli account utente Azure si applicano anche agli account utente guest Azure.

Per gestire le proprietà in modo differenziato per gli oggetti Azure, è possibile creare poteri personalizzati selezionando attributi dell'oggetto specifici.

Implementazione di poteri personalizzati

Per creare un potere personalizzato, è necessario creare un nuovo potere o clonarne uno esistente. È possibile utilizzare un potere esistente come modello per delegare nuovi poteri. Un potere definisce le proprietà di un oggetto che un amministratore aggiunto può visualizzare, modificare o creare nel dominio o sottoalbero gestito. I poteri personalizzati possono includere l'accesso a più proprietà, come ad esempio il potere *View All User Properties* (Visualizza tutte le proprietà utente).

Nota: non è possibile clonare tutti i poteri integrati.

Per implementare poteri personalizzati si utilizza il nodo **Delegation Management** (Gestione delega) > **Powers** (Poteri) nella Console di delega e configurazione. In questo nodo è possibile eseguire le operazioni seguenti:

- Visualizzare tutte le proprietà del potere
- Creare nuovi poteri
- Clonare poteri esistenti
- Modificare poteri personalizzati
- Generare rapporti sulle modifiche dei poteri

Per eseguire queste azioni, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo Manage Security Model (Gestisci modello di sicurezza).

Prima di creare un nuovo potere, valutare il processo seguente.

1. Esaminare i poteri disponibili in DRA.
2. Decidere se è necessario un potere personalizzato. Se applicabile, è possibile clonare un potere personalizzato esistente.
3. Eseguire le procedure guidate appropriate, ad esempio la procedura guidata New Power (Nuovo potere).

4. Visualizzare il nuovo potere.
5. Modificare il nuovo potere, se necessario.

Il workflow generale per eseguire una delle azioni menzionate in questa sezione inizia con la selezione del nodo **Poteri** e continua con una delle operazioni seguenti:

- Utilizzare il menu Task o il menu di scelta rapida per aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione desiderata.
- Individuare l'oggetto Potere nel riquadro **List items that match my criteria** (Elenca elementi corrispondenti ai miei criteri) e utilizzare il menu **Task** o il menu di scelta rapida per selezionare e aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione necessaria.

Estensione dei poteri

È possibile aggiungere autorizzazioni o funzionalità a un potere estendendolo.

Ad esempio, per consentire a un amministratore aggiunto di creare un account utente, è possibile assegnare il potere *Create User and Modify All Properties* (Crea utente e modifica tutte le proprietà) o il potere *Create User and Modify Limited Properties* (Crea utente e modifica proprietà limitate). Se si assegna anche il potere *Add New User to Group* (Aggiungi nuovo utente a gruppo), l'amministratore aggiunto potrà aggiungere il nuovo account utente a un gruppo quando utilizza la procedura guidata Crea utente. In questo caso, il potere *Add New User to Group* (Aggiungi nuovo utente a gruppo) offre una funzione aggiuntiva nella procedura guidata. Il potere *Add New User to Group* (Aggiungi nuovo utente a gruppo) è il **potere esteso**.

I poteri estesi non consentono di per sé di aggiungere autorizzazioni o funzionalità. Per poter delegare un task che include un potere esteso, è necessario assegnare il potere esteso insieme al potere che si desidera estendere.

Nota

- Per creare un gruppo e includerlo in una vista ActiveView, è necessario disporre del potere *Add New Group to ActiveView* (Aggiungi nuovo gruppo a vista ActiveView) per la vista ActiveView specificata. La vista ActiveView specificata deve includere anche il container OU o integrato che conterrà il nuovo gruppo.
- Per clonare un gruppo e includerlo in una vista ActiveView, è necessario disporre del potere *Add Cloned Group to ActiveView* (Aggiungi gruppo clonato a vista ActiveView) per la vista ActiveView specificata. Nella vista ActiveView specificata deve essere incluso anche il gruppo di origine e il container OU o integrato che contiene tale nuovo gruppo.

Nella tabella seguente sono elencati alcuni esempi di azioni che è possibile configurare quando si crea un nuovo potere o si modificano le proprietà di un potere esistente:

Per delegare questo task	Assegnare questo potere	E questo potere esteso
Clonare un gruppo e includere il nuovo gruppo in una vista ActiveView specificata	Clone Group and Modify All Properties (Clona gruppo e modifica tutte le proprietà)	Add Cloned Group to ActiveView (Aggiungi gruppo clonato a vista ActiveView)

Per delegare questo task	Assegnare questo potere	E questo potere esteso
Creare un gruppo e includerlo in una vista ActiveView specificata	Create Group and Modify All Properties (Crea gruppo e modifica tutte le proprietà)	Add New Group to ActiveView (Aggiungi nuovo gruppo a vista ActiveView)
Creare un contatto abilitato per la posta	Create Contact and Modify All Properties (Crea contatto e modifica tutte le proprietà) Create Contact and Modify Limited Properties (Crea contatto e modifica proprietà limitate)	Enable Email for New Contact (Abilita e-mail per nuovo contatto)
Creare un gruppo abilitato per la posta	Create Group and Modify All Properties (Crea gruppo e modifica tutte le proprietà)	Enable Email for New Group (Abilita e-mail per nuovo gruppo)
Creare un account utente abilitato per la posta	Create User and Modify All Properties (Crea utente e modifica tutte le proprietà) Create User and Modify Limited Properties (Crea utente e modifica proprietà limitate)	Enable Email for New User (Abilita e-mail per nuovo utente)
Creare un account utente e aggiungerlo a gruppi specifici	Create User and Modify All Properties (Crea utente e modifica tutte le proprietà) Create User and Modify Limited Properties (Crea utente e modifica proprietà limitate)	Add New User to Group (Aggiungi nuovo utente a gruppo)

10 Assegnazioni di deleghe

Le assegnazioni di deleghe si gestiscono mediante la Console di delega e configurazione nel nodo **Delegation Management** (Gestione delega) > **Amministratore aggiunto**. In questo nodo è possibile visualizzare i poteri e i ruoli assegnati agli amministratori aggiunti e gestire le assegnazioni di ruoli e viste ActiveView. Mediante i gruppi di amministratori aggiunti è inoltre possibile:

- Aggiungere membri ai gruppi
- Creare gruppi
- Clonare gruppi
- Eliminare gruppi
- Modificare proprietà dei gruppi

Per visualizzare e gestire le assegnazioni e apportare modifiche ai gruppi di amministratori aggiunti, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo Manage Security Model (Gestisci modello di sicurezza).

Il workflow generale per eseguire una delle azioni menzionate in questa sezione inizia con la selezione del nodo **Amministratori aggiunti** e continua con una delle operazioni seguenti:

- Utilizzare il menu Task o il menu di scelta rapida per aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione desiderata.
- Individuare il gruppo o l'amministratore aggiunto nel riquadro **List items that match my criteria** (Elenca elementi corrispondenti ai miei criteri) e utilizzare il menu **Task** o il menu di scelta rapida per selezionare e aprire la procedura guidata o la finestra di dialogo corrispondente per eseguire l'azione necessaria.

IV Configurazione dei componenti e dei processi

In questo capitolo vengono fornite informazioni per la configurazione iniziale di DRA con i server e le personalizzazioni dei server, le console e le personalizzazioni delle console, l'amministrazione di Azure, l'amministrazione delle cartelle pubbliche e la connessione ai server.

11 Configurazione iniziale

In questa sezione si descrivono i passaggi di configurazione da eseguire se si installa Directory and Resource Administrator per la prima volta.

Elenco di controllo della configurazione

Per la configurazione di DRA per il primo utilizzo, utilizzare come guida l'elenco di controllo seguente.

Passaggi	Dettagli
Installazione di una licenza di DRA	Utilizzare l'utility Health Check per applicare una licenza di DRA. Per ulteriori informazioni sulle licenze di DRA, vedere Requisiti relativi alle licenze.
Configurazione dei server DRA e delle funzioni	Configurare l'MMS, le eccezioni di clonazione, la replica dei file, la registrazione degli eventi, la memorizzazione nella cache, AD LDS, i gruppi dinamici, il Cestino, la generazione di rapporti, Cronologia modifiche unificata e il server di workflow.
Configurazione della generazione di rapporti della cronologia delle modifiche (facoltativo)	Configurare la generazione di rapporti della cronologia delle modifiche se si desidera eseguire l'integrazione con un server Change Guardian per raccogliere i dati della cronologia delle modifiche per gli eventi utente interni ed esterni a DRA.
Configurazione dei servizi DRA per un account gMSA (facoltativo)	Configurare i servizi DRA per un account del servizio gestito del gruppo (gMSA) se si desidera gestire il protocollo di autenticazione su più server rispetto a un unico server.
Configurazione del client di delega e configurazione	Configurare le modalità di accesso e visualizzazione degli elementi nel client di configurazione e delega.
Configurazione del client Web	Configurare il logout automatico, i certificati, le connessioni al server e i componenti di autenticazione.

Installazione o upgrade delle licenze

Per DRA è necessario un file della chiave di licenza. Questo file contiene le informazioni sulla licenza dell'utente e viene installato nel server di amministrazione. Una volta installato il server di amministrazione, utilizzare l'utility Health Check per installare la licenza acquistata. Se necessaria, nel pacchetto di installazione è inoltre inclusa una chiave di licenza di valutazione (`TrialLicense.lic`) che consente di gestire un numero illimitato di account utente e di caselle postali per 30 giorni.

Per eseguire l'upgrade di una licenza esistente o di valutazione, aprire la Console di delega e configurazione e passare a **Configuration Management** (Gestione configurazione) > **Update License** (Aggiorna licenza). Quando si esegue l'upgrade della licenza, eseguire l'upgrade del file di licenza in ciascun server di amministrazione.

È possibile visualizzare la licenza del prodotto nella Delegation and Configuration Console (Console di delega e configurazione). Per visualizzare la licenza del prodotto, passare a **File** > **DRA Properties** (Proprietà di DRA) > **License** (Licenza).

Configurazione dei server DRA e delle funzioni

La gestione dell'accesso con il minimo privilegio per i task di Active Directory mediante DRA richiede la configurazione di numerosi componenti e processi, fra i quali le configurazioni generali e dei componenti client. In questa sezione vengono fornite informazioni relative ai componenti e ai processi generali che devono essere configurati per DRA.

Configurazione del set multimaster

In un ambiente MMS si utilizzano più server di amministrazione per gestire lo stesso set di domini e server membri. Un MMS è costituito da un server di amministrazione primario e più server di amministrazione secondari.

La modalità di default per il server di amministrazione è quella primaria. Man mano che si aggiungono server secondari all'ambiente MMS, va ricordato che un server di amministrazione secondario può appartenere a un solo set di server.

Affinché ciascun server del set gestisca gli stessi dati, sincronizzare periodicamente i server secondari con il server di amministrazione primario. Per ridurre le attività di manutenzione, utilizzare lo stesso account del servizio per tutti i server di amministrazione della foresta di domini.

Importante

- Quando si installa il server secondario, selezionare **Secondary Administration Server** (Server di amministrazione secondario) nel programma di installazione.
- La versione di DRA del nuovo server secondario deve essere uguale a quella del server primario di DRA affinché tutte le funzioni disponibili nel server primario lo siano anche in quello secondario.

- "Aggiunta di un server di amministrazione secondario" a pagina 89
- "Innalzamento del livello di un server di amministrazione secondario" a pagina 90
- "Abbassamento di livello di un server di amministrazione primario" a pagina 91
- "Pianificazione della sincronizzazione" a pagina 91

Aggiunta di un server di amministrazione secondario

È possibile aggiungere un server di amministrazione secondario a un MMS esistente mediante il client di delega e configurazione.

Nota: per aggiungere un nuovo server secondario, è necessario prima di tutto installare Directory and Resource Administrator nel computer del server di amministrazione. Per ulteriori informazioni, vedere Installazione del server di amministrazione DRA.

Per aggiungere un server di amministrazione secondario:

1. Fare clic con il pulsante destro del mouse su **Administration Servers** (Server di amministrazione) nel nodo Configuration Management (Gestione configurazione) e selezionare **Add Secondary Server** (Aggiungi server secondario).
2. Nella procedura guidata per l'aggiunta di un server secondario, fare clic su Avanti.
3. Nella scheda Secondary server (Server secondario), specificare il nome del server di amministrazione secondario che si desidera aggiungere all'MMS.

4 Nella scheda Access account (Account di accesso), specificare un account di servizio del server di amministrazione secondario. DRA utilizza questo account solo per aggiungere il server di amministrazione secondario all'MMS.

5 Nella scheda Multi-Master access account (Account di accesso multimaster), specificare un account di accesso che deve essere utilizzato dal server di amministrazione primario per le operazioni dell'MMS. Si consiglia di non utilizzare l'account di servizio del server di amministrazione secondario come account di accesso multimaster. È possibile specificare qualsiasi account utente dal dominio associato al server di amministrazione secondario. L'account di accesso multimaster deve far parte del gruppo di amministratori locale sul server secondario. Se l'account di accesso multimaster non dispone di privilegi sufficienti per eseguire operazioni MMS, il server DRA delega automaticamente i poteri necessari all'account di accesso multimaster.

Innalzamento del livello di un server di amministrazione secondario

È possibile alzare il livello di un server di amministrazione secondario facendolo diventare un server di amministrazione primario. Quando si alza di livello un server di amministrazione secondario trasformandolo in un server di amministrazione primario, il server di amministrazione primario esistente diventa un server di amministrazione secondario nel set di server. Per alzare di livello un server di amministrazione secondario, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini). Prima di alzare di livello un server di amministrazione secondario, sincronizzare l'MMS affinché utilizzi la configurazione più recente.

Per informazioni sulla sincronizzazione dell'MMS, vedere Pianificazione della sincronizzazione.

Nota: un server appena trasformato in primario può eseguire la connessione solo ai server secondari che erano disponibili durante il processo di innalzamento del livello. Se durante tale processo un server secondario è diventato non disponibile, contattare il Supporto tecnico.

Per alzare di livello un server di amministrazione secondario:

1 Passare al nodo **Configuration Management** (Gestione configurazione) > **Administration Servers** (Server di amministrazione).

2 Nel riquadro a destra, selezionare il server di amministrazione secondario che si desidera alzare di livello.

3 Nel menu Task, fare clic su **Advanced** (Avanzate) > **Promote Server** (Alza livello server).

Importante: quando l'account del servizio del server secondario è diverso da quello del server primario o il server secondario viene installato in un dominio diverso da quello del server primario (domini attendibili/domini non attendibili) e si alza il livello del server secondario, prima di eseguire l'operazione assicurarsi di delegare i ruoli seguenti: **Audit All Objects**(Revisiona tutti gli oggetti), **Configure Servers and Domains** (Configura server e domini) e **Generate UI Reports** (Genera rapporti UI). Verificare quindi che le sincronizzazioni dell'MMS abbiano esito positivo.

Abbassamento di livello di un server di amministrazione primario

È possibile abbassare il livello di un server di amministrazione primario facendolo diventare un server di amministrazione secondario. Per abbassare il livello di un server di amministrazione primario, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Per abbassare il livello di un server di amministrazione primario:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **Administration Servers** (Server di amministrazione).
2. Nel riquadro a destra, selezionare il server di amministrazione primario che si desidera abbassare di livello.
3. Nel menu Task, fare clic su **Advanced** (Avanzate) > **Demote Server** (Abbassa livello server).
4. Specificare il computer che si desidera designare come nuovo server di amministrazione primario e fare clic su **OK**.

Pianificazione della sincronizzazione

La sincronizzazione assicura che tutti i server di amministrazione dell'MMS utilizzino gli stessi dati di configurazione. Sebbene sia possibile sincronizzare manualmente i server in qualsiasi momento, la pianificazione di default è impostata per sincronizzare l'MMS ogni 4 ore. Tale pianificazione può essere modificata per adattarla alle esigenze aziendali specifiche.

Per modificare la pianificazione della sincronizzazione o sincronizzare manualmente i server dell'MMS, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Per accedere alla pianificazione della sincronizzazione o eseguire la sincronizzazione manuale, passare a **Configuration Management** (Gestione configurazione) > **Administration Servers** (Server di amministrazione) e utilizzare il menu **Task** oppure le opzioni visualizzate facendo clic con il pulsante destro del mouse su un server selezionato. La pianificazione della sincronizzazione è disponibile nelle proprietà del server selezionato.

Caratteristiche delle opzioni di sincronizzazione

Le opzioni per la sincronizzazione dei server MMS sono quattro:

- Selezione del server primario e sincronizzazione di tutti i server secondari mediante "Synchronize All Servers" (Sincronizza tutti i server)
- Selezione di un server secondario e sincronizzazione solo di tale server.
- Configurazione della pianificazione della sincronizzazione dei server primario e secondari in modo indipendente
- Configurazione della pianificazione della sincronizzazione di tutti i server. Questa opzione è abilitata quando nella pianificazione della sincronizzazione del server primario è selezionata l'impostazione seguente:

  Configure secondary Administration servers when refreshing the primary Administration server (Configura i server di amministrazione secondari durante l'aggiornamento del server di amministrazione primario)

Nota: se si deseleziona questa opzione, i file di configurazione vengono copiati nei server secondari in base alla pianificazione del primario, ma vengono caricati in base alla pianificazione configurata nel server secondario e non nello stesso momento. Questa impostazione è utile se i server risiedono in fusi orari diversi. Ad esempio, è possibile configurare tutti i server per aggiornarne la configurazione durante la notte, anche se gli orari potrebbero essere diversi a causa dei fusi orari.

Gestione delle eccezioni di clonazione

Le eccezioni di clonazione consentono di definire proprietà per utenti, gruppi, contatti e computer che non verranno copiate in caso di clonazione di uno di questi oggetti.

Disponendo dei poteri appropriati, è possibile gestire le eccezioni di clonazione. Il ruolo Manage Clone Exceptions (Gestisci eccezioni di clonazione) concede poteri di visualizzazione, creazione ed eliminazione delle eccezioni di clonazione.

Per visualizzare o eliminare un'eccezione di clonazione esistente oppure per creare una nuova eccezione di clonazione, passare a **Configuration Management** (Gestione configurazione) > **Clone Exceptions** (Eccezioni di clonazione) > **Task** o fare clic con il pulsante destro del mouse per visualizzare le opzioni.

Replica di file

Quando si creano strumenti personalizzati, potrebbe essere necessario installare i file di supporto utilizzati da tali strumenti nel computer della Console di delega e configurazione di DRA per poter eseguire lo strumento stesso. È possibile utilizzare le funzionalità di replica dei file di DRA per replicare in modo rapido e semplice i file di supporto degli strumenti personalizzati dal server di amministrazione primario ai server di amministrazione secondari nell'MMS, come anche ai computer client DRA. La replica dei file può essere utile anche per replicare script di attivazione dal server primario a quelli secondari.

Le funzioni Custom Tools (Strumenti personalizzati) e File Replication (Replica file) sono disponibili solo nella Console di delega e configurazione.

Per garantire che i computer client DRA possano accedere ai file degli strumenti personalizzati, è possibile utilizzare contemporaneamente sia strumenti personalizzati che la replica dei file. I file degli strumenti personalizzati vengono replicati nei server di amministrazione secondari affinché i computer client DRA che eseguono la connessione a server di amministrazione secondari possano accedere a tali strumenti personalizzati.

I file degli strumenti personalizzati vengono replicati dal server di amministrazione primario ai server di amministrazione secondari durante il processo di sincronizzazione dell'MMS. Quando i computer client DRA eseguono la connessione ai server di amministrazione, viene effettuato il download dei file degli strumenti personalizzati nei computer client DRA.

Nota: l'ubicazione in cui viene effettuato il download dei file degli strumenti personalizzati nei computer client DRA è:

{DirInstallazioneDRA}`\{ID MMS}\Download`

L'ID MMS è l'identificazione del set multimaster da cui DRA effettua il download dei file degli strumenti personalizzati.

- "Upload di file di strumenti personalizzati per la replica" a pagina 93
- "Replica di più file tra server di amministrazione" a pagina 94
- "Replica di più file nei computer client DRA" a pagina 94

Upload di file di strumenti personalizzati per la replica

Quando si effettua l'upload di file nel server di amministrazione primario, è necessario specificare i file di cui si desidera effettuare l'upload e la replica dal server di amministrazione primario a tutti i server di amministrazione secondari che appartengono all'MMS. In DRA è possibile effettuare l'upload di file di libreria, file script e file eseguibili.

Il ruolo Replicate Files (Replica file) consente di replicare i file dal server di amministrazione primario ai server di amministrazione secondari dell'MMS come anche ai computer client DRA. Il ruolo include i poteri seguenti:

- **Delete Files from Server (Elimina file dal server):** questo potere consente a DRA di eliminare i file che non sono più presenti nel server di amministrazione primario, nei server di amministrazione secondari e nei computer client DRA.
- **Set File Information (Imposta informazioni file):** questo potere consente a DRA di aggiornare le informazioni sui file nei server di amministrazione secondari.
- **Upload Files to Server (Effettua upload dei file nel server):** questo potere consente a DRA di effettuare l'upload di file dal computer client DRA al server di amministrazione primario.

Nota: mediante l'interfaccia utente di replica dei file nella Console di delega e configurazione è possibile effettuare l'upload per la replica di un solo file per volta.

Per effettuare l'upload di un file di uno strumento personalizzato nel server di amministrazione primario:

1. Passare a **Configuration Management** (Gestione configurazione) > **File Replication** (Replica file).
2. Fare clic su **Upload File** (Effettua upload del file) nel menu Task.
3. Per cercare e selezionare il file di cui si desidera effettuare l'upload, fare clic su **Browse** (Sfoglia).
4. *Se si desidera effettuare il download del file selezionato in tutti i computer client DRA*, selezionare la casella di controllo **Download to all client computers** (Effettua download in tutti i computer client).
5. *Se si desidera registrare una libreria COM*, selezionare la casella di controllo **Register COM library** (Registra libreria COM).
6. Fare clic su **OK**.

Nota

- L'upload del file script o dei file di supporto che devono essere replicati in altri server di amministrazione secondari viene effettuato all'interno della cartella *{DirInstallazioneDRA}*\FileTransfer\Replicate del server di amministrazione primario. La cartella *{DirInstallazioneDRA}*\FileTransfer\Replicate è denominata anche *{Percorso_File_Replicati_DRA}*.

- L'upload del file script o dei file di supporto che devono essere replicati nei computer client DRA viene effettuato nella cartella *{DirInstallazioneDRA}*\FileTransfer\Download del server di amministrazione primario.
- Il file dello strumento personalizzato di cui è stato effettuato l'upload nel server di amministrazione primario viene distribuito ai server di amministrazione secondari nel corso della sincronizzazione pianificata o della sincronizzazione manuale successiva.

Replica di più file tra server di amministrazione

Se si desidera effettuare l'upload di più file e replicarli tra server di amministrazione primario e server di amministrazione secondari dell'MMS, è possibile effettuare manualmente l'upload per la replica copiando i file nella directory di replica del server di amministrazione primario, che si trova nell'ubicazione seguente:

{DRAInstallDir}\FileTransfer\Replicate

La directory di replica viene creata al momento dell'installazione di DRA.

Il server di amministrazione identifica automaticamente i file nella directory di replica e li replica tra i server di amministrazione durante la sincronizzazione pianificata successiva. Al termine della sincronizzazione, i file di cui è stato effettuato l'upload vengono visualizzati nella finestra File Replication (Replica di file) della Console di delega e configurazione.

Nota: se si desidera replicare file che contengono librerie COM che devono essere registrate, non è possibile copiarli manualmente nella directory di replica del server di amministrazione. Per effettuare l'upload di ciascun file e registrare la libreria COM, è necessario utilizzare la Console di delega e configurazione.

Replica di più file nei computer client DRA

Se si desidera replicare più file dal server di amministrazione primario ai computer client DRA, è possibile copiarli nella directory di replica del client nel server di amministrazione primario, che si trova nell'ubicazione seguente:

{DRAInstallDir}\FileTransfer\Download

La directory di replica del client viene creata al momento dell'installazione di DRA.

Il server di amministrazione individua automaticamente i file nella cartella Download ed esegue la replica nei server di amministrazione secondari durante la sincronizzazione pianificata successiva. Al termine della sincronizzazione, i file di cui è stato effettuato l'upload vengono visualizzati nella finestra File Replication (Replica di file) della Console di delega e configurazione. Il download dei file replicati nei computer client DRA viene effettuato non appena essi eseguono la connessione ai server di amministrazione dopo la replica.

Nota: se si desidera replicare file che contengono librerie COM che devono essere registrate, non è possibile copiarli nella directory di download del server di amministrazione. Per effettuare l'upload di ciascun file e registrare la libreria COM, è necessario utilizzare la Console di delega e configurazione.

Azure Sync (Sincronizzazione Azure)

Azure Sync (Sincronizzazione Azure) consente di applicare policy relative a caratteri non validi e lunghezze in caratteri per evitare errori di sincronizzazione delle directory. Selezionando questa opzione si avrà la certezza che per tutte le proprietà sincronizzate con Azure Active Directory i caratteri non validi non saranno ammessi e verranno applicati limiti al numero di caratteri.

Per abilitare Azure Sync (Sincronizzazione Azure):

1. Nel riquadro a sinistra fare clic su **Configuration Management** (Gestione configurazione).
2. In Common Tasks (Task comuni) nel riquadro a destra, fare clic su **Update Administration Server Options** (Aggiorna opzioni server di amministrazione).
3. Nella scheda Azure Sync (Sincronizzazione Azure) selezionare **Enforce online mailbox policies for invalid characters and character length** (Applica policy di casella postale online per caratteri non validi e lunghezza dei caratteri).

Abilitazione di più gestori per i gruppi

Quando si abilita il supporto per più gestori per la gestione di un gruppo, uno dei due attributi di default viene utilizzato per memorizzare i gestori del gruppo. Nel caso in cui si utilizzi Microsoft Exchange, l'attributo è `msExchCoManagedByLink`. Nel caso in cui non si utilizzi Microsoft Exchange, l'attributo di default è `nonSecurityMember`. Quest'ultima opzione è modificabile. Tuttavia, se è necessario modificare l'impostazione, si consiglia di contattare il Supporto tecnico per stabilire un attributo appropriato.

Per abilitare il supporto di più gestori per i gruppi:

1. Nel riquadro a sinistra fare clic su **Configuration Management** (Gestione configurazione).
2. In Common Tasks (Task comuni) nel riquadro a destra, fare clic su **Update Administration Server Options** (Aggiorna opzioni server di amministrazione).
3. Nella scheda Enable Support for Group Multiple Managers (Abilita supporto di più gestori per i gruppi), selezionare la casella di controllo **Enable support for group's multiple managers** (Abilita supporto di più gestori per i gruppi).

Comunicazioni cifrate

Questa funzione consente di abilitare o disabilitare l'utilizzo della comunicazione cifrata tra il client di delega e configurazione e il server di amministrazione. Per default, le password degli account sono cifrate in DRA. Questa funzione non esegue la cifratura delle comunicazioni del client Web o di PowerShell, che viene gestita separatamente mediante certificati server.

L'utilizzo delle comunicazioni cifrate può incidere negativamente sulle prestazioni. Per default, le comunicazioni cifrate sono disabilitate. Se si abilita l'opzione, i dati vengono cifrati durante la comunicazione tra le interfacce utente e il server di amministrazione. In DRA si utilizza la cifratura standard Microsoft per Remote Procedure Call (RPC).

Per abilitare le comunicazioni cifrate, passare a **Configuration Management** (Gestione configurazione) > **Update Administration Server Options** (Aggiorna opzioni server di amministrazione) > **General** (Generale) e selezionare la casella di controllo **Encrypted Communications** (Comunicazioni cifrate) nella scheda.

Nota: per cifrare tutte le comunicazioni tra le interfacce utente e il server di amministrazione, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Definizione di attributi virtuali

Mediante gli attributi virtuali è possibile creare nuove proprietà e associarle a utenti, gruppi, gruppi di distribuzione dinamici, contatti, computer e unità organizzative. Gli attributi virtuali consentono di creare nuove proprietà senza che sia necessario estendere lo schema di Active Directory.

Grazie agli attributi virtuali è possibile aggiungere nuove proprietà agli oggetti di Active Directory. Per creare, abilitare, disabilitare, associare e annullare l'associazione degli attributi virtuali è necessario utilizzare il server di amministrazione primario. Gli attributi virtuali creati in AD LDS vengono memorizzati in DRA. Gli attributi virtuali vengono replicati dal server di amministrazione primario ai server di amministrazione secondari durante il processo di sincronizzazione dell'MMS.

Disponendo dei poteri appropriati, è possibile gestire gli attributi virtuali. Il ruolo Manage Virtual Attributes (Gestisci attributi virtuali) assegna i poteri necessari per creare, abilitare, associare, annullare l'associazione, disabilitare e visualizzare gli attributi virtuali.

- “Creazione di attributi virtuali” a pagina 96
- “Associazione di attributi virtuali agli oggetti” a pagina 96
- “Annullamento dell'associazione degli attributi virtuali” a pagina 97
- “Disabilitazione degli attributi virtuali” a pagina 97

Creazione di attributi virtuali

Per creare attributi virtuali è necessario il ruolo *Create Virtual Attributes* (Crea attributi virtuali), mentre per visualizzarli si utilizza il ruolo *View Virtual Attributes* (Visualizza attributi virtuali).

Per creare un attributo virtuale, passare al nodo **Configuration Management** (Gestione configurazione) > **Virtual Attributes** (Attributi virtuali) > **Managed Attributes** (Attributi gestiti) e fare clic su **New Virtual Attribute** (Nuovo attributo virtuale) nel menu Task.

Associazione di attributi virtuali agli oggetti

È possibile associare agli oggetti Active Directory solo attributi virtuali abilitati. Dopo aver associato un attributo virtuale a un oggetto, l'attributo virtuale è disponibile fra le proprietà dell'oggetto stesso.

Per esporre gli attributi virtuali mediante le interfacce utente di DRA, è necessario creare una pagina personalizzata delle proprietà.

Per associare un attributo virtuale a un oggetto, passare al nodo **Configuration Management** (Gestione configurazione) > **Virtual Attributes** (Attributi virtuali) > **Managed Attributes** (Attributi gestiti), fare clic con il pulsante destro del mouse sull'attributo virtuale che si desidera utilizzare e selezionare **Associate** (Associa) > (tipo di oggetto).

Nota

- È possibile associare gli attributi virtuali soltanto a utenti, gruppi, gruppi di distribuzione dinamici, computer, contatti e unità organizzative.
- Quando si associa un attributo virtuale a un oggetto, in DRA vengono creati automaticamente due poteri personalizzati di default, necessari agli amministratori aggiunti per gestire l'attributo virtuale.

Annullamento dell'associazione degli attributi virtuali

L'associazione degli attributi virtuali agli oggetti Active Directory può essere annullata. Per i nuovi oggetti creati, nelle proprietà non viene più visualizzato l'attributo virtuale per cui è stata annullata l'associazione.

Per annullare l'associazione di un attributo virtuale a un oggetto Active Directory, passare al nodo **Configuration Management** (Gestione configurazione) > **Virtual Attributes** (Attributi virtuali) > **Managed Classes** (Classi gestite) > (tipo di oggetto). Fare clic con il pulsante destro del mouse sull'attributo virtuale e selezionare **Disassociate** (Annulla associazione).

Disabilitazione degli attributi virtuali

È possibile disabilitare gli attributi virtuali a condizione che non siano associati a un oggetto Active Directory. Quando si disabilita un attributo virtuale, gli amministratori non possono visualizzarlo né associarlo a un oggetto.

Per disabilitare un attributo virtuale, passare a **Configuration Management** (Gestione configurazione) > **Managed Attributes** (Attributi gestiti). Fare clic con il pulsante destro del mouse sull'attributo desiderato nel riquadro dell'elenco e selezionare **Disable** (Disabilita).

Configurazione della memorizzazione nella cache

Il server di amministrazione crea e gestisce una **cache degli account** in cui sono memorizzate parti di Active Directory per i domini gestiti. La cache degli account viene utilizzata in DRA per migliorare le prestazioni di gestione degli account utente, dei gruppi, dei contatti e degli account computer.

Per pianificare gli orari di aggiornamento della cache o visualizzarne lo stato, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Nota: per eseguire aggiornamenti incrementali della cache degli account in domini che contengono sottoalberi gestiti, verificare che l'account del servizio disponga dell'accesso in lettura per il container Oggetti eliminati, nonché per tutti gli oggetti nel dominio del sottoalbero. Per verificare e delegare le autorizzazioni appropriate, è possibile utilizzare l'utility Deleted Objects.

- “Aggiornamenti completi e incrementali” a pagina 98
- “Intervalli pianificati di default” a pagina 99

Aggiornamenti completi e incrementali

Quando si esegue un aggiornamento incrementale della cache degli account, vengono aggiornati solo i dati modificati dopo l'ultimo aggiornamento. L'aggiornamento incrementale è un metodo semplificato per stare al passo con i continui cambiamenti di Active Directory. Si utilizza per aggiornare rapidamente la cache degli account generando però un impatto minimo sulle attività aziendali.

Importante: Microsoft Server limita a cinque il numero di utenti che possono essere connessi contemporaneamente alla sessione WinRM/WinRS e anche il numero di shell per utente è limitato a cinque. Accertarsi quindi che l'account utente corrispondente sia limitato a cinque shell per i server secondari di DRA.

Un aggiornamento incrementale aggiorna i dati seguenti:

- Oggetti nuovi e clonati
- Oggetti eliminati e spostati
- Appartenenze a gruppi
- Tutte le proprietà memorizzate nella cache per gli oggetti modificati

Con l'aggiornamento completo, invece, viene ricreata la cache degli account di DRA per il dominio specificato.

Nota: quando è in corso un aggiornamento completo della cache degli account, il dominio non è disponibile per gli utenti di DRA.

Esecuzione di un aggiornamento completo della cache degli account

Per aggiornare la cache degli account, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo “Configure Servers and Domains” (Configura server e domini).

Per eseguire immediatamente un aggiornamento completo della cache degli account:

1. Passare a **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini gestiti).
2. Fare clic con il pulsante destro del mouse sul dominio desiderato e selezionare **Properties** (Proprietà).
3. Fare clic su **Refresh Now** (Aggiorna ora) nella scheda **Full refresh** (Aggiornamento completo).

Intervalli pianificati di default

La frequenza di aggiornamento della cache degli account varia a seconda della frequenza dei cambiamenti aziendali. Utilizzare l'aggiornamento incrementale per aggiornare frequentemente la cache degli account, garantendo così che le informazioni su Active Directory in DRA siano le più recenti.

Di default, il server di amministrazione esegue un aggiornamento incrementale della cache degli account agli intervalli seguenti:

Tipo di dominio	Intervallo di aggiornamento pianificato di default
Domini gestiti	Ogni 5 minuti
Domini attendibili	Ogni ora
Tenant di Azure	Ogni 15 minuti

Sebbene non sia possibile pianificare un aggiornamento completo della cache degli account, tale aggiornamento viene eseguito automaticamente in DRA nelle seguenti circostanze:

- Dopo la configurazione iniziale di un dominio gestito.
- Dopo l'upgrade di DRA a una nuova versione completa da una versione precedente.
- Dopo l'installazione di un service pack di DRA.

L'esecuzione di un aggiornamento completo della cache degli account può richiedere alcuni minuti.

Considerazioni

Affinché DRA disponga delle informazioni più recenti, è necessario aggiornare periodicamente la cache degli account. Prima di eseguire o pianificare un aggiornamento della cache degli account, valutare i fattori seguenti:

- Per eseguire un aggiornamento incrementale della cache degli account, l'account del servizio del server di amministrazione o l'account di accesso deve disporre dell'autorizzazione per accedere agli oggetti eliminati nell'istanza di Active Directory del dominio gestito o attendibile.
- Quando DRA esegue un aggiornamento della cache degli account, il server di amministrazione non include i gruppi di sicurezza locali di dominio dai domini attendibili. Poiché la cache non contiene tali gruppi, in DRA non è possibile aggiungere un gruppo di sicurezza locale di dominio dal dominio attendibile a un gruppo locale nel server membro gestito.
- Se si omette un dominio attendibile dall'aggiornamento della cache degli account, il server di amministrazione omette tale dominio anche dall'aggiornamento della configurazione dei domini.
- Se nell'aggiornamento della cache degli account si include un dominio attendibile precedentemente omesso, eseguire un aggiornamento completo della cache degli account per il dominio gestito. Ciò garantisce che la cache degli account nel server di amministrazione del dominio gestito rifletta correttamente i dati di appartenenza ai gruppi nei domini attendibili e gestiti.

- Se si imposta l'intervallo di aggiornamento incrementale della cache degli account su **Mai**, il server di amministrazione esegue solo l'aggiornamento completo della cache degli account. L'aggiornamento completo della cache degli account potrebbe richiedere un po' di tempo, durante il quale non è possibile gestire gli oggetti del dominio.
- DRA non è in grado di determinare automaticamente quando si apportano modifiche mediante altri strumenti, come ad esempio Servizi directory di Microsoft. Le operazioni non eseguite all'interno di DRA possono compromettere l'accuratezza delle informazioni memorizzate nella cache. Ad esempio, se si utilizza un altro strumento per aggiungere una casella postale a un account utente, non è possibile utilizzare Exchange per gestire la casella postale fino a quando la cache degli account non viene aggiornata.
- L'esecuzione di un aggiornamento completo della cache degli account elimina le statistiche degli ultimi login conservate nella cache. Successivamente, il server di amministrazione raccoglie le informazioni sugli ultimi login da tutti i controller di dominio.

Abilitazione della raccolta stampanti di Active Directory

La raccolta stampanti di AD è disabilitata per default. Per abilitarla, passare a **Configuration Management** (Gestione configurazione) > **Update Administration Server Options** (Aggiorna opzioni server di amministrazione) > **General** (Generale) e selezionare la casella di controllo Collect Printers (Raccogli stampanti) nella scheda.

AD LDS

È possibile configurare l'aggiornamento di pulizia di AD LDS affinché venga eseguito in base a una pianificazione per i domini specifici. L'impostazione di default è "Mai". È inoltre possibile visualizzare lo stato di pulizia e informazioni specifiche relative alla configurazione di AD LDS (ADAM).

Per configurare la pianificazione o visualizzare lo stato di pulizia di AD LDS, fare clic con il pulsante destro del mouse sul dominio desiderato nel nodo **Account and Resource Management** (Gestione account e risorse) > **All My Managed Objects** (Tutti i miei oggetti gestiti) e selezionare rispettivamente **Properties** (Proprietà) > **Adlds Cleanup Refresh Schedule** (Pianificazione aggiornamento pulizia AD LDS) o **Adlds Cleanup status** (Stato pulizia AD LDS).

Per visualizzare le informazioni sulla configurazione di AD LDS (ADAM), passare a **Configuration Management** (Gestione configurazione) > **Update Server Options** (Aggiorna opzioni server) > **ADAM Configuration** (Configurazione ADAM).

Gruppo dinamico

Un gruppo dinamico è costituito da membri che variano in base a un set prestabilito di criteri che si configurano nelle proprietà del gruppo. Nelle proprietà del dominio è possibile configurare l'aggiornamento dei gruppi dinamici in base a una pianificazione per i domini specifici. L'impostazione di default è "Mai". È inoltre possibile visualizzare lo stato di aggiornamento.

Per configurare la pianificazione o visualizzare lo stato di aggiornamento dei gruppi dinamici, fare clic con il pulsante destro del mouse sul dominio desiderato nel nodo **Account and Resource Management** (Gestione account e risorse) > **All My Managed Objects** (Tutti i miei oggetti gestiti) e selezionare rispettivamente **Properties** (Proprietà) > **Dynamic group refresh** (Aggiornamento gruppi dinamici) o **Dynamic group status** (Stato gruppi dinamici).

Per ulteriori informazioni sui gruppi dinamici, vedere Gruppi dinamici di DRA.

Configurazione del Cestino

È possibile abilitare o disabilitare il Cestino per ciascun dominio Microsoft Windows o per gli oggetti all'interno di tali domini e configurare i tempi e le modalità di pulizia del Cestino.

Per informazioni dettagliate sull'uso del Cestino, vedere Cestino.

Abilitazione del Cestino

È possibile abilitare il Cestino per domini Microsoft Windows specifici e per gli oggetti all'interno di tali domini. Per default, il Cestino è abilitato per ciascun dominio gestito da DRA e per tutti gli oggetti del dominio stesso. Per abilitare il Cestino è necessario essere membri del gruppo di amministratori o amministratori della configurazione di DRA.

Se nell'ambiente è presente la configurazione riportata di seguito, utilizzare l'utility Recycle Bin per abilitare la funzione:

- DRA gestisce un sottoalbero del dominio.
- L'account del servizio del server di amministrazione o di accesso non dispone dell'autorizzazione per creare il container Cestino, per spostare gli account in questo container e per modificare gli account nel container.

È inoltre possibile utilizzare l'utility Recycle Bin per verificare le autorizzazioni dell'account del servizio del server di amministrazione o di accesso per il container Cestino.

Per abilitare il Cestino, fare clic con il pulsante destro del mouse sul dominio desiderato nel nodo **Recycle Bin** (Cestino) e selezionare **Enable Recycle Bin** (Abilita cestino).

Disabilitazione del Cestino

È possibile disabilitare il Cestino per domini Microsoft Windows specifici e per gli oggetti all'interno di tali domini. Se un Cestino disabilitato contiene account, non è possibile visualizzare, eliminare definitivamente né ripristinare tali account.

Per disabilitare il Cestino è necessario essere membri del gruppo di amministratori di DRA o del gruppo di amministratori aggiunti di configurazione di DRA.

Per disabilitare il Cestino, fare clic con il pulsante destro del mouse sul dominio desiderato nel nodo **Recycle Bin** (Cestino) e selezionare **Disable Recycle Bin** (Disabilita cestino).

Configurazione e pulizia degli oggetti nel Cestino

Per default, la pulizia del Cestino viene eseguita quotidianamente. È possibile modificare la configurazione per pulire il Cestino del dominio ogni x giorni. Durante la pulizia pianificata, vengono eliminati dal Cestino gli oggetti con data antecedente al numero di giorni configurato per ciascun tipo di oggetto. L'impostazione di default per ciascun tipo prevede l'eliminazione degli oggetti con

data antecedente a 1 giorno. È possibile personalizzare il comportamento del processo di pulizia del Cestino disabilitando, abilitando nuovamente e impostando il tempo di permanenza degli oggetti di ciascun tipo.

Per configurare la pulizia del Cestino, selezionare il dominio desiderato nella Console di delega e configurazione e passare alla scheda **Recycle Bin** (Cestino) in **Task** > **Properties** (Proprietà).

Configurazione dei rapporti

Nelle sezioni seguenti sono riportate informazioni concettuali sui rapporti di gestione di DRA e i relativi servizi di raccolta che è possibile abilitare. Per accedere alla procedura guidata di configurazione dei servizi di raccolta, passare a **Configuration Management** (Gestione configurazione) > **Update Reporting Service Configuration** (Aggiorna configurazione servizio di generazione rapporti).

Configurazione del servizio di raccolta di Active Directory

Il servizio di raccolta di Active Directory raccoglie un set di attributi specificato da Active Directory per ciascun utente, gruppo, contatto, computer, unità organizzativa e gruppo di distribuzione dinamico gestito in DRA. Tali attributi vengono memorizzati nel database generazione di rapporti e utilizzati per generare rapporti nell'apposita console.

È possibile configurare il servizio di raccolta di Active Directory specificando gli attributi da raccogliere e memorizzare nel database generazione di rapporti. È anche possibile configurare il server di amministrazione DRA in cui eseguire il servizio di raccolta.

Configurazione del servizio di raccolta di DRA

Il servizio di raccolta di DRA raccoglie informazioni sulla configurazione di DRA e le memorizza nel database generazione di rapporti, utilizzato per generare rapporti nell'apposita console.

Per abilitare il servizio di raccolta di DRA, è necessario specificare in quale server di amministrazione DRA deve essere eseguito. Come best practice, il servizio di raccolta di DRA deve essere pianificato affinché venga eseguito successivamente al servizio di raccolta di Active Directory, negli orari in cui il carico del server è minore o al di fuori del normale orario di lavoro.

Configurazione del servizio di raccolta del tenant di Azure

Il servizio di raccolta del tenant di Azure raccoglie informazioni relative a utenti, contatti e gruppi Azure che vengono sincronizzati con il tenant di Azure Active Directory e memorizza tali informazioni nel database generazione di rapporti, utilizzato per generare rapporti nell'apposita console.

Per abilitare il servizio di raccolta del tenant di Azure, è necessario specificare in quale server di amministrazione DRA tale servizio verrà eseguito.

Nota: il tenant di Azure può eseguire la raccolta solo dopo che il servizio di raccolta di Active Directory del dominio corrispondente ha completato la propria raccolta.

Configurazione del servizio di raccolta dei rapporti di gestione

Il servizio di raccolta dei rapporti di gestione raccoglie informazioni sulla revisione di DRA e le memorizza nel database generazione di rapporti, utilizzato per generare rapporti nell'apposita console. Quando si abilita il servizio di raccolta, è possibile configurare la frequenza di upload dei dati nel database per le query eseguite con lo strumento DRA Reporting.

Questa configurazione richiede che l'account del servizio DRA disponga dell'autorizzazione **sysadmin** in SQL Server per il server di generazione dei rapporti. Le opzioni configurabili sono illustrate di seguito:

- **Audit Export Data Interval (Intervallo di esportazione dei dati di revisione):** intervallo di tempo per l'esportazione dei dati di revisione dal log di traccia DRA (LAS) al database "SMCubeDepot" in SQL Server.
- **Management Report Summarization Interval (Intervallo di riepilogo per i rapporti di gestione):** intervallo di tempo per il trasferimento dei dati di revisione dal database SMCubeDepot al database generazione di rapporti di DRA, dove possono essere oggetto di query eseguite con lo strumento di generazione dei rapporti di DRA.

Raccolta delle statistiche degli ultimi login

È possibile configurare DRA per raccogliere le statistiche degli ultimi login da tutti i controller del dominio gestito. Per abilitare e pianificare la raccolta delle statistiche degli ultimi login, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Per default, la funzione di raccolta delle statistiche degli ultimi login è disabilitata. Se si desidera raccogliere i dati statistici degli ultimi login, è necessario abilitare la funzione. Dopo aver abilitato la raccolta delle statistiche degli ultimi login, è possibile visualizzare quelle di un utente specifico o lo stato della raccolta delle statistiche degli ultimi login.

Per raccogliere le statistiche degli ultimi login:

1. Passare a **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini gestiti).
2. Fare clic con il pulsante destro del mouse sul dominio desiderato e selezionare **Properties** (Proprietà).
3. Fare clic sulla scheda **Last logon schedule** (Pianificazione ultimi login) per configurare la raccolta delle statistiche degli ultimi login.

Delega dei poteri di configurazione del server di Workflow Automation

Per gestire il workflow, assegnare il ruolo di amministrazione del server di Workflow Automation o i seguenti poteri applicabili agli amministratori aggiunti:

- Create Workflow Event and Modify All Properties (Crea evento workflow e modifica tutte le proprietà)
- Delete Workflow Automation Server Configuration (Elimina configurazione del server di Workflow Automation)

- Set Workflow Automation Server Configuration Information (Imposta informazioni di configurazione del server di Workflow Automation)
- Start Workflow (Avvia workflow)
- View All Workflow Event Properties (Visualizza tutte le proprietà degli eventi del workflow)
- View All Workflow Properties (Visualizza tutte le proprietà del workflow)
- View Workflow Automation Server Configuration Information (Visualizza informazioni di configurazione del server di Workflow Automation)

Per delegare i poteri di configurazione del server di Workflow Automation:

1. Fare clic su **Poteri** nel nodo Delegation Management (Gestione delega) e utilizzare la funzione di ricerca degli oggetti per individuare e selezionare i poteri del workflow desiderati.
2. Fare clic con il pulsante destro del mouse su uno dei poteri del workflow e selezionare **Delegate Roles and Powers** (Delega ruoli e poteri).
3. Cercare l'utente, il gruppo o il gruppo di amministratori aggiunti specifico a cui si desidera delegare i poteri.
4. Utilizzare il **selettore oggetti** per trovare e aggiungere gli oggetti desiderati, quindi fare clic su **Roles and Powers** (Ruoli e poteri) nella **procedura guidata**.
5. Fare clic su **ActiveViews** (Viste ActiveView) e usare il **selettore oggetti** per individuare le viste ActiveView che si desidera aggiungere.
6. Fare clic su **Next** (Avanti) e successivamente su **Finish** (Fine) per completare il processo di delega.

Configurazione del server di Workflow Automation

Per utilizzare Workflow Automation in DRA, è necessario installare il motore di Workflow Automation in un server Windows Server e configurare il server di Workflow Automation tramite la Console di delega e configurazione.

Per configurare il server di Workflow Automation:

1. Eseguire il login alla Console di delega e configurazione.

   Per i poteri di Workflow Automation, vedere Delega dei poteri di configurazione del server di Workflow Automation.
2. Espandere **Configuration Management** (Gestione configurazione) > **Integration Servers** (Server di integrazione).
3. Fare clic con il pulsante destro del mouse su **Workflow Automation** e selezionare **New Workflow Automation Server** (Nuovo server di Workflow Automation).
4. Nella procedura guidata **Add Workflow Automation Server** (Aggiungi server di Workflow Automation), specificare i dettagli, ad esempio il nome del server, la porta, il protocollo e l'account di accesso.
5. Verificare la connessione al server e fare clic su **Finish** (Fine) per salvare la configurazione.

Per informazioni sull'installazione del motore di Workflow Automation, vedere la *Workflow Automation Administrator Guide* (Guida all'amministrazione di Workflow Automation) nel sito della documentazione di DRA.

Delega dei poteri di ricerca LDAP

DRA consente di ricercare gli oggetti LDAP nei domini Active Directory locali, ad esempio utenti, contatti, computer, gruppi e unità organizzative dal server LDAP. Il server DRA continua a gestire l'operazione ed è il controller di dominio in cui viene eseguita la ricerca. Utilizzare i filtri di ricerca per eseguire ricerche più efficienti ed efficaci. È inoltre possibile salvare la query di ricerca per un uso futuro ed è possibile condividerla come query pubblica oppure farne un uso personale rendendola privata. È possibile modificare le query salvate. Il ruolo LDAP Advanced Queries (Query avanzate LDAP) fornisce agli amministratori aggiunti i poteri per la creazione e la gestione di query di ricerca LDAP. Per delegare la creazione e la gestione di di query di ricerca LDAP, utilizzare i poteri seguenti:

- Create Private Advanced Query (Crea query avanzata privata)
- Create Public Advanced Query (Crea query avanzata pubblica)
- Delete Public Advanced Query (Elimina query avanzata pubblica)
- Execute Advanced Query (Esegui query avanzata)
- Execute Save Advanced Query (Esegui salvataggio query avanzata)
- Modify Public Query (Modifica query pubblica)
- View Advanced Query (Visualizza query avanzata)

Per delegare i poteri delle query LDAP:

1. Fare clic su **Poteri** nel nodo Delegation Management (Gestione delega) e utilizzare la funzione di ricerca degli oggetti per individuare e selezionare i poteri delle query LDAP avanzate desiderati.
2. Fare clic con il pulsante destro del mouse su uno dei poteri LDAP e selezionare **Delegate Roles and Powers** (Delega ruoli e poteri).
3. Cercare l'utente, il gruppo o il gruppo di amministratori aggiunti specifico a cui si desidera delegare i poteri.
4. Utilizzare il **selettore oggetti** per trovare e aggiungere gli oggetti desiderati, quindi fare clic su **Roles and Powers** (Ruoli e poteri) nella **procedura guidata**.
5. Fare clic su **ActiveViews** (Viste ActiveView) e usare il **selettore oggetti** per individuare le viste ActiveView che si desidera aggiungere.
6. Fare clic su **Next** (Avanti) e successivamente su **Finish** (Fine) per completare il processo di delega.

Per accedere alla funzione di ricerca nella Console Web, passare a **Gestione > LDAP Search** (Ricerca LDAP).

Configurazione della generazione di rapporti della cronologia delle modifiche

DRA consente di delegare le modifiche gestite in un'organizzazione aziendale e Change Guardian (CG) consente di monitorare le modifiche gestite e non gestite che si verificano in Active Directory. L'integrazione tra DRA e CG offre:

- Possibilità di visualizzare l'amministratore aggiunto delegato di DRA che ha apportato una modifica ad Active Directory negli eventi CG per le modifiche apportate tramite DRA.

- Possibilità di visualizzare la cronologia delle modifiche recenti di un oggetto in DRA, sia di quelle apportate tramite DRA che di quelle catturate da CG originate al di fuori di DRA.
- Le modifiche apportate tramite DRA sono designate come modifiche "gestite" in CG.

Per configurare la generazione di rapporti della cronologia delle modifiche di DRA, attenersi alla seguente procedura:

1. Installare l'agente Windows di Change Guardian.
2. Aggiungere una chiave di licenza di Active Directory.
3. Configurare Active Directory.
4. Creare e assegnare una policy Active Directory.
5. Gestire i domini Active Directory.
6. Abilitare la registrazione degli eventi.
7. Configurare la Cronologia modifiche unificata.

Una volta completati tali passaggi per l'installazione di Change Guardian e la configurazione dell'integrazione con DRA e CG, gli utenti possono generare e visualizzare i rapporti della Cronologia modifiche unificata nella console Web.

Per ulteriori informazioni, vedere "Generazione di rapporti di Cronologia modifiche" nella *Directory and Resource Administrator User Guide* (Guida dell'utente di Directory and Resource Administrator).

Installare l'agente Windows di Change Guardian

Prima di iniziare l'integrazione con DRA e CG, installare l'agente Windows Change Guardian. Per ulteriori informazioni, vedere la *Change Guardian Installation and Administration Guide* (Guida all'installazione e all'amministrazione di Change Guardian).

Aggiungere una chiave di licenza di Active Directory

È necessario aggiungere licenze sia per il server e le applicazioni Change Guardian o per i moduli che si intende monitorare. Per ulteriori informazioni, vedere la *Change Guardian Installation and Administration Guide* (Guida all'installazione e all'amministrazione di Change Guardian).

Configurare Active Directory

Per configurare Active Directory per la Cronologia modifiche, fare riferimento alle seguenti sezioni:

Configurazione del log degli eventi di sicurezza

Configurare il log degli eventi di sicurezza in modo che gli eventi di Active Directory vengano registrati nel log degli eventi finché non vengono processati da Change Guardian.

Per configurare il log degli eventi di sicurezza:

1. Eseguire il login come amministratore a un computer del dominio che si desidera configurare.
2. Per aprire la Console Gestione Criteri di gruppo, immettere quanto segue al prompt dei comandi: `gpmc.msc`

3 Aprire **Forest (Foresta) > Domains (Domini)** > *NomeDominio*> **Domain Controllers (controller di dominio)**.

4 Fare clic con il pulsante destro del mouse su **Default Domain Controllers Policy** (Criterio controller di dominio predefiniti), quindi fare clic su **Edit** (Modifica).

Nota: La modifica della policy dei controller del dominio di default è importante perché un oggetto GPO collegato all'unità organizzativa (OU) del controller del dominio (DC) con un ordine di collegamento superiore può ignorare questa configurazione quando si riavvia il computer o si esegue di nuovo `gpUpdate`. Se gli standard aziendali non consentono di modificare la policy dei controller del dominio di default, creare un oggetto GPO per le impostazioni di Change Guardian, aggiungere tali impostazioni all'oggetto GPO e impostarlo in modo che abbia l'ordine di collegamento più alto nell'unità organizzativa dei controller di dominio.

---

5 Espandere **Computer Configuration (Configurazione computer) > Policies (Criteri) > Windows Settings (Impostazioni di Windows) > Security Settings (Impostazioni di sicurezza)**.

6 Selezionare **Event Log** (Registro eventi) e impostare:

- **Maximum security log size** (Dimensione massima registro protezione) a 10240 KB (10 MB) o a un valore superiore
- **Retention method for security log** (Criteri gestione registro protezione) su **Overwrite events as needed** (Sovrascrivi eventi se necessario).

7 Per aggiornare le impostazioni delle policy, eseguire il comando `gpUpdate` dal prompt dei comandi.

Per verificare che la configurazione sia stata eseguita correttamente:

1 Aprire un prompt dei comandi come amministratore del computer.

2 Avviare il Visualizzatore eventi: `eventvwr`

3 In Registri di Windows, fare clic con il pulsante destro del mouse su **Sicurezza** e selezionare **Proprietà**.

4 Assicurarsi che nelle impostazioni sia impostata la dimensione massima del registro di 10240 KB (10 MB) o valore superiore e che sia selezionata l'opzione “Sovrascrivi eventi se necessario”..

Configurazione della revisione AD

Configurare la revisione AD per abilitare la registrazione degli eventi AD nel log degli eventi di sicurezza.

Configurare l'oggetto GPO della policy dei controller del dominio di default tramite Controlla accesso al servizio directory per monitorare sia gli eventi con esito positivo che negativo.

Per configurare la revisione AD:

1 Eseguire il login come amministratore a un computer del dominio che si desidera configurare.

2 Per aprire la Console Gestione Criteri di gruppo, eseguire `gpmc.msc` dal prompt dei comandi.

3 Espandere **Forest (Foresta) > Domains (Domini)** > *NomeDominio*> **Domain Controllers (controller di dominio)**.

4 Fare clic con il pulsante destro del mouse su **Default Domain Controllers Policy** (Criterio controller di dominio predefiniti), quindi fare clic su **Edit** (Modifica).

Nota: La modifica della policy dei controller del dominio di default è importante perché un oggetto GPO collegato all'unità organizzativa (OU) del controller del dominio (DC) con un ordine di collegamento superiore può ignorare questa configurazione quando si riavvia il computer o si esegue di nuovo `gpUpdate`. Se gli standard aziendali non consentono di modificare la policy dei controller del dominio di default, creare un oggetto GPO per le impostazioni di Change Guardian, aggiungere tali impostazioni all'oggetto GPO e impostarlo in modo che abbia l'ordine di collegamento più alto nell'unità organizzativa dei controller di dominio.

5 Espandere **Computer Configuration (Configurazione computer) > Policies (Criteri) > Windows Settings (Impostazioni di Windows) > Security Settings (Impostazioni di sicurezza) > Advanced Audit Policy Configuration (Configurazione avanzata dei criteri di controllo) > Audit Policies (Criteri controllo)**.

   5a Per configurare AD e Criteri di gruppo, in **Account Management** (Gestione account) e **Policy Change** (Modifica criteri), selezionare quanto segue per ciascuna sottocategoria: **Configure the following audit events** (Configura gli eventi di controllo seguenti), **Success** (Operazioni riuscite) e **Failure** (Operazioni non riuscite).

   5b Per configurare solo AD, in **DS Access** (Accesso DS), selezionare quanto segue per ciascuna sottocategoria: **Configure the following audit events** (Configura gli eventi di controllo seguenti), **Success** (Operazioni riuscite) e **Failure** (Operazioni non riuscite).

6 Espandere **Computer Configuration (Configurazione computer) > Policies (Criteri) > Windows Settings (Impostazioni di Windows) > Security Settings (Impostazioni sicurezza) > Local Policies (Criteri locali) > Audit Policy (Criteri controllo)**.

   6a Per ciascuna delle seguenti policy, selezionare **Define these policy settings (Definisci le impostazioni relative ai criteri)**, **Success (Operazioni riuscite)** e **Failure** (Operazioni non riuscite) nella scheda **Security Policy Setting (Impostazione criteri di sicurezza)**:

   - **Audit account management (Controlla gestione degli account)**
   - **Audit directory service access (Controlla accesso al servizio directory)**
   - **Audit policy change (Controlla modifica ai criteri)**

7 Per aggiornare le impostazioni delle policy, eseguire il comando `gpUpdate` dal prompt dei comandi.

Per ulteriori informazioni, vedere *Monitoraggio dei segnali di compromissione di Active Directory* nel sito della documentazione Microsoft

Configurazione della revisione di utenti e gruppi

Configurare la revisione di utenti e gruppi per revisionare le seguenti attività:

- Attività di accesso e fine sessione degli utenti locali e degli utenti Active Directory
- Impostazioni locali degli utenti
- Impostazioni locali dei gruppi

Per configurare la revisione di utenti e gruppi:

1 Eseguire il login come amministratore a un computer del dominio che si desidera configurare.

2 Aprire Microsoft Management Console e selezionare **File > Aggiungi/Rimuovi snap-in**.

3 Selezionare **'Editor oggetti Criteri di gruppo** e fare clic su **Aggiungi**.

4. Nella finestra Selezione oggetto Criteri di gruppo, fare clic su **Sfoglia**.
5. Selezionare **Domain Controllers.*FQDN*** (Controller di dominio.FQDN), dove *FQDN* è il nome di dominio completo per il computer del controller del dominio.
6. Selezionare **Default Domain Controllers Policy** (Criterio controller di dominio predefiniti).
7. In Microsoft Management Console, espandere **Default Domain Controllers Policy (Criterio controller di dominio predefiniti)*FQDN (Nome di dominio completo)* > Computer Configuration (Configurazione computer) > Policies (Criteri) > Windows Settings (Impostazioni di Windows) > Security Settings (Impostazioni di sicurezza) > Local Policies (Criteri locali) > Audit Policies (Criteri controllo)**.
8. In **Audit Account Logon Events** (Controlla eventi accesso account) e **Audit Logon Events** (Controlla eventi di accesso), selezionare **Define these policy settings** (Definisci le impostazioni relative ai criteri), **Success** (Operazioni riuscite) e **Failure** (Operazioni non riuscite).
9. In Microsoft Management Console, espandere **Default Domain Controllers Policy (Criterio controller di dominio predefiniti)*FQDN (Nome di dominio completo)* > Computer Configuration (Configurazione computer) > Policies (Criteri) > Windows Settings (Impostazioni di Windows) > Security Settings (Impostazioni di sicurezza) > Advanced Audit Policy Configuration (Configurazione avanzata dei criteri di controllo) > Audit Policies (Criteri controllo) > Logon/Logoff (Accesso/fine sessione)**.
10. In **Audit Logon** (Controlla Accesso), selezionare**Audit Logon** (Controlla Accesso), **Success** (Operazioni riuscite) e **Failure** (Operazioni non riuscite).
11. In **Audit Logoff** (Controlla Fine sessione), selezionare**Audit Logoff** (Controlla Fine sessione), **Success** (Operazioni riuscite) e **Failure** (Operazioni non riuscite).
12. Per aggiornare le impostazioni delle policy, eseguire il comando `gpupdate /force` dal prompt dei comandi.

Configurazione degli elenchi di controllo dell'accesso di sicurezza

Per monitorare tutte le modifiche degli oggetti attuali e futuri all'interno di Active Directory, configurare il nodo del dominio.

Per configurare i SACL (Security Access Control Lists, Elenchi di controllo dell'accesso di sicurezza):

1. Eseguire il login come amministratore a un computer del dominio che si desidera configurare.
2. Per aprire lo strumento di configurazione ADSI Edit (Modifica ADSI), eseguire `adsiedit.msc` dal prompt dei comandi.
3. Fare clic con il pulsante destro del mouse su **ADSI Edit** (Modifica ADSI) e selezionare **Connect to** (Connetti a).
4. Nella finestra Connection Settings (Impostazioni di connessione), specificare quanto segue:
   - **Name** (Nome) come `Default naming context` (Contesto dei nomi predefinito).
   - **Path** (Percorso) del dominio da configurare.
   - Se si sta eseguendo questo passaggio per la prima volta, selezionare **Default naming context** (Contesto dei nomi predefinito).
   - Se lo si sta eseguendo per la seconda volta, selezionare **Schema**.
   - Se lo si sta eseguendo la terza volta, selezionare **Configuration** (Configurazione).

Nota: Per configurare i punti di connessione per **Default naming context** (Contesto dei nomi predefinito), **Schema** e **Configuration** (Configurazione), è necessario eseguire tre volte la procedura dal Passaggio 4 al Passo 11.

5 In **Connection Point** (Punto di connessione), impostare **Select a well known Naming Context** (Selezionare un contesto dei nomi noto) su **Default naming context** (Contesto dei nomi predefinito).

6 Nella finestra ADSI Edit (Modifica ADSI), espandere **Default naming context** (Contesto dei nomi predefinito).

7 Fare clic con il pulsante destro del mouse sul nodo nel punto di connessione (inizia con DC= o CN=), quindi fare clic su **Properties** (Proprietà).

8 Nella scheda **Security** (Sicurezza), fare clic su**Advanced (Avanzate) > Auditing (Controllo) > Add (Aggiungi)**.

9 In **Applies to** (Si applica a) o **Apply onto** (Applica a), selezionare **This object and all descendant objects** (Questo oggetto e tutti i discendenti).

10 Configurare la revisione per il monitoraggio di tutti gli utenti:

10a Fare clic su **Select a principal** (Seleziona un'entità) e immettereeveryone in **Enter the object name to select** (Immettere il nome dell'oggetto da selezionare).

10b Specificare le seguenti opzioni:

- **Type** (Tipo) come **All** (Tutti)
- Selezionare **Permissions** (Autorizzazioni) come:
  - **Write All Properties** (Scrivi tutte le proprietà)
  - **Delete** (Elimina)
  - **Modify Permissions** (Autorizzazioni di modifica)
  - **Modify Owner** (Proprietario della modifica)
  - **Create All Child Objects** (Crea tutti gli oggetti figlio)

    Gli altri nodi correlati agli oggetti figlio vengono selezionati automaticamente
  - **Delete All Child Objects** (Elimina tutti gli oggetti figlio)

    Gli altri nodi correlati agli oggetti figlio vengono selezionati automaticamente

11 Deselezionare l'opzione **Apply these auditing entries to objects and/or containers within this container only** (Applica queste voci di controllo solo a oggetti e/o contenitori in questo contenitore).

12 Ripetere la procedura dal Passaggio 4 al Passo 11 due o più volte.

Creare e assegnare una policy Active Directory

È possibile creare nuove policy senza impostazioni preconfigurate.

Per creare una policy:

1 Nel Policy Editor (Editor delle policy), selezionare una delle applicazioni, ad esempio Active Directory.

2 Espandere l'elenco delle policy e selezionare il tipo di policy che si desidera creare. Ad esempio, selezionare **Active Directory Policies (Policy Active Directory) > AD Object (Oggetto AD)**.

3 Nella schermata Configuration Policy (Policy di configurazione), apportare le modifiche appropriate.

4 (Condizionale) Se si desidera abilitare immediatamente la policy, selezionare **Enable this policy revision now** (Abilita la revisione policy ora)..

Per assegnare:

1 Fare clic su **CONFIGURATION (CONFIGURAZIONE) > Policies (Criteri) > Assign Policies (Assegna criteri)**.

2 (Condizionale) Per effettuare l'assegnazione a un gruppo di agenti, fare clic su **Agents Groups (Gruppi di agenti)** e **Default Group (Gruppo predefinito)** o **Custom Group (Gruppo personalizzato)**, quindi fare clic sul nome del gruppo.

3 (Condizionale) Per effettuare l'assegnazione a un agente, fare clic su **AGENTS (AGENTI)** e selezionare il nome dell'agente.

4 Fare clic sull'icona in **ASSIGN UNASSIGN (ASSEGNA/ANNULLA ASSEGNAZIONE)**.

5 Selezionare le policy da **POLICY SETS (SET DI CRITERI)**, **POLICIES (CRITERI)** o entrambi, quindi fare clic su **APPLY (APPLICA)**.

Nota: Non è possibile assegnare policy utilizzando gruppi di agenti per i seguenti tipi di risorse: Azure AD, AWS per IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365

Gestire i domini Active Directory

Per configurare un dominio in DRA come dominio gestito, vedere Gestione di domini Active Directory.

Abilitare la registrazione degli eventi in DRA

Quando è abilitata la revisione di AD Domain Services, gli eventi di DRA vengono registrati come se fossero generati dall'account del servizio DRA o dall'account di accesso ai domini, se uno di questi account è configurato. La registrazione degli eventi costituisce un'ulteriore evoluzione di questa funzione, poiché genera un ulteriore evento AD DS che identifica l'amministratore aggiunto che ha eseguito l'operazione.

Affinché tali eventi vengano generati, è necessario configurare la revisione di AD DS e abilitare la registrazione degli eventi nel server di amministrazione DRA. Quando la registrazione degli eventi è abilitata, è possibile visualizzare le modifiche apportate dagli amministratori aggiunti nei rapporti sugli eventi di Change Guardian.

- Per configurare la revisione di AD DS, consultare la documentazione Microsoft *AD DS Auditing Step-by-Step Guide* (Guida dettagliata al controllo di servizi di dominio Active Directory).
- Per configurare l'integrazione con Change Guardian, vedere Configurazione dei server di Cronologia modifiche unificata.
- Per abilitare la registrazione degli eventi, aprire la Console di delega e configurazione come amministratore di DRA ed effettuare le operazioni seguenti:
  1. Passare a **Configuration Management** (Gestione configurazione) > **Update Administration Server Options** (Aggiorna opzioni server di amministrazione) > **Event Stamping** (Registrazione eventi).

2. Selezionare un tipo di oggetto e fare clic su **Update** (Aggiorna).
3. Selezionare un attributo da utilizzare per la registrazione degli eventi relativi a quel tipo di oggetto.

   DRA supporta attualmente la registrazione degli eventi per utenti, gruppi, contatti, computer e unità organizzative.

   È inoltre necessario che gli attributi siano presenti nello schema di Active Directory per ciascun dominio gestito. Questo fattore va tenuto in considerazione quando si aggiungono domini gestiti dopo la configurazione della registrazione degli eventi. Se si aggiungesse un dominio gestito che non contiene un attributo selezionato, le operazioni da tale dominio non verrebbero sottoposte a revisione con i dati di registrazione degli eventi.

   Poiché DRA modifica tali attributi, si dovranno selezionare attributi non utilizzati da DRA o da qualsiasi altra applicazione dell'ambiente in uso.

Per ulteriori informazioni sulla registrazione degli eventi, vedere Caratteristiche della registrazione eventi.

Configurare la Cronologia modifiche unificata

La funzione del server di Cronologia modifiche unificata (UCH, Unified Change History) consente di generare rapporti relativi alle modifiche apportate esternamente a DRA.

Delega dei poteri di configurazione del server di Cronologia modifiche unificata

Per la gestione del server di Cronologia modifiche unificata, assegnare agli amministratori aggiunti il ruolo di amministrazione del server di Cronologia modifiche unificata o i poteri applicabili seguenti:

- Delete Unified Change History Server Configuration (Elimina configurazione del server Cronologia modifiche unificata)
- Set Unified Change History Configuration Information (Imposta informazioni di configurazione di Cronologia modifiche unificata)
- View Unified Change History Configuration Information (Visualizza informazioni di configurazione di Cronologia modifiche unificata)

Per delegare i poteri del server di Cronologia modifiche unificata:

1. Fare clic su **Poteri** nel nodo Delegation Management (Gestione delega) e utilizzare la funzione di ricerca degli oggetti per individuare e selezionare i poteri UCH desiderati.
2. Fare clic con il pulsante destro del mouse su uno dei poteri UHC e selezionare **Delegate Roles and Powers** (Delega ruoli e poteri).
3. Cercare l'utente, il gruppo o il gruppo di amministratori aggiunti specifico a cui si desidera delegare i poteri.
4. Utilizzare il **selettore oggetti** per trovare e aggiungere gli oggetti desiderati, quindi fare clic su **Roles and Powers** (Ruoli e poteri) nella **procedura guidata**.

5 Fare clic su **ActiveViews** (Viste ActiveView) e usare il **selettore oggetti** per individuare le viste ActiveView che si desidera aggiungere.

6 Fare clic su **Next** (Avanti) e successivamente su **Finish** (Fine) per completare il processo di delega.

Configurazione dei server di Cronologia modifiche unificata

Per configurare i server di Cronologia modifiche unificata:

1 Eseguire il login alla Console di delega e configurazione.

2 Espandere **Configuration Management** (Gestione configurazione) > **Integration Servers** (Server di integrazione).

3 Fare clic con il pulsante destro del mouse su **Unified Change History** (Cronologia modifiche unificata) e selezionare **New Unified Change History Server** (Nuovo server di Cronologia modifiche unificata).

4 Specificare il nome o l'indirizzo IP del server di Cronologia modifiche unificata, il numero di porta, il tipo di server e i dettagli dell'account di accesso nella configurazione di Cronologia modifiche unificata.

5 Verificare la connessione al server e fare clic su **Finish** (Fine) per salvare la configurazione.

6 Aggiungere altri server in base alle esigenze.

Accedere ai rapporti di Cronologia modifiche unificata

Per generare e visualizzare i rapporti di Cronologia modifiche unificata sugli oggetti Active Directory tramite Change Guardian, vedere "Generazione di rapporti di Cronologia modifiche" nella *Directory and Resource Administrator User Guide* (Guida dell'utente di Directory and Resource Administrator).

Configurazione dei servizi DRA per un account del servizio gestito del gruppo

Se necessario, è possibile utilizzare un account del servizio gestito del gruppo (gMSA) per i servizi DRA. Per ulteriori informazioni sull'utilizzo di account gMSA, vedere il riferimento Microsoft *Group Managed Service Accounts Overview* (Panoramica sugli account di servizio gestito del gruppo). In questa sezione viene illustrato come configurare DRA per un account gMSA dopo l'aggiunta dell'account ad Active Directory.

Importante: Non utilizzare l'account gMSA come account di servizio durante l'installazione di DRA.

Per configurare il server di amministrazione primario DRA per un account gMSA:

1 Aggiungere l'account gMSA come membro dei seguenti gruppi:

- Gruppo di amministratori locale sul server DRA
- Gruppo AD LDS nel dominio gestito DRA

2 Modificare l'account di login nelle proprietà del servizio per ciascun servizio riportato di seguito all'account gMSA:
   - NetIQ Administration Service (Servizio di amministrazione NetIQ)
   - Servizio Revisione di NetIQ DRA
   - Servizio Cache di NetIQ DRA
   - Servizio Core di NetIQ DRA
   - Archivio log di NetIQ DRA
   - Servizio Replica di NetIQ DRA
   - Servizio Rest di NetIQ DRA
   - Servizio Skype di NetIQ DRA
3 Riavviare tutti i servizi.
4 Delegare il ruolo "Audit all objects" (Revisiona tutti gli oggetti) all'account gMSA eseguendo il seguente comando:

```
Add-DRAAssignments -Identifier "All Objects" -Users "CN=<gMSA_name>,
CN=Managed Service Accounts, DC=MyDomain, DC=corp" -Roles "Audit All
Objects"
```

Per configurare un server di amministrazione secondario DRA per un account gMSA:

1 Installare il server secondario.
2 Sul server primario, assegnare il ruolo **Configure Servers and Domains** (Configura server e domini) alla vista ActiveView **Administration Servers and Managed Domains** (Server di amministrazione e domini gestiti) per l'account di servizio del server secondario.
3 Sul server primario, aggiungere un nuovo server secondario e specificare l'account di servizio del server secondario.
4 Aggiungere l'account gMSA al gruppo di amministratori locale sul server di amministrazione secondario DRA.
5 Sul server secondario, modificare l'account di login di tutti i servizi DRA all'account gMSA e riavviare i servizi DRA.

Configurazione del client di delega e configurazione

Il client di delega e configurazione fornisce l'accesso a task di configurazione e delega per soddisfare esigenze aziendali di gestione che vanno dall'amministrazione distribuita all'applicazione delle policy. Mediante la Console di delega e configurazione è possibile impostare il modello di sicurezza e le configurazioni dei server per gestire in modo efficace le attività aziendali.

Per configurare il client di delega e configurazione:

1 Avviare il client di delega e configurazione e passare a **Configuration Management** (Gestione amministrazione) > **Update Administration Server Options** (Aggiorna opzioni server di amministrazione).
2 Fare clic sulla scheda **Client Options** (Opzioni client) e definire le impostazioni desiderate utilizzando le opzioni di configurazione visualizzate:
   - Consentire agli utenti di effettuare ricerche in base alla vista ActiveView

- Nascondere oggetti di sola origine dagli elenchi della console
- Mostrare oggetti Active Directory avanzati
- Mostrare il comando di sicurezza
- Mostrare le caselle postali condivise e delle risorse quando si effettuano ricerche di utenti
- Impostare per default il suffisso UPN dell'utente sul dominio corrente
- Numero massimo di elementi modificabili per volta (selezione multipla)
- Opzioni di ricerca
- Opzione di ritorno a capo
- Unità dei limiti dello spazio delle caselle postali di Exchange

Configurazione del client Web

È possibile configurare la Console Web per l'autenticazione tramite smart card o l'autenticazione a più fattori, come anche personalizzare il branding con il logo e il titolo dell'applicazione desiderati.

Avvio della Console Web

È possibile avviare la Console Web da qualsiasi computer, dispositivo iOS o Android dotato di un browser Web. Per avviare la Console, specificare l'URL appropriato nel campo dell'indirizzo del browser Web. Ad esempio, se il componente Web è installato nel computer HOUserver, digitare `https://HOUserver/draclient` nel campo dell'indirizzo del browser Web.

Nota: per visualizzare nella Console Web l'account corrente e le informazioni più recenti di Microsoft Exchange, impostare il browser Web affinché verifichi se sono presenti versioni più recenti delle pagine memorizzate nella cache a ogni apertura.

Logout automatico

È possibile definire un incremento di tempo affinché la console Web esegua automaticamente il logout dopo un determinato periodo di inattività, oppure impostare di non eseguire mai il logout automatico.

Per configurare il logout automatico nella console Web, accedere ad **Amministrazione** > **Configurazione** >**Logout automatico**.

Connessione server DRA

È possibile utilizzare una delle seguenti 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)

Per configurare la connessione al server DRA nella console Web, accedere ad **Amministrazione** > **Configurazione** > **Connessione server DRA**.

Autenticazione

In questa sezione sono riportate informazioni per la configurazione dell'autenticazione con smart card, l'autenticazione di Windows e l'autenticazione multifattori tramite l'integrazione con Advanced Authentication.

- "Autenticazione con smart card" a pagina 116
- "Autenticazione di Windows" a pagina 118
- "Autenticazione multifattori con Advanced Authentication" a pagina 119

Autenticazione con smart card

Per configurare la Console Web affinché accetti un utente in base alle credenziali client provenienti dalla sua smart card, è necessario configurare Internet Information Services (IIS) e il file di configurazione dei servizi REST.

Importante: assicurarsi che i certificati nella smart card siano stati installati anche nell'archivio radice dei certificati nel server Web, in quanto IIS deve essere in grado di trovare i certificati corrispondenti a quelli della card.

1 Installare i componenti di autenticazione nel server Web.

1a Avviare Server Manager.

1b Fare clic su **Server Web (IIS)**.

1c Spostarsi nella sezione Servizi ruolo e fare clic su **Aggiungi servizi ruolo**.

1d Passare al nodo dei servizi Ruolo di sicurezza, selezionare **Autenticazione di Windows** e successivamente **Autenticazione mapping certificati client**.

2 Abilitare l'autenticazione nel server Web.

2a Avviare **Gestione IIS**.

2b Selezionare il server Web.

2c Individuare l'icona **Autenticazione** nella sezione IIS e fare doppio clic su di essa.

2d Abilitare "Autenticazione certificati client Active Directory" e "Autenticazione di Windows".

3 Configurare il client DRA.

3a Selezionare il client DRA.

3b Individuare l'icona **Autenticazione** nella sezione IIS e fare doppio clic su di essa.

3c Abilitare "Autenticazione di Windows" e disabilitare "Autenticazione anonima".

4 Abilitare i certificati SSL e client nel client DRA.

4a Individuare l'icona **Servizi SSL** nella sezione IIS e fare doppio clic su di essa.

4b Selezionare **Richiedi SSL** e successivamente **Richiedi** in Certificati client.

Suggerimento: se l'opzione è disponibile, selezionare **Richiedi SSL a 128 bit**.

---

5 Configurare l'applicazione Web dei servizi REST.

5a Selezionare l'applicazione Web dei servizi REST.

5b Individuare l'icona **Autenticazione** nella sezione IIS e fare doppio clic su di essa.

5c Abilitare "Autenticazione di Windows" e disabilitare "Autenticazione anonima".

6 Abilitare SSL e i certificati client nell'applicazione Web dei servizi REST.

6a Individuare l'icona **Servizi SSL** nella sezione IIS e fare doppio clic su di essa.

6b Selezionare **Richiedi SSL** e successivamente **Richiedi** in Certificati client.

Suggerimento: se l'opzione è disponibile, selezionare **Richiedi SSL a 128 bit**.

---

7 Configurare il file del servizio Web WCF.

7a Selezionare l'applicazione Web dei servizi REST e passare a Visualizzazione contenuto.

7b Individuare il file `.svc` e fare clic su di esso con il pulsante destro del mouse.

7c Selezionare **Passa a visualizzazione funzionalità**.

7d Individuare l'icona **Autenticazione** nella sezione IIS e fare doppio clic su di essa.

7e Abilitare "Autenticazione anonima" e disabilitare tutti gli altri metodi di autenticazione.

8 Modificare il file di configurazione dei servizi REST.

8a Aprire il file `C:\inetpub\wwwroot\DRAClient\rest\web.config` utilizzando un editor di testo.

8b Individuare la riga `<authentication mode="None" />` ed eliminarla.

8c Rimuovere il commento dalle righe specificate di seguito:

- Al di sotto della riga `<system.serviceModel>`:

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy">
<endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding"
name="webHttpEndpoint"
contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </
services>
```

- Al di sotto della riga `<serviceDebug includeExceptionDetailInFaults="false"/>`:

```
<serviceAuthorization impersonateCallerForAllOperations="true" /
> <serviceCredentials> <clientCertificate> <authentication
mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```

- Al di sopra della riga `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />`:

```
<bindings> <webHttpBinding> <binding
name="webHttpEndpointBinding"> <security mode="Transport">
<transport clientCredentialType="Certificate" /> </security> </
binding> </webHttpBinding> </bindings>
```

9. Salvare il file e riavviare il server IIS.

Autenticazione di Windows

Per abilitare l'autenticazione di Windows nella Console Web, è necessario configurare Internet Information Services (IIS) e il file di configurazione dei servizi REST.

1. Aprire Gestione IIS.
2. Nel pannello Connessioni, individuare l'applicazione Web dei servizi REST e selezionarla.
3. Nel riquadro a destra, passare alla sezione IIS e fare doppio clic su **Autenticazione**.
4. Abilitare **Autenticazione di Windows** e disabilitare tutti gli altri metodi di autenticazione.
5. Dopo aver abilitato l'autenticazione Windows, l'opzione **Provider** viene aggiunta al menu di scelta rapida e al pannello Azioni sul lato destro della finestra di gestione. Aprire la finestra di dialogo Provider e spostare **NTLM** all'inizio dell'elenco.
6. Utilizzare un editor di testo per aprire il file `C:\inetpub\wwwroot\DRAClient\rest\web.config` e individuare la riga `<authentication mode="None" />`.
7. Modificare `"None"` impostando `"Windows"` e salvare il file.
8. Riavviare il server IIS.

Autenticazione multifattori con Advanced Authentication

Advanced Authentication Framework (AAF) è il nostro pacchetto software di punta che permette di andare oltre i semplici nome utente e password per adottare un metodo più sicuro di protezione delle informazioni sensibili mediante l'autenticazione multifattori.

Advanced Authentication supporta i protocolli di comunicazione seguenti per la sicurezza:

- TLS 1.2 (impostazione di default), TLS 1.1, TLS 1.0
- SSL 3.0

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.

I tipi di categorie o fattori di autenticazione sono tre:

- *Conoscenza*. Questa categoria impone la conoscenza di un'informazione specifica, ad esempio una password o un codice di attivazione.
- *Possesso*. Questa categoria impone il possesso di un dispositivo di autenticazione, ad esempio una smart card o uno smartphone.
- *Corpo*. Questa categoria impone l'utilizzo di una parte del corpo, ad esempio l'impronta digitale, come metodo di verifica.

Ogni fattore di autenticazione contiene almeno un metodo di autenticazione. Un metodo di autenticazione è una tecnica specifica che si utilizza per stabilire l'identità dell'utente, ad esempio mediante un'impronta digitale o una password.

Un processo di autenticazione può essere considerato avanzato se utilizza più tipi di metodi di autenticazione, ad esempio se richiede una password e un'impronta digitale.

Advanced Authentication supporta i metodi di autenticazione seguenti:

- Password LDAP
- Remote Authentication Dial-In User Service (RADIUS)
- Smartphone

Suggerimento: per utilizzare il metodo Smartphone l'utente deve effettuare il download di un'app iOS o Android. Per ulteriori informazioni, vedere la *Advanced Authentication - Smartphone Applications User Guide* (Advanced Authentication - Guida dell'utente delle applicazioni per smartphone), disponibile sul sito Web della documentazione di NetIQ.

Le informazioni riportate nelle sezioni seguenti consentono di configurare la Console Web per l'utilizzo dell'autenticazione multifattori.

Importante: sebbene alcuni dei passaggi descritti nelle sezioni seguenti si eseguano all'interno della Console Web, la maggior parte del processo di configurazione dell'autenticazione multifattori si effettua mediante AAF. Queste procedure presuppongono che AFF sia già stato installato e che la documentazione della guida in linea di AAF sia accessibile.

Aggiunta di archivi ad Advanced Authentication Framework

Il primo passaggio per configurare la Console Web consiste nell'utilizzare l'autenticazione a più fattori in modo da aggiungere ad AFF tutti i domini Active Directory che contengono gli amministratori di DRA e gli amministratori aggiunti gestiti da DRA. Questi domini sono denominati archivi e contengono gli attributi di identità degli utenti e dei gruppi che si desidera autenticare.

1. Eseguire il login al portale di amministrazione di AAF con nome utente e password di livello amministrativo.
2. Spostarsi nel pannello a sinistra e fare clic su **Archivi**.
3. Fare clic su **Aggiungi**.
4. Compilare il modulo.

   Suggerimento: **Tipo LDAP** è **AD**.

   Suggerimento: digitare nome utente e password di un livello amministrativo nei campi corrispondenti.
5. Fare clic su **Add server** (Aggiungi server).
6. Digitare l'indirizzo IP del server LDAP nel campo **Indirizzo**.
7. Fare clic su **Salva**.
8. Ripetere i passaggi da 3 a 7 per tutti gli altri archivi AD gestiti da DRA.
9. Per ogni archivio elencato nella pagina Archivi, fare clic su **Sincronizza ora** per eseguire la sincronizzazione con il server AAF.

Creazione di catene di autenticazione

Una catena di autenticazione è costituita da almeno un metodo di autenticazione. I metodi della catena vengono richiamati nell'ordine in cui sono stati aggiunti alla catena stessa. Affinché un utente possa eseguire l'autenticazione, deve superare tutti i metodi della catena. Ad esempio, è possibile creare una catena contenente i metodi Password LDAP ed SMS. Quando un utente tenta di eseguire l'autenticazione mediante questa catena, deve innanzitutto eseguire l'autenticazione utilizzando la password LDAP e, successivamente, riceverà un SMS sul proprio cellulare con una password OTP. Immettendo la password, avrà soddisfatto i requisiti di tutti i metodi della catena e l'autenticazione avrà esito positivo. Le catene di autenticazione possono essere assegnate a un utente specifico o a un gruppo.

Per creare una catena di autenticazione:

1. Eseguire il login al portale di amministrazione di AAF con nome utente e password di livello amministrativo.
2. Aprire il pannello a sinistra e fare clic su **Catene**. Nel pannello a destra viene visualizzato l'elenco delle catene attualmente disponibili.
3. Fare clic su **Aggiungi**.
4. Compilare il modulo. Tutti i campi sono obbligatori.

Importante: aggiungere i metodi nell'ordine in cui devono essere richiamati, vale a dire che se si desidera che l'utente immetta prima di tutto una password LDAP, aggiungere Password LDAP come primo elemento della catena.

Importante: verificare che lo switch **Applica se utilizzata da proprietario endpoint** sia impostato su OFF.

5 Impostare **È abilitato** su ON.

6 Digitare i nomi dei ruoli o dei gruppi oggetto della richiesta di autenticazione nel campo **Ruoli e gruppi**.

Suggerimento: Se si desidera che la catena venga applicata a tutti gli utenti, digitare `all users` (tutti gli utenti) nel campo **Roles & Groups** (Ruoli e gruppi) e selezionare **All Users** (Tutti gli utenti) nell'elenco a discesa risultante.

Tutti gli eventuali utenti o gruppi selezionati vengono aggiunti sotto il campo **Ruoli e gruppi**.

7 Fare clic su **Salva**.

Creazione di eventi di autenticazione

Gli eventi di autenticazione vengono attivati da un'applicazione, in questo caso la Console Web, che intende autenticare un utente. È necessario assegnare all'evento almeno una catena di autenticazione, affinché quando l'evento viene attivato, i metodi della catena associata all'evento vengano richiamati per autenticare l'utente.

Un endpoint è un dispositivo, ad esempio un computer o uno smartphone, in cui viene eseguito il software che attiva l'evento di autenticazione. Dopo aver creato l'evento, DRA registra l'endpoint in AAF.

È possibile utilizzare la casella della white list Endpoint per limitare l'accesso a un evento a endpoint specifici, oppure è possibile consentire a tutti gli endpoint di accedere all'evento.

Per creare un evento di autenticazione:

1 Eseguire il login al portale di amministrazione di AAF con nome utente e password di livello amministrativo.

2 Aprire il pannello a sinistra e fare clic su **Eventi**. Nel pannello a destra viene visualizzato l'elenco degli eventi attualmente disponibili.

3 Fare clic su **Aggiungi**.

4 Compilare il modulo. Tutti i campi sono obbligatori.

Importante: verificare che lo switch **È abilitato** sia impostato su ON.

5 Se si desidera limitare l'accesso a endpoint specifici, aprire la sezione della white list Endpoint e spostare gli endpoint desiderati dall'elenco *Disponibili* all'elenco *Utilizzati*.

Suggerimento: se non sono presenti endpoint nell'elenco *Utilizzati*, l'evento sarà disponibile per tutti gli endpoint.

Abilitazione della Console Web

Dopo aver configurato le catene e gli eventi è possibile eseguire il login alla Console Web come amministratore e abilitare Advanced Authentication.

Dopo aver eseguito l'abilitazione, tutti gli utenti dovranno effettuare l'autenticazione tramite AAF per poter accedere alla Console Web.

Importante: prima di abilitare la Console Web è necessario aver eseguito la registrazione nei metodi di autenticazione che la Console Web utilizzerà per autenticare gli utenti. Per indicazioni su come eseguire la registrazione dei metodi di autenticazione, vedere la *Advanced Authentication - Tenant Administration Guide* (Advanced Authentication - Guida all'amministrazione dei tenant).

Per abilitare Advanced Authentication, eseguire il login alla Console Web e passare ad **Amministrazione** > **Configurazione** > **Advanced Authentication**. Selezionare la casella di controllo **Abilitato** e configurare il modulo in base alle istruzioni fornite per ciascun campo.

Suggerimento: dopo aver salvato la configurazione, l'endpoint viene creato in AAF. Per visualizzarlo o modificarlo, eseguire il login al portale di amministrazione di AAF con un nome utente e una password di livello amministrativo e fare clic su **Endpoint** nel riquadro a sinistra.

Passaggi finali

1. Eseguire il login al portale di amministrazione di AAF con un nome utente e una password di livello amministrativo e fare clic su **Eventi** nel riquadro a sinistra.
2. Per modificare gli eventi della Console Web:
   - **2a** Aprire l'evento per la modifica.
   - **2b** Passare alla sezione della white list Endpoint e spostare l'endpoint creato durante la configurazione della Console Web dall'elenco **Disponibili** all'elenco **Utilizzati**. In questo modo solo la Console Web potrà utilizzare tali eventi.
3. Fare clic su **Salva**.

12 Connessione di sistemi gestiti

In questa sezione vengono fornite informazioni per eseguire la connessione e la configurazione di sistemi gestiti relativi a domini e componenti di Microsoft Exchange quali cartelle pubbliche, Exchange, Office 365 e Skype for Business Online.

Gestione di domini Active Directory

È possibile aggiungere nuovi domini e computer gestiti mediante il client di delega e configurazione dopo aver installato il server di amministrazione. È anche possibile aggiungere sottoalberi e domini attendibili, oltre che configurare i relativi account di accesso di Exchange e dominio. Per aggiungere domini e computer gestiti, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Nota: dopo aver aggiunto i domini gestiti, verificare che le pianificazioni degli aggiornamenti della cache degli account per tali domini siano corrette.

Aggiunta di domini e computer gestiti

Per aggiungere un dominio o un computer gestito:

1 Passare a **Configuration Management** (Gestione configurazione) > **New Managed Domain** (Nuovo dominio gestito).

2. Specificare il componente che si desidera aggiungere selezionando il pulsante di scelta corrispondente e specificando il nome del dominio o del computer:
   - **Gestire un dominio**
     - Se si desidera gestire il sottoalbero di un dominio, vedere Aggiunta di un sottoalbero gestito.
     - Se si aggiunge un nuovo dominio con il protocollo LDAP sicuro abilitato sui controller di dominio e si desidera che DRA utilizzi SSL per comunicare con i controller di dominio, selezionare **This domain is configured for LDAP over SSL** (Questo dominio è configurato per LDAP su SSL). Per ulteriori informazioni, vedere Configurazione di DRA per l'esecuzione di Active Directory in modalità protetta.
   - **Gestire un computer**

   Fare clic su **Next** (Avanti) dopo aver completato la configurazione.
3. Nella scheda **Domain access** (Accesso al dominio), specificare le credenziali dell'account che si desidera utilizzare per l'accesso al dominio o al computer in DRA. Per default, DRA utilizza l'account del servizio del server di amministrazione.
4. Verificare il riepilogo e fare clic su **Finish** (Fine).
5. Per iniziare a gestire gli oggetti del dominio o del computer, aggiornare la configurazione del dominio.

Definizione di account di accesso ai domini

Per ciascun dominio o sottoalbero gestito, è possibile specificare un account da utilizzare per l'accesso come alternativa all'account del servizio del server di amministrazione. Questo account alternativo è detto account di accesso. Per configurare un account di accesso, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Per specificare un account di accesso per un server membro, è necessario disporre dell'autorizzazione per gestire il dominio in cui risiede il membro. È possibile gestire i membri di un dominio solo se risiedono all'interno di un dominio gestito a cui è possibile accedere tramite il server di amministrazione.

Per specificare un account di accesso:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini Gestiti).
2. Fare clic con il pulsante destro del mouse sul dominio o sul sottoalbero per cui si desidera specificare un account di accesso, quindi fare clic su **Properties** (Proprietà).
3. Nella scheda Domain access account (Account di accesso al dominio), fare clic su **Use the following account to access this domain** (Usa l'account seguente per accedere a questo dominio).
4. Specificare e confermare le credenziali dell'account e fare clic su **OK**.

Per informazioni su come configurare questo account di minimo privilegio, vedere Account di accesso DRA con minimo privilegio.

Definizione di account di accesso a Exchange

Per ciascun dominio, in DRA è possibile gestire gli oggetti di Exchange utilizzando l'account di accesso al dominio di DRA o un account di accesso a Exchange separato. Per configurare un account di accesso a Exchange, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Importante: Microsoft Server limita a cinque il numero di utenti che possono essere connessi contemporaneamente alla sessione WinRM/WinRS e anche il numero di shell per utente è limitato a cinque. Accertarsi quindi che l'account utente corrispondente sia limitato a cinque shell per i server secondari di DRA.

Per specificare un account di accesso a Exchange:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini Gestiti).
2. Fare clic con il pulsante destro del mouse sul dominio o sul sottoalbero per cui si desidera specificare un account di accesso, quindi fare clic su **Properties** (Proprietà).
3. Nella scheda Exchange access account (Account di accesso a Exchange), fare clic su **Use the following account to access all Exchange servers** (Usa l'account seguente per accedere a tutti i server Exchange).
4. Specificare e confermare le credenziali dell'account e fare clic su **OK**.

Per informazioni su come configurare questo account di minimo privilegio, vedere Account di accesso DRA con minimo privilegio.

Aggiunta di un sottoalbero gestito

Dopo aver installato il server di amministrazione, è possibile aggiungere sottoalberi gestiti e mancanti da domini Microsoft Windows specifici. Per aggiungere un sottoalbero gestito, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Per informazioni sulle versioni supportate di Microsoft Windows, vedere Requisiti del server di amministrazione DRA e della console Web.

Tramite la gestione di un sottoalbero di un dominio Windows, è possibile utilizzare DRA per mettere in sicurezza un reparto o una divisione all'interno di un dominio aziendale più ampio.

Ad esempio, è possibile specificare il sottoalbero Houston nel dominio SOUTHWEST, così che DRA possa gestire in modo sicuro solo gli oggetti contenuti dell'unità organizzativa Houston e nelle sue unità organizzative secondarie. Questa flessibilità permette di gestire uno o più sottoalberi senza dover disporre di autorizzazioni amministrative per l'intero dominio.

Nota

- Per verificare che l'account specificato disponga delle autorizzazioni per gestire il sottoalbero ed eseguire aggiornamenti incrementali della cache degli account, utilizzare l'utility Deleted Objects per verificare e delegare le autorizzazioni appropriate.
- Dopo aver aggiunto i sottoalberi gestiti, verificare che le pianificazioni degli aggiornamenti della cache degli account per i domini corrispondenti siano corrette.

Per aggiungere un sottoalbero gestito:

1. Passare a **Configuration Management** (Gestione configurazione) > **New Manage Domain** (Nuovo dominio gestito).
2. Nella scheda Domain or server (Dominio o server), fare clic su **Manage a domain** (Gestisci un dominio) e specificare il dominio del sottoalbero che si desidera gestire.
3. Specificare il dominio del sottoalbero che si desidera gestire.
4. Selezionare **Manage a subtree of this domain** (Gestisci un sottoalbero di questo dominio) e fare clic su **Next** (Avanti).
5. Nella scheda Subtrees (Sottoalberi), fare clic su **Add** (Aggiungi) per specificare il sottoalbero che si desidera gestire. È possibile specificare più di un sottoalbero.
6. Nella scheda Account di accesso, specificare le credenziali dell'account che si desidera utilizzare per l'accesso al sottoalbero in DRA. Per default, DRA utilizza l'account del servizio del server di amministrazione.
7. Verificare il riepilogo e fare clic su **Finish** (Fine).
8. Per iniziare a gestire gli oggetti del sottoalbero, aggiornare la configurazione del dominio.

Aggiunta di un dominio attendibile

I domini attendibili consentono l'autenticazione utente a sistemi gestiti in tutto l'ambiente gestito. Dopo aver aggiunto un dominio attendibile, è possibile specificare account di accesso al dominio e a Exchange, pianificare aggiornamenti della cache ed eseguire altre azioni sulle proprietà del dominio, proprio come nel caso di un dominio gestito.

Per aggiungere un dominio attendibile:

1. Nel nodo **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini gestiti), selezionare il dominio gestito con un dominio attendibile associato.
2. Fare clic su **Trusted domains** (Domini attendibili) nel riquadro Dettagli. Il riquadro Details (Dettagli) deve essere attivato nel menu Visualizza.
3. Fare clic con il pulsante destro del mouse sul dominio attendibile e selezionare **Properties** (Proprietà).
4. Deselezionare **Ignore this trusted domain** (Ignora questo dominio attendibile) e applicare le modifiche desiderate.

Nota: L'aggiunta di un dominio attendibile avvia un aggiornamento completo della cache degli account, con l'invio di una notifica dell'operazione mediante un prompt di conferma quando si fa clic su **Apply** (Applica).

Configurazione di DRA per l'esecuzione di Active Directory in modalità protetta

Active Directory in modalità protetta viene definito da un ambiente DRA configurato per l'esecuzione tramite protocollo LDAPS (LDAP su SSL) per cifrare le comunicazioni tra DRA e Active Directory, in modo da garantire un ambiente più protetto.

Per utilizzare Active Directory in modalità protetta, durante l'upgrade a una versione di DRA 10.x da una versione 9.x, è necessario che LDAPS venga abilitato dopo l'upgrade. Per questa funzione è anche necessario configurare la funzione di rilevazione automatica per il rilevamento e la connessione ai server DRA e REST.

Abilitazione di LDAP su SSL (LDAPS)

Se si esegue l'upgrade a DRA 10.x da una versione 9.x, eseguire le operazioni riportate di seguito. Se si sta configurando DRA per una nuova installazione, vedere Aggiunta di domini e computer gestiti.

1. Passare a **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini gestiti) nella Console di delega e configurazione di DRA.
2. Fare clic con il pulsante destro del mouse sul dominio e selezionare Proprietà.
3. Nella scheda Generale, abilitare **This domain is configured for LDAP over SSL** (Questo dominio è configurato per LDAP su SSL), quindi fare clic su **OK**.
4. Riavviare NetIQ Administration Service (Servizio di amministrazione NetIQ).

Nota: Se si sta configurando anche la rilevazione automatica per l'utilizzo di per l'utilizzo di Active Directory in modalità protetta, è possibile attendere il riavvio dei servizi dopo il completamento della configurazione. Per ulteriori informazioni, vedere Configurazione della rilevazione automatica per LDAPS.

Configurazione della rilevazione automatica per LDAPS

La rilevazione automatica è il meccanismo usato dal client per la connessione automatica all'ambiente DRA disponibile.

Per configurare DRA per un ambiente in cui è in esecuzione per l'utilizzo di Active Directory in modalità protetta, configurare la chiave di registro `ClientSSLAllDomains`:

1. Avviare l'utility Editor del Registro di sistema.
2. Fare clic con il pulsante destro del mouse sul nodo `HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions`.
3. Selezionare **Nuovo** > **Valore DWORD (32 bit)**.
4. Denominare la nuova chiave `ClientSSLAllDomains`.
5. Impostare il valore della chiave di registro a 1.
6. Dopo aver aggiunto la chiave di registro `ClientSSLAllDomains`, riavviare i seguenti servizi:
   - Servizio Publishing World Wide Web
   - Servizio Rest di NetIQ DRA

Connessione alle cartelle pubbliche

Con DRA è possibile gestire le cartelle pubbliche di Microsoft Exchange. Configurando i domini della foresta delle cartelle pubbliche e concedendo poteri agli amministratori aggiunti, è possibile utilizzare DRA per gestire alcune proprietà delle cartelle pubbliche.

Importante: per gestire l'amministrazione delle cartelle pubbliche, è necessario innanzitutto abilitare il supporto per Microsoft Exchange in DRA e disporre dei poteri applicabili.

- Per informazioni sull'abilitazione del supporto per Microsoft Exchange, vedere Abilitazione di Microsoft Exchange.
- Per informazioni sulle autorizzazioni degli account, vedere Account di accesso DRA con minimo privilegio.

Per configurare il supporto per le cartelle pubbliche di Exchange:

1. Fare clic con il pulsante destro del mouse su **Managed Public Folder Forests** (Foreste cartelle pubbliche gestite) nel nodo Configuration and Management (Configurazione e gestione) e successivamente su **New Public Folder Forest** (Nuova foresta cartelle pubbliche).
2. Fare clic su **Forest Domain** (Dominio foresta), specificare la foresta Active Directory in cui sono ubicati gli oggetti delle cartelle pubbliche e fare clic su **Next** (Avanti).
3. In **Domain access** (Accesso al dominio), specificare l'account di accesso.

   Importante: se si utilizza il server secondario, l'opzione **Use the Primary Administration Server domain access account** (Usa l'account con accesso al dominio del server di amministrazione primario) risulterà disponibile.

   ---
4. In **Exchange access** (Accesso a Exchange), specificare l'account che si desidera utilizzare in DRA per l'accesso sicuro ai server Exchange.

   Importante: se si utilizza il server secondario, l'opzione **Use the Primary Administration Server Exchange access account** (Usa l'account di accesso a Exchange del server di amministrazione primario) risulterà disponibile.

   ---
5. In **Exchange server** (Server Exchange), selezionare il server Exchange che si desidera utilizzare in DRA per la gestione delle cartelle pubbliche.
6. In **Summary** (Riepilogo), verificare i dettagli dell'account e del server Exchange, quindi fare clic su **Finish** (Fine) per completare il processo.

   Il server DRA esegue un aggiornamento completo della cache degli account per le cartelle pubbliche. La nuova foresta delle cartelle pubbliche verrà visualizzata nella console al termine dell'aggiornamento della cache, che potrebbe richiedere alcuni minuti.

Nota: è possibile rimuovere un dominio selezionato di una foresta di cartelle pubbliche dal menu **Task** o dal menu di scelta rapida.

- "Visualizzazione e modifica delle proprietà del dominio delle cartelle pubbliche" a pagina 129
- "Delega dei poteri delle cartelle pubbliche" a pagina 129

Visualizzazione e modifica delle proprietà del dominio delle cartelle pubbliche

Per visualizzare o modificare le proprietà del dominio delle cartelle pubbliche:

1. Fare clic su **Managed Public Folder Forests** (Foreste cartelle pubbliche gestite) nel nodo Configuration Management (Gestione configurazione) per visualizzare le cartelle pubbliche.
2. Fare clic con il pulsante destro del mouse sull'account delle cartelle pubbliche che si desidera visualizzare e selezionare **Properties** (Proprietà).
3. Nelle proprietà di **Public Folder Forest** (Foresta cartelle pubbliche), è possibile eseguire le operazioni seguenti:
   - **General (Generale):** consente di visualizzare i dettagli dell'account delle cartelle pubbliche e aggiornare il campo **Server Exchange**, utilizzato dal server DRA per eseguire attività di Exchange nel server cartelle pubbliche.
   - **Statistics (Statistiche):** consente di visualizzare il numero di cartelle pubbliche e il numero di cartelle pubbliche abilitate per la posta.
   - **Incremental Status (Stato incrementale):** consente di visualizzare o aggiornare lo stato incrementale della cache degli account.
   - **Incremental schedule (Pianificazione incrementale):** consente di visualizzare la pianificazione incrementale dell'aggiornamento della cache e pianificare nuovamente un aggiornamento della cache.
   - **Full status (Stato completo):** consente di visualizzare lo stato completo di aggiornamento della cache degli account.
   - **Full refresh (Aggiornamento completo):** consente di eseguire immediatamente un aggiornamento completo della cache degli account.

     NetIQ consiglia di eseguire un **aggiornamento completo** solo se i dati della cache delle cartelle pubbliche sono danneggiati.
   - **Domain access (Accesso al dominio):** consente di visualizzare i dettagli dell'account del servizio DRA o ignorare gli account di accesso.
   - **Exchange access (Accesso a Exchange):** consente di visualizzare o aggiornare l'accesso sicuro ai server Exchange.

Delega dei poteri delle cartelle pubbliche

Mediante le viste ActiveView è possibile definire i poteri e gestire la delega delle cartelle pubbliche. È possibile specificare le regole per aggiungere oggetti gestiti, scegliere domini e assegnare poteri, per poi delegare i poteri delle cartelle pubbliche agli amministratori aggiunti.

Per creare una vista ActiveView e delegare i poteri delle cartelle pubbliche:

1. Nel nodo **Delegation Management** (Gestione delega), fare clic su **ActiveViews** (Viste ActiveView).
2. Fare clic su **Next** (Avanti) nella **procedura guidata > Create ActiveView** (Crea vista ActiveView), selezionare la regola desiderata nell'elenco a discesa **Add** (Aggiungi) e scegliere Public Folders (Cartelle pubbliche) come tipo di oggetto. Ad esempio, per creare una regola di corrispondenza oggetti, selezionare **Objects that match a rule** (Oggetti che corrispondono alla regola) e scegliere **Public Folders** (Cartelle pubbliche) come tipo di oggetto.

3. Specificare la regola ActiveView che si desidera aggiungere alla cartella pubblica e fare clic su **Next** (Avanti).
4. Specificare il nome della vista ActiveView e fare clic su **Finish** (Fine).
5. Fare clic con il pulsante destro del mouse su **ActiveViews** (Viste ActiveView), passare a **Delegate Administration** (Delega amministrazione) > **Assistant Admins** (Amministratori aggiunti) e scegliere il tipo di amministratore nell'elenco a discesa **Add** (Aggiungi) della **procedura guidata**.
6. Cercare l'utente, il gruppo o il gruppo di amministratori aggiunti specifico a cui si desidera delegare i poteri.
7. Utilizzare il **selettore oggetti** per trovare e aggiungere gli oggetti desiderati, quindi fare clic su **Roles and Powers** (Ruoli e poteri) nella **procedura guidata**.
8. Selezionare **Roles** (Ruoli) nell'elenco a discesa **Add** (Aggiungi), quindi cercare e aggiungere il ruolo di amministratore delle cartelle pubbliche.
9. Selezionare Powers (Poteri) nell'elenco a discesa **Add** (Aggiungi), quindi individuare e aggiungere eventuali poteri aggiuntivi che si desidera assegnare agli amministratori aggiunti che non fanno parte del ruolo di amministratore delle cartelle pubbliche.
10. Fare clic su **Next** (Avanti) e successivamente su **Finish** (Fine) per completare il processo di delega.

Una volta completata la delega dei poteri delle cartelle pubbliche, gli utenti autorizzati potranno eseguire operazioni di creazione, lettura, aggiornamento ed eliminazione delle proprietà delle cartelle pubbliche nei domini configurati tramite la Console Web.

Abilitazione di Microsoft Exchange

L'abilitazione di Microsoft Exchange consente di sfruttare le funzioni di Exchange e Exchange Online, incluse le policy di Microsoft Exchange, la casella postale integrata e la gestione degli oggetti abilitati per la posta. È possibile abilitare o disabilitare il supporto di Microsoft Exchange in ciascun server di amministrazione per Microsoft Exchange Server 2013 e versioni successive.

Per abilitare Exchange è necessario disporre dei privilegi richiesti, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), inoltre la licenza deve includere il supporto per Exchange. Per ulteriori informazioni sui requisiti di Microsoft Exchange, vedere Piattaforme supportate.

Per abilitare il supporto di Microsoft Exchange e Exchange Online:

1. Nella Console di delega e configurazione, passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange).
2. Selezionare **Enable Exchange Policy** (Abilita policy di Exchange) e fare clic su **Apply** (Applica).

Configurazione dei tenant di Azure

DRA consente di gestire i tenant di Azure utilizzando l'autenticazione di base o l'autenticazione a più fattori mediante certificati.

Con uno o più tenant di Azure, è possibile configurare DRA in modo da interagire con Azure Active Directory per la gestione degli oggetti Azure. Questi oggetti includono utenti, utenti guest, contatti e gruppi creati in Azure e utenti, contatti e gruppi sincronizzati con il tenant di Azure dai domini gestiti DRA.

L'amministratore DRA o un amministratore aggiunto con il ruolo delegato "Configure Servers and Domains" (Configura server e domini) è in grado di gestire i tenant di Azure. I ruoli integrati di Azure sono necessari per gestire gli oggetti Azure nella console Web.

I moduli Azure PowerShell, Azure Active Directory, Azure Resource Manager Profile ed Exchange Online sono necessari per la gestione dei task Azure. Per ulteriori informazioni, vedere Piattaforme supportate.

È inoltre necessario disporre di un account in Azure Active Directory. Per ulteriori informazioni sulle autorizzazioni dell'account di accesso tenant di Azure, vedere Account di accesso DRA con minimo privilegio.

Nella Delegation and Configuration Console (Console di delega e configurazione) è possibile eseguire i task di configurazione riportati di seguito. Le operazioni sugli oggetti Azure vengono eseguite solo nella console Web. Per ulteriori informazioni, vedere Gestione degli oggetti Azure nella Guida dell'utente di NetIQ Directory and Resource Administrator.

Aggiunta di un nuovo tenant di Azure

Per gestire un nuovo tenant di Azure è necessario creare un'applicazione Azure offline utilizzando lo script PowerShell fornito da DRA. DRA concede automaticamente le autorizzazioni necessarie all'applicazione Azure per gestire gli oggetti nel tenant. Per un elenco delle autorizzazioni necessarie per l'applicazione Azure, vedere Account di accesso DRA con minimo privilegio.

Per creare un'applicazione Azure per DRA e aggiungere un tenant di Azure:

1. Nella Delegation and Configuration Console (Console di delega e configurazione) passare a **Configuration Management** (Gestione configurazione) > **Tenant di Azure**.
2. Fare clic con il pulsante destro del mouse su **Tenant di Azure** e selezionare **New Azure Tenant** (Nuovo tenant di Azure). Fare clic su **Avanti**.

3 Creare l'applicazione Azure e specificare i dettagli richiesti nella scheda **Azure Application** (Applicazione Azure).

3a Avviare una sessione di PowerShell sul server di amministrazione DRA e passare a `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`

3b Eseguire `. .\NewDraAzureApplication.ps1` per caricare PowerShell.

3c Eseguire il cmdlet `New-DRAAzureApplication` specificando i seguenti parametri:

- <name> - Nome dell'applicazione dalla procedura guidata tenant.

  Importante: Micro Focus consiglia di utilizzare il nome specificato nella console DRA.

- (Facoltativo) <environment> - Specificare AzureCloud, AzureChinaCloud, AzureGermanyCloud o AzureUSGovernment, a seconda del tenant in uso.

3d Nella finestra di dialogo delle credenziali, specificare le credenziali dell'amministratore globale. Vengono generati l'ID tenant di Azure, l'ID oggetto, l'ID applicazione e il segreto client (password dell'applicazione).

Nota: DRA utilizza i moduli PowerShell di Azure AD ed Exchange Online e l'API Microsoft Graph per accedere ai dati. L'ID applicazione e il segreto dell'applicazione vengono utilizzati durante l'accesso ad Azure Active Directory mediante l'API Microsoft Graph.

3e Copiare l'`ID tenant`, l'`ID oggetto`, l'`ID applicazione` e il `segreto client` nella scheda **Azure Application** (Applicazione Azure) della procedura guidata Add New Azure Tenant (Aggiunta nuovo tenant di Azure), quindi fare clic su **Avanti**. DRA convalida l'applicazione Azure.

4 Nella scheda **Autenticazione**, selezionare un tipo di autenticazione.

DRA supporta sia l'autenticazione basata su certificato che l'autenticazione di base quando si utilizzano i moduli PowerShell Azure AD ed Exchange Online.

- **Certificate-based authentication** (Autenticazione basata su certificato): questa è l'opzione di default. DRA crea un certificato autofirmato e lo associa all'applicazione Azure. Se non si desidera utilizzare il certificato autofirmato, è possibile effettuare l'upload del proprio certificato dopo aver preso in gestione il tenant. Per ulteriori informazioni, vedere Upload manuale di un certificato.
- **Basic authentication** (Autenticazione di base): questa è l'opzione precedente. DRA utilizza l'account utente specificato per eseguire l'autenticazione con Azure Active Directory.

Fare clic su **Avanti**.

5 (Facoltativo) Nella scheda **Custom Azure Tenant Source Anchor Attribute** (Attributo ancoraggio di origine tenant di Azure personalizzato), specificare l'attributo dell'ancoraggio di origine utilizzato per mappare gli oggetti Active Directory ad Azure durante la sincronizzazione. Fare clic su **Avanti**.

6 Fare clic su **Finish** (Fine).

L'aggiunta del tenant di Azure potrebbe richiedere alcuni minuti. Una volta aggiunto il tenant, DRA esegue un aggiornamento completo della cache degli account per il tenant e il tenant aggiunto viene visualizzato nel riquadro di visualizzazione Tenant di Azure.

Per visualizzare il tipo di autenticazione per il tenant di Azure, fare clic con il pulsante destro del mouse sul tenant e scegliere **Proprietà** > **Autenticazione**.

Per visualizzare le informazioni sul certificato, fare clic con il pulsante destro del mouse sul tenant e scegliere **Proprietà** > **Certificate Info** (Informazioni sul certificato).

Upload manuale di un certificato

Se si desidera utilizzare il proprio certificato o se il certificato personalizzato esistente è scaduto e si desidera specificare un nuovo certificato, è possibile effettuare l'upload del certificato dalla pagina delle proprietà del tenant di Azure. I formati di file di certificato supportati sono `.pfx` e `.cer`

Importante: Accertarsi che il certificato manuale specificato sia protetto con una password complessa.

Per effettuare l'upload di un certificato:

1. Aprire la Delegation and Configuration Console (Console di delega e configurazione) e passare a **Configuration Management** (Gestione configurazione) > **Tenant di Azure**.
2. Fare clic con il pulsante destro del mouse sul tenant di Azure e scegliere **Proprietà** > **Autenticazione**. Assicurarsi che l'opzione **Manual customer certificate** (Certificato manuale del cliente) sia selezionata.
3. Selezionare la scheda **Certificate Info** (Informazioni sul certificato).
4. In **New certificate** (Nuovo certificato), fare clic su **Browse** (Sfoglia) per selezionare un file di certificato. Se si desidera specificare un file di certificato `.cer`, assicurarsi che nell'archivio personale dell'utente dell'account del servizio sia installato un certificato con la chiave privata.
5. Specificare la password per il certificato, se necessario.
6. Applicare le modifiche. I dettagli del certificato vengono aggiornati.

Importante:

- Se il server di amministrazione primario è configurato con la **Basic authentication** (Autenticazione di base), assicurarsi di specificare manualmente le credenziali per la **Basic authentication** (Autenticazione di base) sui server di amministrazione secondari per il corretto aggiornamento completo della cache degli account. L'account di accesso deve essere univoco su ciascun server di amministrazione dell'MMS impostato.
- Se il server di amministrazione primario è configurato con il tipo di autenticazione **Manual customer certificate** (Certificato manuale del cliente) o **Automatic self-signed certificate** (Certificato autofirmato automatico), i server di amministrazione secondari visualizzano il tipo di autenticazione come **Automatic self-signed certificate** (Certificato autofirmato automatico). Per effettuare l'upload del proprio certificato, è necessario modificare manualmente il tipo di autenticazione in **Manual customer certificate** (Certificato manuale del cliente) nel server di amministrazione secondario. Il certificato deve essere univoco su ciascun server di amministrazione dell'MMS impostato.

Configurazione dell'autenticazione basata su certificato per un'applicazione Azure dopo l'upgrade alla versione 10.2

Dopo aver eseguito l'upgrade a DRA 10.2, è possibile passare dall'autenticazione di base all'autenticazione basata su certificato e configurare l'applicazione Azure in modo che utilizzi l'autenticazione basata su certificato. L'applicazione Azure richiede autorizzazioni aggiuntive per l'autenticazione basata su certificato. Per applicare le autorizzazioni necessarie all'applicazione Azure, è necessario eseguire lo script `UpdateDraAzureApplication Permission.ps1`.

Per configurare l'applicazione Azure in modo che utilizzi l'autenticazione basata su certificato dopo l'upgrade, eseguire i passaggi seguenti:

1. Aprire la Delegation and Configuration Console (Console di delega e configurazione) e passare a **Configuration Management** (Gestione configurazione) > **Tenant di Azure**.
2. Fare clic con il pulsante destro del mouse sul tenant di Azure e selezionare **Proprietà > Autenticazione**. L'opzione **Basic authentication** (Autenticazione di base) è selezionata di default.
3. Modificare il tipo di autenticazione in **Automatic self-signed certificate** (Certificato autofirmato automatico) o **Manual customer certificate** (Certificato manuale del cliente).
4. Fare clic sulla scheda **Certificate Info** (Informazioni sul certificato).
5. Aggiornare l'applicazione Azure applicando le autorizzazioni necessarie per l'autenticazione basata su certificato.
   - **5a** Avviare una sessione di PowerShell sul server di amministrazione DRA e passare a `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`
   - **5b** Eseguire `. .\UpdateDraAzureApplicationPermission.ps1` per caricare PowerShell.
   - **5c** Eseguire il cmdlet `UpdateDraAzureApplication Permission` specificando il nome dell'applicazione Azure disponibile nella scheda **Azure Application** (Applicazione Azure).
   - **5d** Nella finestra di dialogo delle credenziali, specificare le credenziali dell'amministratore globale. Viene generato l'ID dell'oggetto Applicazione.
   - **5e** Copiare l'ID dell'oggetto Applicazione nella scheda **Certificate Info** (Informazioni sul certificato). Se è stata selezionata l'opzione **Manual customer certificate** (Certificato manuale del cliente), effettuare l'upload del certificato nell'area New Certificate (Nuovo certificato).
6. Applicare le modifiche. I dettagli del certificato vengono aggiornati.

Reimpostazione del segreto client per un'applicazione Azure

Se è necessario reimpostare il segreto client per un'applicazione Azure, attenersi alla procedura seguente.

Per reimpostare il segreto client per un'applicazione Azure:

1. Avviare una sessione di PowerShell sul server di amministrazione DRA e passare a `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`
2. Eseguire `. .\ResetDraAzureApplicationClientSecret.ps1` per caricare PowerShell.
3. Eseguire il cmdlet `ResetDraAzureApplicationClientSecret` per la richiesta dei parametri.

4 Specificare i seguenti parametri per `Reset-DraAzureApplicationClientSecret`:
   - `<name>` - Nome dell'applicazione dalla procedura guidata tenant.
   - (Facoltativo) `<environment>` - Specificare AzureCloud, AzureChinaCloud, AzureGermanyCloud o AzureUSGovernment, a seconda del tenant in uso.
5 Nella finestra di dialogo delle credenziali, specificare le credenziali dell'amministratore globale.

   Vengono generati l'ID e il segreto client dell'applicazione Azure.
6 Copiare il segreto client nella console DRA (procedura guidata tenant).
   6a Aprire la Delegation and Configuration Console (Console di delega e configurazione) e passare a **Configuration Management** (Gestione configurazione) > **Tenant di Azure**.
   6b Fare clic con il pulsante destro del mouse sul tenant di Azure e scegliere **Proprietà** > **Azure Application** (Applicazione Azure).
   6c Incollare il segreto del client dell'applicazione Azure generato dallo script nel campo **Client Secret** (Segreto client).
   6d Applicare le modifiche.

Configurazione dell'invito dell'utente guest Azure

Quando si invitano utenti guest Azure ad Azure Active Directory, DRA invia un'e-mail all'utente guest Azure con un messaggio di benvenuto personalizzato che include un collegamento di invito. È possibile configurare questo messaggio di benvenuto e il collegamento di invito o l'URL di reindirizzamento che si desidera visualizzare nell'invito. L'utente guest Azure viene reindirizzato all'URL configurato dopo aver accettato l'invito, in cui gli utenti guest Azure possono eseguire il login utilizzando le proprie credenziali.

Per configurare l'invito dell'utente guest:

1 Nella Delegation and Configuration Console (Console di delega e configurazione) passare a **Configuration Management** (Gestione configurazione) > **Tenant di Azure**.
2 Selezionare il tenant di Azure gestito per il quale si desidera configurare l'invito, fare clic con il pulsante destro del mouse e selezionare **Proprietà**.
3 Fare clic sulla scheda **Guest Invite Config** (Configurazione invito guest).
4 Specificare il messaggio di benvenuto e il collegamento di invito.
5 Applicare le modifiche.

Gestione delle password per gli account di accesso

È possibile reimpostare le password per gli account di accesso utilizzati per gestire un dominio, un server secondario, Exchange o un tenant di Azure da DRA. Se la password per uno di questi account di accesso è in scadenza o viene dimenticata, è possibile reimpostarla nei seguenti modi:

- Reimpostare manualmente la password nella Console di delega e configurazione.
- Pianificare un lavoro per controllare la scadenza della password degli account di accesso e reimpostare quelle in scadenza.

È possibile reimpostare la password per gli account di accesso sia dal server primario che dal server secondario. Se lo stesso account di accesso viene utilizzato in più istanze dello stesso dominio, ad esempio per gestire una casella postale di Exchange o un server secondario, il server DRA aggiorna automaticamente la password per tutte le istanze di utilizzo dell'account di accesso, eliminando così la necessità di aggiornare manualmente la password per ciascuna istanza. Se il server di amministrazione secondario utilizza l'account di accesso al dominio del server di amministrazione primario, il server DRA aggiorna automaticamente la password per l'account di accesso nel server di amministrazione secondario.

- "Reimpostare la password manualmente" a pagina 136
- "Pianificare un lavoro per la reimpostazione della password" a pagina 137

Reimpostare la password manualmente

Utilizzare la Console di delega e configurazione per reimpostare manualmente la password per un account di accesso.

Per reimpostare manualmente la password per un account di accesso:

1. Nella Console di delega e configurazione, fare clic su **Configuration Management** (Gestione configurazione).
2. Selezionare un dominio gestito o un tenant di Azure e visualizzare le proprietà.
3. Nella pagina delle proprietà, specificare le informazioni seguenti:
   - Per aggiornare la password di un account di accesso al dominio, nella scheda Domain access (Accesso al dominio), specificare una nuova password per l'account di accesso al dominio. Selezionare **Update password in Active Directory** (Aggiorna password in Active Directory).
   - Per aggiornare la password di un account di accesso a Exchange, nella scheda Exchange access (Accesso a Exchange), specificare una nuova password per l'account di accesso a Exchange. Selezionare **Update password in Active Directory** (Aggiorna password in Active Directory).
   - Per aggiornare la password di un account di accesso tenant di Azure, nella scheda Tenant access (Accesso tenant), specificare una nuova password per l'account di accesso tenant. Selezionare **Update Azure tenant access account password** (Aggiorna password account di accesso tenant di Azure).
   - Per aggiornare la password di un account di accesso per un server di amministrazione secondario, selezionare **Configuration Management** (Gestione configurazione) > **Administration Servers** (Server di amministrazione) nel server di amministrazione primario. Selezionare il server di amministrazione secondario per il quale si desidera aggiornare la password, fare clic con il pulsante destro del mouse e selezionare **Properties** (Proprietà). Nella scheda Access account (Account di accesso), specificare una nuova password per l'account di accesso. Selezionare **Update password in Active Directory** (Aggiorna password in Active Directory).

Nota

- Assicurarsi che l'account di accesso del server di amministrazione secondario non sia l'account di servizio del server di amministrazione secondario. L'account di accesso deve far parte del gruppo di amministratori locale sul server di amministrazione secondario.
- Se si utilizza l'account con meno privilegi come account di accesso, assicurarsi che a tale account in Active Directory sia assegnata l'autorizzazione "Reset Password" (Reimpostazione password), affinché la reimpostazione della password venga eseguita correttamente in DRA.

Pianificare un lavoro per la reimpostazione della password

È possibile pianificare l'esecuzione del lavoro di reimpostazione della password a intervalli predefiniti in modo da reimpostare le password in scadenza per gli account di accesso. Verranno reimpostate tutte le password dell'account di accesso in scadenza prima della successiva esecuzione pianificata del lavoro. Verrà generata automaticamente una nuova password in base alle policy per le password.

Il lavoro è disabilitato di default. È possibile pianificare il lavoro una volta alla settimana o a un intervallo specifico, in base alle proprie esigenze. In un ambiente MMS, se si configura il lavoro sul server primario, assicurarsi che il lavoro sia configurato su tutti i server di MMS.

Per configurare il lavoro:

1. Sul server in cui si desidera pianificare il lavoro, accedere alla voce di registro `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\UpdateAccessAccPWD.Freq`.
2. Fare clic con il pulsante destro del mouse e selezionare **Modifica**.
3. Nel campo **Dati valore**, specificare la frequenza con cui si desidera eseguire il lavoro.
   - Per pianificare un lavoro settimanale, specificare la frequenza nel formato `Weekly <Giorno della settimana> <Ora nel formato 24 ore>`. Ad esempio, per pianificare l'esecuzione del lavoro ogni sabato alle 18.00, immettere:

     `Weekly 06 18:00`

     Dove 6 indica il giorno della settimana e `18:00` indica l'ora nel formato 24 ore.
   - Per pianificare l'esecuzione del lavoro a un intervallo specifico, specificare la frequenza nel formato `Interval <Ora nel formato 24 ore>`. Ad esempio, per pianificare l'esecuzione del lavoro ogni 8 ore, immettere:

     `Interval 08:00`

   Si consiglia di pianificare l'esecuzione del lavoro nei fine settimana.

   Nota: Il lavoro di reimpostazione della password non supporta la frequenza giornaliera. Se si configura la frequenza giornaliera, il server DRA reimposta automaticamente la pianificazione su `Weekly 06 00:00` al riavvio di NetIQ Administration Service (Servizio di amministrazione NetIQ).
4. Fare clic su **OK**.
5. Riavviare il servizio di amministrazione DRA per applicare le modifiche.

Nota: Per ciascun tenant di Azure configurato, il lavoro crea la chiave di registro seguente per la policy password di default con una validità di 90 giorni: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\<tenantName>.ValidityPeriod`. La data di scadenza della password per l'account di accesso tenant viene calcolata in base al periodo di validità del tenant. Quando la password è in scadenza, il lavoro reimposta la password per l'account di accesso tenant.

Abilitare l'autenticazione prioritaria LDAP

È possibile configurare un'autenticazione prioritaria LDAP per le modifiche del gestore personalizzato LDAP nella console Web. Se questa funzione è abilitata, è possibile impostare il tipo di autenticazione per i gestori di query LDAP personalizzati in modo da richiedere l'account prioritario LDAP per l'autenticazione della connessione.

Per attivare questa funzione:

1. Passare a **Configuration Management (Gestione configurazione)** > **Update Administration Server Options (Aggiorna opzioni server di amministrazione)** nella Console di delega e configurazione.
2. Selezionare la scheda **LDAP Override Account** (Account prioritario LDAP) nella finestra Administration Server Options (Opzioni del server di amministrazione).
3. Specificare il nome account, il dominio e la password e applicare le modifiche.

   Ad esempio: `nome@dominio` o `dominio\nome`

Per informazioni sull'utilizzo di questa funzione nelle personalizzazioni della console Web, vedere Passaggi di base per la creazione di un gestore personalizzato.

V Policy e automazione dei processi

In questo capitolo vengono fornite informazioni utili per comprendere il funzionamento delle policy nell'ambiente DRA e si illustrano le opzioni disponibili per le policy. Vengono inoltre descritte le modalità di utilizzo dei trigger e del workflow automatizzato per l'automazione dei processi quando si utilizzano gli oggetti di Active Directory.

13 Caratteristiche delle policy di DRA

In DRA è possibile configurare varie policy che contribuiscono a mettere in sicurezza l'azienda e a evitare il danneggiamento dei dati. Le policy operano nell'ambito del modello di sicurezza dinamico, facendo sì che la loro applicazione sia sempre al passo con la continua evoluzione aziendale. La definizione di policy, quali le convenzioni di denominazione, i limiti di utilizzo del disco e la convalida di proprietà, consente di applicare regole che hanno la funzione di preservare l'integrità dei dati aziendali.

In DRA è possibile definire rapidamente le regole delle policy per le seguenti aree di gestione aziendale:

- Microsoft Exchange
- Licenza per Office 365
- Home directory
- Generazione di password

In DRA sono inoltre disponibili policy integrate per gruppi, account utente e computer.

Per gestire o definire le policy, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nei ruoli DRA Admins (Amministratori di DRA) e Manage Policies e Automation Triggers (Gestisci policy e trigger di automazione). Per facilitare la gestione delle policy, in DRA è disponibile il rapporto sui dettagli della policy, che include le informazioni seguenti:

- Stato di abilitazione della policy
- Operazioni associate
- Oggetti disciplinati dalla policy
- Dettagli relativi all'ambito della policy

Questo rapporto è utile per verificare che le policy siano state definite in modo corretto. Può essere utilizzato anche per confrontare le proprietà delle policy, rilevare conflitti e migliorare l'applicazione in tutta l'azienda.

Modalità di applicazione delle policy del server di amministrazione

Un task o un'operazione di amministrazione può essere associato a una o più policy. Quando si effettua un'operazione associata a una policy, il server di amministrazione esegue la policy e applica le regole specificate. Se rileva una violazione della policy, restituisce un messaggio di errore. Se, invece, non rileva alcuna violazione della policy, porta a termine l'operazione. È possibile limitare l'ambito di una policy associandola a viste ActiveView o gruppi di amministratori aggiunti specifici.

Se un'operazione è associata a più policy, il server di amministrazione le applica in ordine alfabetico. Vale a dire che la policy A viene applicata prima della policy B, indipendentemente dalle regole specificate.

Affinché non si verifichino conflitti tra le policy, attenersi alle linee guida seguenti:

- Denominare le policy in modo che vengano eseguite nell'ordine corretto
- Verificare che ciascuna policy non interferisca con le convalide o le azioni eseguite da altre policy
- Eseguire prove accurate delle policy personalizzate prima di implementarle nell'ambiente di produzione

Ogni volta che si esegue una policy, il server di amministrazione immette lo stato della policy nel log di revisione. Queste voci di log registrano il codice restituito, le operazioni associate, gli oggetti su cui sono state eseguite le operazioni e se la policy personalizzata ha avuto esito positivo.

Avviso: le policy vengono eseguite utilizzando l'account del servizio di amministrazione. Poiché l'account del servizio dispone di autorizzazioni di amministratore, le policy hanno un accesso completo a tutti i dati aziendali. Pertanto, gli amministratori aggiunti associati al ruolo Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione) potrebbero acquisire più potere del previsto.

Policy integrate

Le policy integrate vengono implementate quando si installa il server di amministrazione. Per le policy si utilizzano i termini seguenti:

Ambito della policy

Definisce gli oggetti o le proprietà a cui viene applicata la policy in DRA. Ad esempio, alcune policy possono essere applicate ad amministratori aggiunti specifici in viste ActiveView specifiche. Alcune policy consentono di scegliere tra diverse classi di oggetti, quali gruppi o account utente.

Policy globali

Applicano le regole della policy a tutti gli oggetti della classe o del tipo specificato nei domini gestiti. Le policy globali non consentono di limitare l'ambito degli oggetti a cui la policy viene applicata.

Relazione della policy

Indica se la policy viene applicata singolarmente o congiuntamente ad altre. Per stabilire la relazione di una policy, definire due o più regole valide per la stessa azione, quindi scegliere l'opzione relativa al membro di un gruppo di policy. Se i parametri dell'operazione o della proprietà soddisfano una delle regole, l'operazione ha esito positivo.

Argomenti delle policy integrate:

- “Caratteristiche delle policy integrate” a pagina 143
- “Policy disponibili” a pagina 143
- “Utilizzo delle policy integrate” a pagina 146

Caratteristiche delle policy integrate

Le policy integrate forniscono regole aziendali per gestire problemi comuni di sicurezza e integrità dei dati. Queste policy sono parte integrante del modello di sicurezza di default e consentono di integrare le funzioni di sicurezza di DRA nella configurazione aziendale esistente.

In DRA si possono utilizzare due metodi per applicare una policy. È possibile creare policy personalizzate o scegliere tra le varie policy integrate. Le policy integrate facilitano il processo applicativo perché evitano di dover sviluppare script personalizzati. Se si desidera implementare policy personalizzate, è possibile adattare una policy integrata esistente in base alle proprie esigenze specifiche. La maggior parte delle policy consente di modificare il testo del messaggio di errore, di rinominare la policy, di aggiungere una descrizione e di specificare le modalità di applicazione.

Quando si installa DRA, vengono abilitate varie policy integrate. Le policy seguenti sono implementate di default. Se non si desidera applicarle, è possibile disabilitarle o eliminarle.

Nome policy	Valore di default	Descrizione
$ComputerNameLengthPolicy	64 15 (pre Windows 2000)	Limita il numero di caratteri del nome del computer o del nome del computer precedente a Windows 2000
$GroupNameLengthPolicy	64 20 (pre Windows 2000)	Limita il numero di caratteri del nome del gruppo o del nome del gruppo precedente a Windows 2000
$GroupSizePolicy	5000	Limita il numero di membri di un gruppo
$NameUniquenessPolicy	Nessuno	Garantisce che i nomi CN precedenti a Windows 2000 siano univoci in tutti i domini gestiti
$SpecialGroupsPolicy	Nessuno	Impedisce l'escalation incontrollata dei poteri nell'ambiente.
$UCPowerConflictPolicy	Nessuno	Impedisce l'escalation rendendo i poteri User Clone (Clona utente) e User Create (Crea utente) reciprocamente esclusivi
$UPNUniquenessPolicy	Nessuno	Garantisce che i nomi UPN siano univoci in tutti i domini gestiti
$UserNameLengthPolicy	64 20 (nome di login di livello inferiore)	Limita il numero di caratteri nel nome utente di login o nel nome di login di livello inferiore

Policy disponibili

In DRA sono disponibili svariate policy che è possibile personalizzare in funzione del modello di sicurezza.

Nota: è possibile creare una policy che richiede una voce per una proprietà che non è attualmente disponibile nelle interfacce utente di DRA. Se la policy richiede una voce e nell'interfaccia utente non è disponibile un campo per immettere il valore, ad esempio un reparto per un nuovo account utente, non sarà possibile creare o gestire l'oggetto. Per evitare questo problema, configurare policy che richiedano solo le proprietà a cui è possibile accedere dalle interfacce utente.

Create a Custom Policy (Crea una policy personalizzata)

Consente di collegare uno script o un eseguibile a un'operazione di DRA o Exchange. Mediante le policy personalizzate è possibile convalidare qualsiasi operazione desiderata.

Enforce a Maximum Name Length (Applica lunghezza massima nome)

Consente di imporre a livello globale una lunghezza massima consentita per i nomi di account utente, gruppi, unità organizzative, contatti o computer.

La policy controlla il nome del container (nome comune o cn) e il nome precedente a Windows 2000 (nome di accesso dell'utente).

Enforce Maximum Number of Group Members (Applica numero massimo di membri per il gruppo)

Consente di imporre a livello globale limiti relativi al numero di membri di un gruppo.

Enforce Unique Pre-Windows 2000 Account Names (Applica nomi account univoci pre Windows 2000)

Consente di verificare che un nome precedente a Windows 2000 sia univoco in tutti i domini gestiti. Nei domini Microsoft Windows, i nomi precedenti a Windows 2000 devono essere univoci all'interno del dominio. Questa policy globale applica la regola in tutti i domini gestiti.

Enforce unique User Principal Names (UPNs) (Applica nomi univoci per le entità utente)

Consente di verificare che il nome dell'entità utente (UPN) sia univoco in tutti i domini gestiti. Nei domini Microsoft Windows, gli UPN devono essere univoci all'interno del dominio. Questa policy applica la regola in tutti i domini gestiti. Poiché si tratta di una policy globale, in DRA è disponibile il nome, la descrizione e la relazione della policy.

Limit actions on members of special groups (Limita azioni sui membri per gruppi speciali)

Impedisce la gestione dei membri di un gruppo di amministratori a coloro che non sono membri del gruppo stesso. Questa policy globale è abilitata per default.

Quando si limitano le azioni sui membri dei gruppi di amministratori, la procedura guidata Create Policy (Crea policy) non richiede informazioni aggiuntive. È possibile specificare un messaggio di errore personalizzato. Poiché si tratta di una policy globale, in DRA è disponibile il nome, la descrizione e la relazione della policy.

Prevent assistant administrators from Creating and Cloning Users in Same AV (Impedisci agli amministratori aggiunti di creare e clonare utenti nella stessa vista ActiveView)

Impedisce la possibile escalation di poteri. Quando la policy è abilitata, è possibile creare o clonare account utente, ma non è possibile disporre di entrambi i poteri. Questa policy globale assicura che l'utente non possa creare e clonare account utente nella stessa vista ActiveView.

La policy non richiede informazioni aggiuntive.

Set Naming Convention Policy (Policy di impostazione di convenzioni di denominazione)

Consente di stabilire convenzioni di denominazione applicabili ad amministratori aggiunti, viste ActiveView e classi di oggetti specifiche, ad esempio account utente o gruppi.

È inoltre possibile specificare i nomi esatti controllati dalla policy.

Create a Policy to Validate a Specific Property (Crea policy per convalidare una proprietà specifica)

Consente di creare una policy per convalidare qualsiasi proprietà di un oggetto OU o Account. È possibile specificare un valore di default, una maschera di formato delle proprietà, valori e intervalli validi.

Utilizzare questa policy per imporre l'integrità dei dati attraverso la convalida di particolari campi di immissione quando si creano, si clonano o si modificano proprietà di oggetti specifici. La policy offre una straordinaria flessibilità e il potere di convalidare voci, fornire voci di default e limitare le scelte delle voci disponibili per vari campi delle proprietà. Permette di imporre l'immissione di una voce corretta affinché un task venga eseguito, preservando così l'integrità dei dati in tutti i domini gestiti.

Si supponga ad esempio che esistano tre reparti: produzione, vendite e amministrazione. È possibile limitare le voci accettate in DRA solo a tali tre valori. È possibile utilizzare la policy anche per imporre formati corretti dei numeri telefonici, per fornire un intervallo di dati validi o per richiedere una voce per il campo dell'indirizzo e-mail. Per specificare più maschere di formato per un numero telefonico, ad esempio `(123)456 7890` e anche `456 7890`, definire la maschera di formato della proprietà immettendo `(###)### ####,### ####`.

Create Policy to Enforce Office 365 Licenses (Crea policy per applicare le licenze di Office 365)

Consente di creare una policy per assegnare le licenze di Office 365 in base all'appartenenza a un gruppo Active Directory. La policy applica anche la rimozione delle licenze di Office 365 quando un membro viene rimosso dal gruppo Active Directory corrispondente.

Se un utente che non è sincronizzato con il cloud viene aggiunto al gruppo Active Directory, la sincronizzazione viene eseguita prima di assegnare all'utente una licenza di Office 365.

Durante la creazione della policy è possibile specificare varie proprietà e impostazioni, come il nome della policy e il testo del messaggio di errore che viene visualizzato quando un amministratore aggiunto tenta di eseguire un'azione che viola la policy.

L'impostazione **Ensure only licenses assigned by DRA policies are enabled on accounts. All other licenses will be removed.** (Verificare che sugli account siano abilitate solo le licenze assegnate dalle policy DRA. Tutte le altre licenze verranno rimosse) è inclusa nella pagina delle proprietà del tenant, che può essere configurata per ciascun tenant. Questa impostazione viene utilizzata per le policy di licenza Office 365 di DRA per configurare la modalità di applicazione delle assegnazioni delle licenze:

Se questa impostazione è abilitata, l'applicazione delle licenze DRA garantirà che solo le licenze assegnate tramite le policy DRA siano soggette a provisioning per gli account (le licenze assegnate esternamente a DRA verranno rimosse dagli account assegnati alla policy di licenza). Se questa impostazione è disabilitata (impostazione di default), l'applicazione delle licenze DRA garantirà che le licenze specifiche incluse nelle policy di Office 365 siano soggette a provisioning per gli account (se viene rimossa l'assegnazione di un account da una policy di licenza, solo le licenze assegnate da tale policy non saranno più soggette a provisioning).

Utilizzo delle policy integrate

Poiché le policy integrate fanno parte del modello di sicurezza di default, è possibile utilizzarle per applicare il modello di sicurezza in uso oppure modificarle affinché rispondano al meglio alle proprie esigenze specifiche. È possibile modificare il nome, le impostazioni delle regole, l'ambito, la relazione della policy e il messaggio di errore di svariate policy integrate. Ogni policy integrata può essere abilitata o disabilitata.

È anche possibile creare nuove policy.

Implementazione di una policy personalizzata

Le policy personalizzate consentono di sfruttare a pieno la potenza e la flessibilità del modello di sicurezza di default. Utilizzando policy personalizzate, è possibile integrare DRA con i componenti già esistenti all'interno dell'azienda, assicurando al contempo che vengano applicate le regole proprietarie. È possibile utilizzare la funzione delle policy personalizzate per estendere le policy aziendali.

Per creare e applicare policy personalizzate si utilizza l'associazione di un eseguibile o di uno script a un'operazione di amministrazione. Ad esempio, lo script di una policy associato all'operazione `UserCreate` potrebbe controllare il database delle risorse umane per verificare se il dipendente specificato esiste. Se il dipendente esiste nel database delle risorse umane e non dispone di un account, lo script recupera l'ID, il nome e il cognome del dipendente dal database. L'operazione viene completata popolando la finestra delle proprietà dell'account utente con le informazioni corrette. Tuttavia, se il dipendente dispone già di un account, l'operazione ha esito negativo.

Gli script assicurano una straordinaria flessibilità e un'enorme potenza. Per creare script personalizzati per le policy, è possibile utilizzare il provider ADSI di Directory and Resource Administrator (provider ADSI), l'SDK (Software Development Kit) e i cmdlet di PowerShell. Per ulteriori informazioni sulla creazione di script personalizzati per le policy, vedere la sezione Reference (Riferimento) sul sito della documentazione di DRA.

Restrizioni per i gruppi di sicurezza integrati nativi

Per rendere l'ambiente più sicuro, in DRA è possibile limitare i poteri concessi ai gruppi di sicurezza integrati di Microsoft Windows. La possibilità di modificare l'appartenenza ai gruppi, le proprietà dei gruppi di sicurezza integrati o le proprietà dei membri dei gruppi può avere implicazioni significative sulla sicurezza. Ad esempio, se è possibile modificare la password di un utente appartenente al gruppo Server Operators, sara quindi possibile eseguire il login come tale utente ed esercitare i poteri delegati al gruppo di sicurezza integrato.

Con DRA è possibile evitare questo problema di sicurezza mediante una policy che controlla i poteri di cui l'utente dispone su un gruppo di sicurezza integrato nativo e i relativi membri. Questa convalida assicura che le azioni richieste non comportino un'escalation dei poteri. Una volta abilitata la policy, un amministratore aggiunto membro di un gruppo di sicurezza integrato, come ad esempio il gruppo Server Operators, può gestire solo gli altri membri dello stesso gruppo.

Restrizioni possibili per i gruppi di sicurezza integrati nativi

Mediante le policy di DRA è possibile limitare i poteri dei gruppi di sicurezza integrati di Microsoft Windows:

- Account Operators
- Administrators
- Backup Operators
- Cert Publishers
- DNS Admins
- Domain Admins
- Enterprise Admins
- Proprietari autori criteri di gruppo
- Print Operators
- Schema Admins

Nota: in DRA si fa riferimento ai gruppi di sicurezza integrati utilizzando i loro identificatori interni. Pertanto, tali gruppi sono supportati anche se vengono rinominati. Questa funzionalità fa sì che DRA possa supportare i gruppi di sicurezza integrati con nomi differenti in paesi diversi. Ad esempio, in DRA si fa riferimento ai gruppi Administrators e *Administratoren* utilizzando lo stesso identificatore interno.

Restrizioni delle azioni sui gruppi di sicurezza integrati nativi

Per limitare il potere che i gruppi di sicurezza integrati nativi e i loro membri possono esercitare, in DRA è possibile utilizzare una policy, denominata `$SpecialGroupsPolicy`, che limita le azioni che un membro di un gruppo di sicurezza integrato nativo può eseguire su altri membri o altri gruppi di sicurezza integrati nativi. La policy è abilitata di default. Se non si desidera limitare le azioni sui gruppi di sicurezza integrati nativi e i loro membri, è possibile disabilitarla.

Quando la policy è abilitata, vengono utilizzate le prove di convalida seguenti per stabilire se una determinata azione è consentita su un gruppo di sicurezza integrato nativo o i suoi membri:

- Un amministratore di Microsoft Windows può eseguire azioni sui gruppi di sicurezza integrati nativi e i relativi membri per i quali dispone dei poteri appropriati.
- Un membro di un gruppo di sicurezza integrato può eseguire azioni sul suo stesso gruppo di sicurezza integrato e i relativi membri, a condizione che disponga dei poteri appropriati.
- Se non si è membri di un gruppo di sicurezza integrato, non è possibile apportare modifiche a un gruppo di sicurezza integrato o ai relativi membri.

Ad esempio, un membro dei gruppi Server Operators e Account Operator che dispone dei poteri appropriati può eseguire azioni sui membri dei gruppi Server Operators e Account Operators, come anche sui membri di entrambi i gruppi. Tuttavia, non può eseguire azioni su un account utente che è membro dei gruppi Print Operators e Account Operators.

In DRA si applicano restrizioni per le azioni seguenti sui gruppi di sicurezza integrati nativi:

- Clonazione di un gruppo

- Creazione di un gruppo
- Eliminazione di un gruppo
- Aggiunta di un membro a un gruppo
- Rimozione di un membro da un gruppo
- Spostamento di un gruppo in un'unità organizzativa
- Modifica delle proprietà di un gruppo
- Copia di una casella postale
- Rimozione di una casella postale
- Clonazione di un account utente
- Creazione di un account utente
- Eliminazione di un account utente
- Spostamento di un account utente in un'unità organizzativa
- Modifica delle proprietà di un account utente

Si applicano restrizioni anche su altre azioni per evitare che l'utente acquisisca poteri su un oggetto. Ad esempio, quando si aggiunge un account utente a un gruppo, viene verificato che non vengano acquisiti poteri aggiuntivi sull'account utente in quanto membro di tale gruppo. Questa convalida contribuisce a evitare un'escalation di potere.

Gestione delle policy

Mediante il nodo Policy and Automation Management (Gestione policy e automazione), è possibile accedere alle policy di Microsoft Exchange e delle home directory, nonché alle policy integrate e personalizzate. Per migliorare la sicurezza aziendale e l'integrità dei dati, utilizzare i seguenti task comuni.

Configurazione delle policy di Exchange

È possibile definire regole di configurazione di Microsoft Exchange, della policy delle caselle postali, di denominazione automatica e di generazione di proxy. Tramite queste regole si possono definire le modalità di gestione delle caselle postali quando un amministratore aggiunto crea, modifica o elimina un account utente.

Configurazione delle policy delle home directory

Quando un amministratore aggiunto crea, rinomina o elimina un account utente, è possibile creare, rinominare o eliminare automaticamente home directory e condivisioni principali. La policy delle home directory consente anche di attivare o disattivare il supporto per la quota disco per le home directory nei server Microsoft Windows e nei server non Windows.

Configurazione delle policy di generazione password

È possibile definire i requisiti per le password generate da DRA.

Per informazioni dettagliate sulla gestione delle policy in DRA, fare riferimento alle seguenti sezioni:

- “Policy di Microsoft Exchange” a pagina 149
- “Policy delle licenze di Office 365” a pagina 150
- “Creazione e implementazione della policy per le home directory” a pagina 151

- “Abilitazione della funzione di generazione password” a pagina 158
- “Task delle policy” a pagina 158

Policy di Microsoft Exchange

In Exchange sono disponibili svariate policy per rendere più efficace la gestione degli oggetti Microsoft Exchange. Tali policy consentono di automatizzare la gestione delle caselle postali, applicare convenzioni di denominazione per gli alias e gli archivi delle caselle postali e generare automaticamente indirizzi e-mail.

Le policy permettono di semplificare i workflow e preservare l'integrità dei dati. Ad esempio, è possibile specificare le modalità di gestione delle caselle postali in Exchange quando si creano, si modificano o si eliminano account utente. Per definire e gestire le policy di Microsoft Exchange, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione).

Definizione di una policy di default per gli indirizzi e-mail

Per specificare la policy di default per gli indirizzi e-mail, è necessario disporre di poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), e la licenza deve includere il supporto per Exchange.

Per specificare una policy di default per gli indirizzi e-mail:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange) > **Proxy Generation** (Generazione proxy).
2. Specificare il dominio del server Microsoft Exchange.
   - **2a** Fare clic su **Browse** (Sfoglia).
   - **2b** Specificare eventuali criteri di ricerca aggiuntivi secondo necessità e fare clic su **Find Now** (Trova ora).
   - **2c** Selezionare il dominio da configurare e fare clic su **OK**.
3. Specificare le regole di generazione proxy per il dominio selezionato.
   - **3a** Fare clic su **Add** (Aggiungi).
   - **3b** Selezionare un tipo di proxy. Ad esempio, fare clic su **Internet Address** (Indirizzo Internet).
   - **3c** Accettare il valore di default o digitare una nuova regola di generazione proxy, quindi fare clic su **OK**.

     Per ulteriori informazioni sulle stringhe di sostituzione supportate per le regole di generazione proxy, vederePolicy del client di delega e configurazione.
4. Fare clic su **Attributi personalizzati** per modificare il nome personalizzato delle proprietà personalizzate della casella postale.
   - **4a** Selezionare l'attributo e fare clic sul pulsante **Edit** (Modifica).
   - **4b** Nella finestra Attribute Properties (Proprietà attributo), immettere il nome dell'attributo nel campo **Custom name** (Nome personalizzato) e fare clic su **OK**.
5. Fare clic su **OK**.

Nota: per modificare gli attributi personalizzati nella policy di Microsoft Exchange, gli amministratori delle policy di DRA devono disporre del potere *Manage Custom Tools* (Gestisci strumenti personalizzati).

Regole delle caselle postali

Le regole delle caselle postali consentono di specificare le modalità di gestione che Exchange utilizza per le caselle postali quando gli amministratori aggiunti creano, clonano, modificano o eliminano gli account utente. Tali regole gestiscono automaticamente le caselle postali di Microsoft Exchange in base a come gli amministratori aggiunti gestiscono gli account utente associati.

Nota: quando si abilita l'opzione **Do not allow Assistant Admins to create a user account without a mailbox** (Non consentire agli amministratori aggiunti di creare un account utente senza una casella postale) nei domini Microsoft Windows, verificare che l'amministratore aggiunto disponga del potere necessario per clonare o creare un account utente. Se si abilita questa opzione, gli amministratori aggiunti dovranno creare gli account utente Windows con una casella postale.

Per specificare le regole delle caselle postali di Microsoft Exchange, è necessario disporre di poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), e la licenza deve includere il supporto per Exchange.

Per specificare le regole delle caselle postali di Exchange:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange) > **Mailbox Rules** (Regole caselle postali).
2. Selezionare le policy delle caselle postali che si desidera vengano applicate da Exchange quando si creano o si modificano gli account utente.
3. Fare clic su **OK**.

Policy delle licenze di Office 365

Per implementare le policy delle licenze di Office 365, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione). La licenza deve supportare anche il prodotto Microsoft Exchange.

Gestione delle licenze di Office 365 mediante DRA (facoltativo)

Se si desidera consentire a DRA di gestire le licenze di Office 365, è necessario eseguire le operazioni seguenti:

- Creare una policy di applicazione delle licenze.
- Abilitare l'opzione **License update schedule** (Pianificazione aggiornamento licenze) nella pagina delle proprietà del tenant.

Creazione di una policy per applicare le licenze di Office 365

Per creare una policy di applicazione delle licenze di Office 365, fare clic sul nodo **Policy and Automation Management** (Gestione policy e automazione) nella Console di delega e configurazione e selezionare **New Policy** (Nuova policy) > **Create New Policy to Enforce Office 365 Licenses** (Crea nuova policy per applicare le licenze di Office 365).

Quando la policy viene applicata e si aggiunge un utente ad Active Directory, in DRA viene utilizzata l'appartenenza ai gruppi per assegnare automaticamente la licenza di Office 365 all'utente.

Pianificazione dell'aggiornamento delle licenze di Office 365

Le policy create per applicare le licenze di Office 365 non vengono applicate in caso di modifiche apportate al di fuori di DRA, a meno che non si abiliti anche la **pianificazione dell'aggiornamento delle licenze** nella pagina delle proprietà del tenant. Il lavoro di aggiornamento delle licenze assicura che le licenze di Office 365 assegnate agli utenti siano conformi alle policy delle licenze di Office 365.

L'azione congiunta di tale lavoro di aggiornamento e delle policy delle licenze di Office 365 assicura che a tutti gli utenti gestiti vengano assegnate solo le licenze di Office 365 previste.

Nota

- Le licenze di Office 365 per gli account utente unicamente online non vengono gestite in DRA. Affinché DRA possa gestire gli utenti con licenze di Office 365, tali utenti devono essere sincronizzati con Active Directory.
- Se si sceglie di utilizzare DRA per gestire le licenze di Office 365, tutte le modifiche manuali apportate alle licenze di Office 365 al di fuori di DRA vengono ignorate alla successiva esecuzione del lavoro di aggiornamento delle licenze.
- Se si abilita il lavoro di aggiornamento delle licenze di Office 365 prima di aver verificato che le relative policy siano state configurate correttamente, le assegnazioni potrebbero risultare errate al termine del lavoro di aggiornamento.

Creazione e implementazione della policy per le home directory

Quando si gestisce un numero elevato di account utente, la creazione e la gestione delle relative home directory e condivisioni principali possono richiedere molto tempo e comportare errori di sicurezza. Inoltre, ogni volta che si crea, si rinomina o si elimina un utente, potrebbero essere necessarie attività aggiuntive di manutenzione. Le policy delle home directory facilitano la gestione della manutenzione di home directory e condivisioni principali.

Con DRA è possibile automatizzare la creazione e la manutenzione delle home directory degli utenti. Ad esempio, è possibile configurare facilmente DRA in modo che il server di amministrazione crei una home directory quando si crea un account utente. In questo caso, se si specifica il percorso di una home directory quando si crea l'account utente, il server crea automaticamente la home directory in base al percorso specificato. Se non si specifica un percorso, il server non crea la home directory.

DRA supporta i percorsi DFS (Distributed File System) per la creazione delle home directory degli utenti o per la configurazione di policy delle home directory per gli utenti in percorsi superiori consentiti. È possibile creare, rinominare ed eliminare le home directory in Netapp Filer e in partizioni e percorsi DFS.

Configurazione delle policy per le home directory

Per configurare le policy di home directory, condivisioni principali e quote disco dei volumi, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione). Ciascuna policy gestisce automaticamente home directory, condivisioni principali e quote disco dei volumi in base a come vengono gestiti gli account utente associati.

Per configurare le policy delle home directory, passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Home Directory Policies** (Configura policy home directory) >

- Home directory
- Home share (Condivisione principale)
- Home Volume Disk Quota (Quota disco volume home)

Requisiti del server di amministrazione

Per ogni computer in cui si desidera creare una condivisione principale, l'account del servizio del server di amministrazione o l'account di accesso deve essere un amministratore di tale computer o un membro del gruppo di amministratori nel dominio corrispondente.

In ciascuna unità in cui DRA gestisce e memorizza le home directory deve esistere una condivisione amministrativa, ad esempio C$ o D$. In DRA le condivisioni amministrative vengono utilizzate per eseguire alcuni task di automazione delle home directory e delle condivisioni principali. Se tali condivisioni non esistono, non è possibile fornire l'automazione delle home directory e delle condivisioni principali.

Configurazione dei percorsi consentiti delle home directory per NetApp Filer

Per configurare i percorsi superiori consentiti per NetApp Filer:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Home Directory Policies** (Configura policy home directory).
2. Nella casella di testo **Allowable parent paths** (Percorsi superiori consentiti), immettere uno dei percorsi consentiti riportati nella tabella seguente:

Tipo di condivisione	Percorso consentito
Windows	(*NomeFile**condivisioneamministrativa:**percorsoradicevolume*h*percorsodirectory*)
Non Windows	(*non windows**condivisione*)

3. Fare clic su **Aggiungi**.
4. Ripetere i passaggi da 1 a 3 per ciascun percorso superiore consentito ogni volta che si desidera applicare le policy delle home directory.

Caratteristiche della policy per le home directory

Per garantire la coerenza con le policy di sicurezza appropriate di Microsoft Windows, in DRA è possibile creare restrizioni di controllo dell'accesso solo a livello di directory. L'utilizzo di restrizioni di controllo dell'accesso a livello di nome della condivisione e di file o di oggetto Directory spesso rende confuso lo schema di accesso sia per gli amministratori che per gli utenti.

Quando si modifica una restrizione di controllo dell'accesso per una condivisione principale, la sicurezza esistente per tale directory non viene modificata. In questo caso, è necessario verificare che gli account utente dispongano dell'accesso appropriato alle loro home directory.

Automazione e regole per le home directory

Con DRA è possibile automatizzare i task di manutenzione delle home directory tramite la gestione delle home directory quando un account utente viene modificato. In DRA è possibile eseguire varie azioni quando si crea, si clona, si modifica, si rinomina o si elimina un account utente.

Per implementare correttamente le policy delle home directory, valutare le linee guida seguenti:

- Verificare che il percorso sia specificato nel formato corretto.
  - Per specificare un percorso per una sola home directory, utilizzare uno dei modelli riportati nella tabella seguente:

Tipo di condivisione	Modello di percorso
Windows	`\\computer\condivisione\`. Ad esempio, se si desidera che DRA crei automaticamente una home directory nella cartella `Home Share` nel computer server01, digitare `\\server01\Home Share\`.
Non Windows	`\\non windows\condivisione`

  - Per standardizzare l'amministrazione delle home directory nella directory radice della condivisione principale corrispondente, utilizzare la sintassi UNC (Universal Naming Convention), ad esempio `\\`*nome server*`\C:\`*percorso directory radice*.
  - Per specificare un percorso per home directory nidificate, utilizzare uno dei modelli riportati nella tabella seguente:

Tipo di condivisione	Modello di percorso
Windows	*computer**condivisione**prima directory**seconda directory*\ Ad esempio, se si desidera che DRA crei automaticamente una home directory in JSmith\Home directory all'interno della cartella della condivisione principale nel computer server01, digitare \\server01\Home Share\JSmith\Home.
Non Windows	*non windows**condivisione**prima directory**seconda directory*\

Nota: DRA supporta anche i formati seguenti: *computer**condivisione**nomeutente* e *computer**condivisione**%nomeutente%*. In tutti i casi, DRA crea automaticamente una home directory per l'account utente associato.

- Quando si definisce una policy o un trigger di automazione per gestire le home directory in NetApp Filer, è necessario utilizzare un formato diverso per specificare la directory.
  - Se si utilizza NetApp Filer, specificare la directory superiore nel formato seguente: *NomeFiler**condivisioneamministrativa:**percorsovolumeradice*h*percorsodirectory*.
  - La variabile della condivisione amministrativa è la condivisione nascosta che consente la mappatura con il volume radice in NetApp Filer, ad esempio *c$*. Ad esempio, se il percorso locale della condivisione in NetApp Filer, denominato usfiler, è c$\vol\vol0\mydirectory, è possibile specificare un percorso radice del tipo \\usfiler\c:\vol\vol0\mydirectory per NetApp Filer.
- Per specificare un percorso DFS durante la creazione delle home directory degli utenti o per configurare le policy delle home directory per gli utenti, utilizzare *server**radice*\<*collegamento*> formato, dove la radice può essere il dominio gestito o una directory radice autonoma nel formato seguente: *NomeFiler**condivisioneamministrativa:**percorsoradicevolume**percorsodirectory* **.**
- Creare una directory condivisa per memorizzare la home directory dell'account utente.
- Assicurarsi che DRA possa accedere al computer o alla condivisione indicata nel percorso.

Creazione della home directory quando si crea un account utente

Questa regola consente a DRA di creare automaticamente le home directory per i nuovi account utente. Quando viene creata una home directory, il server di amministrazione utilizza il percorso specificato nei campi **Home directory** della procedura guidata Crea utente. È possibile modificare successivamente questo percorso mediante la scheda Profilo della finestra delle proprietà utente e la home directory verrà spostata nella nuova ubicazione. Se non si specifica alcun valore in questi campi, non viene creata alcuna home directory per l'account utente.

In DRA è possibile impostare il livello di sicurezza per la nuova directory in base alle opzioni selezionate per le **autorizzazioni delle home directory**. Tali opzioni consentono di controllare l'accesso generale di tutte le home directory.

Ad esempio, è possibile specificare che i membri del gruppo di amministratori hanno il controllo completo mentre i membri del gruppo dell'help desk hanno accesso in lettura alla condivisione in cui vengono create le home directory degli utenti. Perciò, quando DRA crea una home directory utente, la nuova home directory può ereditare i diritti dalla directory superiore. Di conseguenza, i membri del gruppo di amministratori hanno il controllo completo su tutte le home directory degli utenti e i membri del gruppo dell'help desk hanno accesso in lettura a tutte le home directory degli utenti.

Se la home directory specificata esiste già, DRA non crea la home directory e non modifica le autorizzazioni di directory esistenti.

Ridenominazione della home directory quando si rinomina l'account utente

Questa regola consente l'esecuzione automatica delle azioni seguenti:

- Creare una home directory quando si specifica un nuovo percorso per la home directory
- Spostare il contenuto della home directory quando si modifica il percorso della home directory
- Rinominare una home directory quando si rinomina l'account utente

Quando si rinomina un account utente, la home directory esistente viene rinominata in base al nuovo nome dell'account. Se la home directory esistente è in uso, viene creata una nuova home directory con il nuovo nome e la home directory esistente non viene modificata.

Quando si modifica il percorso della home directory, DRA tenta di creare la home directory specificata e di spostare il contenuto della home directory precedente nella nuova ubicazione. È inoltre possibile configurare la policy delle home directory per creare una home directory senza spostare il contenuto dalla home directory esistente. Vengono anche applicati gli ACL assegnati dalla directory precedente alla nuova directory. Se la home directory specificata esiste già, DRA non crea una nuova directory e non modifica le autorizzazioni della directory esistente. Se la home directory precedente non è bloccata, viene eliminata.

Quando la ridenominazione della home directory ha esito negativo, DRA tenta di creare una nuova home directory con un nuovo nome e di copiare il contenuto dalla home directory precedente nella nuova home directory. DRA tenta quindi di eliminare la home directory precedente. È possibile configurare DRA affinché non copi il contenuto dalla home directory precedente a quella nuova, per spostare manualmente il contenuto dalla home directory precedente a quella nuova evitando problemi come la copia di file aperti.

Per eliminare la home directory precedente, DRA deve disporre dell'autorizzazione esplicita a eliminare i file e le sottodirectory di sola lettura dalla home directory precedente. È possibile fornire a DRA l'autorizzazione esplicita a eliminare i file e le sottodirectory di sola lettura dalla home directory precedente.

Directory o percorso superiore consentito per una condivisione principale

In DRA è possibile specificare le directory o i percorsi superiori consentiti per le condivisioni principali nei file server. Se è necessario specificare numerosi percorsi di directory o file server, è possibile esportarli in un file CSV e aggiungerli dal file CSV in DRA tramite la console di DRA. Le informazioni immesse nel campo **Allowable parent paths** (Percorsi superiori consentiti) vengono utilizzate in DRA per garantire che:

- Quando gli amministratori aggiunti eliminano un account utente e la home directory dell'account utente, la directory superiore non venga eliminata dal file server.
- Quando si rinomina un account utente o si modifica il percorso della home directory per un account utente, la home directory venga spostata in una directory o un percorso superiore valido nel file server.

Eliminazione della home directory quando si elimina l'account utente

Questa regola consente a DRA di eliminare automaticamente una home directory quando si elimina l'account utente associato. Se si abilita il Cestino, la home directory non viene eliminata fino a quando l'account utente non viene eliminato dal Cestino. Per eliminare la home directory, DRA deve disporre dell'autorizzazione esplicita a eliminare i file e le sottodirectory di sola lettura dalla home directory precedente. È possibile fornire a DRA l'autorizzazione esplicita a eliminare i file e le sottodirectory di sola lettura dalla home directory precedente.

Automazione e regole delle condivisioni principali

Con DRA è possibile automatizzare i task di manutenzione mediante la gestione delle condivisioni principali quando si modifica un account utente o si gestiscono le home directory. In DRA è possibile eseguire varie azioni quando si crea, si clona, si modifica, si rinomina o si elimina un account utente.

Per garantire la coerenza con le policy di sicurezza appropriate di Microsoft Windows, DRA non crea restrizioni di controllo dell'accesso a livello di nome della condivisione. Crea invece restrizioni di controllo dell'accesso solo a livello di directory. L'utilizzo di restrizioni di controllo dell'accesso a livello di nome della condivisione e di file o di oggetto Directory spesso rende confuso lo schema di accesso sia per gli amministratori che per gli utenti.

Nota: nell'ubicazione specificata deve essere presente una condivisione principale comune, ad esempio `HOMEDIRS`, un livello sopra le home directory.

Ad esempio, il percorso seguente è valido: *HOUSERV1**HOMEDIRS**%nomeutente%*

Il percorso seguente, invece, non è valido: *HOUSERV1**%nomeutente%*

Definizione dei nomi delle condivisioni principali

Quando si definiscono le regole di automazione delle condivisioni principali, è possibile specificare un prefisso e un suffisso per ogni condivisione principale creata automaticamente. Se si specifica un prefisso o un suffisso, è possibile applicare una convenzione di denominazione per le condivisioni principali.

Si supponga, ad esempio, di abilitare le regole di automazione per la creazione di home directory e condivisioni principali. Per la condivisione principale, si specifica come prefisso un carattere di sottolineatura e come suffisso un segno di dollaro. Quando si crea un utente denominato TomS, la sua nuova directory viene mappata nell'unità U e si specifica

`\\HOUSERV1\HOMEDIRS\%nomeutente%` come percorso di directory. In questo esempio, DRA crea una condivisione di rete denominata `_TomS$` che punta a `\\HOUSERV1\HOMEDIRS\TomS directory`.

Creazione di condivisioni principali per i nuovi account utente

Quando viene creata una condivisione principale, il server di amministrazione utilizza il percorso specificato nei campi **Home directory** della procedura guidata Crea utente. È possibile modificare successivamente questo percorso mediante la scheda Profilo della finestra delle proprietà utente.

In DRA il nome della condivisione viene creato aggiungendo al nome utente il prefisso e suffisso eventualmente specificati. Se si utilizzano nomi di account utente lunghi, DRA potrebbe non essere in grado di aggiungere il prefisso e il suffisso specificati per la condivisione principale. Il prefisso e il suffisso, come anche il numero di connessioni consentite, si basano sulle opzioni di creazione della condivisione principale che vengono selezionate.

Creazione di condivisioni principali per gli account utente clonati

Se il nome della condivisione principale generato dal nome dell'account utente appena creato esiste già, DRA elimina la condivisione esistente e ne crea una nuova nella home directory specificata.

Per clonare un account utente, il nome della condivisione dell'account utente deve esistere. Quando si clona un account utente, vengono clonate anche le informazioni della home directory per poi personalizzarle per il nuovo utente.

Modifica delle proprietà delle condivisioni principali

Quando si modifica l'ubicazione della home directory, DRA elimina la condivisione esistente e ne crea una nuova nella nuova home directory. Se la home directory originale è vuota, viene eliminata.

Ridenominazione delle condivisioni principali per gli account utenti rinominati

Quando si rinomina un account utente, DRA elimina la condivisione principale esistente e ne crea una nuova in base al nuovo nome dell'account. La nuova condivisione punta alla home directory esistente.

Eliminazione di condivisioni principali per account utente eliminati

Quando si elimina definitivamente un account utente, DRA elimina la condivisione principale.

Regole di gestione delle quote disco per il volume home

In DRA è possibile gestire le quote disco per i volumi home. È possibile implementare questa policy nei domini nativi in cui risiede la home directory in un computer Microsoft Windows. Per implementare la policy, è necessario specificare una quota disco di almeno 25 MB, affinché vi sia ampio spazio disponibile.

Abilitazione della funzione di generazione password

Questa funzione consente di specificare le impostazioni delle policy per le password generate da DRA. DRA non applica le impostazioni alle password create dagli utenti. Durante la configurazione delle proprietà delle policy delle password, la lunghezza della password non deve essere inferiore a 6 caratteri e superiore a 127 caratteri, tutti i valori possono essere impostati a zero, ad eccezione della lunghezza della password e del limite massimo.

Per configurare le policy di generazione password, passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Password Generation Policies** (Configura policy di generazione password) e selezionare la casella di controllo **Enable Password Policy** (Abilita policy password). Fare clic su **Password Settings** (Impostazioni password) e configurare le proprietà delle policy delle password.

Task delle policy

Per eliminare, abilitare o disabilitare le policy, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione).

Per eseguire una di queste azioni, passare a **Policy and Automation Management** (Gestione policy e automazione) > **Policy**. Fare clic con il pulsante destro del mouse sulla policy che si desidera eliminare, abilitare o disabilitare nel riquadro a destra e selezionare l'azione desiderata.

Implementazione di policy integrate

Per implementare le policy integrate, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione). Per ulteriori informazioni sulle policy integrate, vedere Caratteristiche delle policy integrate.

Nota: prima di associare la policy integrata a un amministratore aggiunto e a una vista ActiveView, assicurarsi che l'amministratore aggiunto sia assegnato a tale vista ActiveView.

Per implementare le policy integrate:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Policy**.
2. Nel menu Task, fare clic su **New Policy** (Nuova policy) e selezionare il tipo di policy integrata che si desidera creare.
3. Specificare i valori appropriati in ciascuna delle finestre della procedura guidata e fare clic su **Next** (Avanti). Ad esempio, è possibile associare la nuova policy a una vista ActiveView specifica, consentendo così a DRA di applicarla agli oggetti inclusi in tale vista ActiveView.
4. Verificare il riepilogo e fare clic su **Finish** (Fine).

Implementazione di policy personalizzate

Per implementare una policy personalizzata, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione).

Per implementare correttamente una policy personalizzata, è necessario scrivere uno script che viene eseguito durante un'operazione specifica (task amministrativo). È possibile associare un eseguibile o uno script all'operazione. DRA supporta script PowerShell sia a 32 bit che a 64 bit. Nello script della policy personalizzata è possibile definire i messaggi di errore da visualizzare ogni volta che un'azione viola la policy. È inoltre possibile specificare un messaggio di errore di default mediante la procedura guidata Create Policy (Crea policy).

Per ulteriori informazioni sulla creazione di policy personalizzate, la visualizzazione di un elenco di operazioni di amministrazione o l'utilizzo di matrici di argomenti, vedere l'SDK. Per ulteriori informazioni, vedere Creazione di script o eseguibili delle policy personalizzate.

Nota

- Prima di associare la policy personalizzata a un amministratore aggiunto e a una vista ActiveView, assicurarsi che l'amministratore aggiunto sia assegnato a tale vista ActiveView.
- Se il percorso dello script o dell'eseguibile della policy personalizzata contiene spazi, racchiudere il percorso tra virgolette (").

Per implementare una policy personalizzata:

1. Scrivere uno script o un eseguibile della policy.
2. Eseguire il login a un computer client DRA con un account a cui è assegnato il ruolo Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione) nel dominio gestito.
3. Avviare la Console di delega e configurazione.
4. Eseguire la connessione al server di amministrazione primario.
5. Nel riquadro a sinistra, espandere **Policy and Automation Management** (Gestione policy e automazione).
6. Fare clic su **Policy**.
7. Nel menu Task, fare clic su **New Policy > Create a Custom Policy** (Nuova policy > Crea policy personalizzata).
8. Specificare i valori appropriati in ciascuna delle finestre della procedura guidata e fare clic su **Next** (Avanti). Ad esempio, è possibile associare la nuova policy a una vista ActiveView specifica, consentendo così a DRA di applicarla agli oggetti inclusi in tale vista ActiveView.
9. Verificare il riepilogo e fare clic su **Finish** (Fine).

Modifica delle proprietà delle policy

Per modificare tutte le proprietà di una policy, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione).

Per modificare le proprietà delle policy:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Policy**.
2. Fare clic con il pulsante destro del mouse sulla policy da modificare e selezionare **Properties** (Proprietà).
3. Modificare le proprietà e le impostazioni desiderate della policy.

Creazione di script o eseguibili delle policy personalizzate

Per ulteriori informazioni sulla creazione di script o eseguibili delle policy personalizzate, vedere l'SDK.

Per accedere all'SDK:

1. Verificare di aver installato l'SDK nel computer in uso. Il programma di installazione crea una scorciatoia per l'SDK nel gruppo di programmi Directory and Resource Administrator. Per ulteriori informazioni, vedere l'elenco di controllo di installazione in Installazione del server di amministrazione DRA.
2. Fare clic sulla scorciatoia dell'SDK nel gruppo di programmi Directory and Resource Administrator.

Policy del client di delega e configurazione

La policy di denominazione automatica include tre configurazioni per le policy di Exchange che sono opzioni esclusive del client di delega e configurazione, a indicare che si tratta di una policy lato client.

Tale policy consente di specificare regole di denominazione automatiche per proprietà specifiche di una casella postale. Le opzioni permettono di stabilire convenzioni di denominazione e generare rapidamente valori standard per il nome visualizzato, il nome della directory e le proprietà dell'alias. Exchange consente di specificare stringhe di sostituzione, come ad esempio `%First` e `%Last`, per svariate opzioni di denominazione automatica.

Quando Exchange genera il nome di una directory o l'alias, verifica che il valore generato sia univoco. Se il valore generato non è univoco, viene aggiunto un segno meno (-) e un numero a due cifre, a partire da `-01`, per rendere univoco il valore. Quando Exchange genera un nome di visualizzazione, non verifica se il valore è univoco.

Per le policy di denominazione automatica e di generazione proxy, Exchange supporta le stringhe di sostituzione seguenti:

%First	**Indica il valore della proprietà Nome per l'account utente associato.**
%Last	Indica il valore della proprietà Cognome per l'account utente associato.
%Initials	Indica il valore della proprietà Iniziali per l'account utente associato.
%Alias	Indica il valore della proprietà Alias della casella postale.
%DirNam	Indica il valore della proprietà Nome directory della casella postale. Quando si generano indirizzi e-mail per le caselle postali di Microsoft Exchange, non sono supportate le stringhe di generazione proxy che specificano la variabile %DirName.
%UserName	Indica il valore della proprietà Nome utente per l'account utente associato.

È inoltre possibile specificare un numero racchiuso tra il segno di percentuale (%) e il nome della stringa di sostituzione, per indicare il numero di caratteri da includere da tale valore. Ad esempio, %2First indica i primi due caratteri dalla proprietà **Nome** dell'account utente.

Ogni regola di denominazione automatica o policy di generazione proxy può contenere una o più stringhe di sostituzione. In ciascuna regola è inoltre possibile specificare i caratteri di prefisso o suffisso per una stringa di sostituzione specifica, ad esempio un punto e uno spazio (.) dopo la stringa di sostituzione %Initials. Se la proprietà della stringa di sostituzione è vuota, Exchange non include il suffisso per tale proprietà.

Si consideri, ad esempio, la regola di denominazione automatica seguente per la proprietà **Nome visualizzato**:

```
%First %1Initials. %Last
```

Se la proprietà **Nome** è Roberta, la proprietà **Iniziali** è Maria e la proprietà **Cognome** è Bianchi, Exchange imposta la proprietà **Nome visualizzato** su Roberta M. Bianchi.

Se la proprietà **Nome** è Michele, la proprietà **Iniziali** è vuota e la proprietà **Cognome** è Gamberini, Exchange imposta la proprietà **Nome visualizzato** su Michele Gamberini.

Definizione di una policy di denominazione automatica per le caselle postali

Per specificare le opzioni di denominazione automatica delle caselle postali, è necessario disporre di poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), e la licenza deve includere il supporto per Exchange.

Per specificare una policy di denominazione automatica per le caselle postali:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange) > **Alias naming** (Denominazione alias).
2. Specificare le informazioni appropriate per generare i nomi.

3. Selezionare **Enforce alias naming rules during mailbox updates** (Applica regole di denominazione alias durante gli aggiornamenti delle caselle postali).
4. Fare clic su **OK**.

Definizione di una policy di denominazione delle risorse

Per specificare le opzioni di denominazione delle risorse, è necessario disporre di poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), e la licenza deve includere il supporto per Exchange.

Per specificare una policy di denominazione delle risorse:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange) > **Resource naming** (Denominazione risorse).
2. Specificare le informazioni appropriate per generare i nomi delle risorse.
3. Selezionare **Enforce resource naming rules during mailbox updates** (Applica regole di denominazione risorse durante gli aggiornamenti delle caselle postali).
4. Fare clic su **OK**.

Definizione di una policy di denominazione degli archivi

Per specificare le opzioni di denominazione degli archivi, è necessario disporre di poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione), e la licenza deve includere il supporto per Exchange.

Per specificare una policy di denominazione degli archivi:

1. Passare a **Policy and Automation Management** (Gestione policy e automazione) > **Configure Exchange Policies** (Configura policy di Exchange) > **Archive naming** (Denominazione archivi).
2. Specificare le informazioni appropriate per generare i nomi degli archivi per gli account utente.
3. Selezionare **Enforce archive naming rules during mailbox updates** (Applica regole di denominazione archivi durante gli aggiornamenti delle caselle postali).
4. Fare clic su **OK**.

14 Trigger di automazione pre e post task

Un trigger di automazione è una regola che associa uno script o un file eseguibile a una o più operazioni. Mediante lo script o il file eseguibile, è possibile automatizzare un workflow esistente e creare un ponte tra DRA e altri archivi di dati. I trigger di automazione consentono di estendere le funzionalità e la sicurezza offerte da DRA.

Per definire un trigger di automazione, è necessario impostare i parametri della regola, le operazioni che devono essere associate al trigger, quale script o file eseguibile deve essere eseguito e, se applicabile, quali viste ActiveView o amministratori aggiunti devono essere associati al trigger. Le regole determinano la modalità di applicazione del trigger da parte del server di amministrazione.

È inoltre possibile specificare uno script o un eseguibile di annullamento per il trigger. Uno **script di annullamento** consente di ripristinare le modifiche apportate in caso di esito negativo dell'operazione.

DRA supporta gli script VBScript e PowerShell.

Modalità di automazione dei processi del server di amministrazione

Oltre all'amministrazione basata su regole ActiveView, con DRA è possibile automatizzare i workflow esistenti ed eseguire automaticamente i task correlati mediante trigger di automazione. L'automazione dei workflow esistenti può semplificare le attività aziendali fornendo al contempo servizi migliori e più rapidi.

Quando il server di amministrazione esegue l'operazione associata al trigger di automazione, viene eseguito anche lo script o l'eseguibile del trigger. Se il trigger è del tipo pre-task, il server esegue lo script o l'eseguibile prima dell'operazione. Se il trigger è del tipo post-task, il server esegue lo script o l'eseguibile dopo l'operazione. Questo processo è denominato transazione. Una **transazione** è un ciclo completo d'implementazione per ciascuna operazione o task del server di amministrazione. Una transazione include le azioni necessarie per completare un'operazione, incluse tutte le eventuali azioni di annullamento che il server di amministrazione deve eseguire in caso di esito negativo dell'operazione.

Ogni volta che viene eseguito un trigger di automazione, il server di amministrazione immette lo stato del trigger nel log di revisione. Queste voci di log registrano il codice restituito, le operazioni associate, gli oggetti su cui sono state eseguite le operazioni e se lo script del trigger ha avuto esito positivo.

Avviso: i trigger di automazione vengono eseguiti utilizzando l'account del servizio del server di amministrazione. Poiché l'account del servizio dispone di autorizzazioni di amministratore, le policy e i trigger di automazione hanno un accesso completo a tutti i dati aziendali. Per definire i trigger di automazione, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione). I

trigger di automazione vengono eseguiti all'interno del contesto di sicurezza dell'account del servizio. Pertanto, gli amministratori aggiunti associati al ruolo Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione) potrebbero acquisire più potere del previsto.

Implementazione di un trigger di automazione

Per implementare i trigger di automazione, è innanzitutto necessario scrivere gli script o gli eseguibili dei trigger e disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Manage Policies and Automation Triggers (Gestisci policy e trigger di automazione).

Per implementare correttamente un trigger personalizzato, è necessario scrivere uno script che viene eseguito durante un'operazione specifica (task amministrativo). È possibile associare un eseguibile o uno script all'operazione. DRA supporta script PowerShell sia a 32 bit che a 64 bit. È possibile specificare se DRA deve applicare il trigger prima (pre-task) o dopo (post-task) l'esecuzione di un'operazione. Nello script del trigger è possibile definire i messaggi di errore da visualizzare nel caso in cui il trigger abbia esito negativo. È inoltre possibile specificare un messaggio di errore di default mediante la procedura guidata Create Automation Trigger (Crea trigger di automazione).

Per ulteriori informazioni sulla creazione di trigger personalizzati, la visualizzazione di un elenco di operazioni di amministrazione o l'utilizzo di matrici di argomenti, vedere l'*SDK*.

Nota

- Prima di associare il trigger di automazione personalizzato a un amministratore aggiunto e a una vista ActiveView, assicurarsi che l'amministratore aggiunto sia assegnato a tale vista ActiveView.
- Se il percorso dello script o dell'eseguibile del trigger personalizzato contiene spazi, racchiudere il percorso tra virgolette (").
- In questo caso, se l'operazione **UserSetInfo** viene utilizzata per un trigger di automazione degli script e viene modificato un attributo dell'utente (eseguendo il trigger), l'attributo modificato viene propagato nell'intera azienda solo dopo l'esecuzione di un'operazione **Find Now** (Trova ora) sull'oggetto utente.

Per implementare un trigger di automazione:

1. Scrivere lo script o il file eseguibile del trigger.
2. Eseguire il login a un computer client DRA con un account a cui è assegnato il ruolo **Manage Policies and Automation Triggers** (Gestisci policy e trigger di automazione) nel dominio gestito.
3. Avviare la Console di delega e configurazione.
4. Eseguire la connessione a un server di amministrazione primario.
5. Utilizzare Replica di file per effettuare l'upload del file di trigger nei server primari e secondari DRA.

   Il percorso della cartella deve esistere già su tutti i server DRA presenti nel dominio gestito. Questo percorso, incluso il file, verrà utilizzato in **Do file path** (Usa percorso file) della procedura guidata Automation Trigger (Trigger di automazione).
6. Nel riquadro a sinistra, espandere **Policy and Automation Management** (Gestione policy e automazione).

7. Fare clic su **Automation Triggers** (Trigger di automazione).
8. Nel menu Task, fare clic su **New Trigger** (Nuovo trigger).
9. Specificare i valori appropriati in ciascuna delle finestre della procedura guidata e fare clic su **Next** (Avanti). Ad esempio, è possibile associare il nuovo trigger a una vista ActiveView specifica, consentendo così a DRA di applicarlo quando gli amministratori aggiunti gestiscono oggetti inclusi in tale vista ActiveView.
10. Verificare il riepilogo e fare clic su **Finish** (Fine).

Importante: Se si dispone di più viste ActiveView configurate per un trigger mediante l'aggiunta di una virgola tra le viste ActiveViews, tali viste verranno biforcate nel trigger durante l'upgrade a una nuova versione di DRA e il trigger non verrà eseguito. Per consentire l'esecuzione dell'operazione dopo l'upgrade, è necessario riconfigurare il trigger oppure crearne uno nuovo.

---

15 Workflow automatizzato

Workflow Automation permette di automatizzare i processi IT mediante la creazione di moduli di workflow personalizzati che vengono eseguiti quando si esegue un workflow o quando vengono attivati da un evento workflow con nome creato nel server di Workflow Automation. Per creare un modulo di workflow, è necessario definire i gruppi di amministratori che possono visualizzarlo. L'invio di moduli o l'esecuzione di processi di workflow dipende dai poteri delegati al gruppo o ai gruppi inclusi durante la creazione del modulo di workflow.

Quando si creano o si modificano moduli di workflow, essi vengono salvati nel server Web. Gli amministratori aggiunti che eseguono il login alla Console Web per tale server hanno accesso ai moduli in base alla configurazione del modulo stesso. I moduli sono generalmente disponibili a tutti gli utenti con le credenziali del server Web. Per limitare l'accesso a un modulo specifico, è necessario aggiungere i gruppi di amministratori aggiunti e nascondere il modulo agli altri utenti. Per poter inviare il modulo, è necessario disporre di uno dei poteri seguenti:

- Create Workflow Event and Modify All Properties (Crea evento workflow e modifica tutte le proprietà)
- Start Workflow (Avvia workflow)

Avvio di un modulo di workflow: i workflow vengono creati sul server di Workflow Automation, che deve essere integrato con DRA tramite la Console di delega e configurazione. 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 le richieste di workflow configurate 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**.

È possibile modificare una richiesta esistente o crearne una nuova. Per modificare una richiesta esistente, passare a **Task** > **Richieste**.

Per creare una richiesta di workflow, passare ad **Amministrazione** > **Personalizzazione** > **Richieste**.

Per creare una richiesta, effettuare le operazioni di base descritte di seguito:

1. Configurare la richiesta per eseguire un *workflow specifico* quando viene inviato un modulo, oppure configurare la richiesta affinché venga eseguita quando attivata da un *evento con nome*.

2. Scegliere il gruppo o i gruppi di amministratori aggiunti inclusi nel processo di workflow e abilitare l'opzione **Il modulo è nascosto** nella scheda **Generale** per limitare l'accesso al modulo a tali utenti.
3. Aggiungere al modulo eventuali campi necessari o pagine delle proprietà aggiuntive.
4. Se applicabile, creare gestori personalizzati per definire ulteriormente il processo di workflow e la modalità di esecuzione.

   Nota: le opzioni del gestore personalizzato relative a una nuova richiesta di workflow non vengono esposte fino a quando non viene eseguito il salvataggio iniziale della richiesta. È possibile accedere, creare e modificare i gestori personalizzati in **Proprietà modulo**.

   ---

5. Disabilitare l'opzione **Il modulo è nascosto** per consentire agli utenti di visualizzare i moduli.

Per informazioni sulla configurazione del server di Workflow Automation, vedere Configurazione del server di Workflow Automation, per la personalizzazione delle richieste del workflow, vedere Personalizzazione dei moduli di richiesta.

VI Revisione e generazione di rapporti

La revisione delle azioni degli utenti è tra gli aspetti più importanti di un'implementazione efficace della sicurezza. Per consentire la revisione e la generazione di rapporti sulle azioni degli amministratori aggiunti, in DRA vengono registrate tutte le operazioni degli utenti nell'archivio dei log che risiede nel computer del server di amministrazione. DRA fornisce rapporti chiari e completi che includono valori precedenti e successivi agli eventi sottoposti a revisione, affinché sia possibile capire esattamente ciò che è cambiato.

16 Attività di revisione

L'attività di revisione dei log degli eventi consente di isolare, eseguire diagnosi e risolvere i problemi dell'ambiente in uso. In questa sezione vengono fornite informazioni utili per abilitare la registrazione degli eventi, comprendere questo processo e come utilizzare gli archivi dei log.

Registro eventi nativo di Windows

Per consentire la revisione e la generazione di rapporti sulle azioni degli amministratori aggiunti, in DRA vengono registrate tutte le operazioni degli utenti nell'archivio dei log che risiede nel computer del server di amministrazione. Le operazioni degli utenti includono tutti i tentativi di modificare le definizioni, ad esempio l'aggiornamento di account utente, l'eliminazione di gruppi o la ridefinizione di viste ActiveView. 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 scrittura degli eventi anche nei registri eventi di Windows.

Abilitazione e disabilitazione della revisione dei registri eventi di Windows per DRA

Quando si installa DRA, gli eventi di revisione non vengono registrati nel registro eventi di Windows per default. 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, consultare la Guida dell'Editor del Registro di sistema di Windows.

Per abilitare la revisione degli eventi:

1 Fare clic su **Start > Esegui**.

2 Digitare `regedit` nel campo **Apri** e fare clic su **OK**.

3 Espandere la chiave di registro seguente: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.

4 Fare clic su **Modifica > Nuovo > valore DWORD**.

5 Immettere `IsNTAuditEnabled` come nome della chiave.

6 Fare clic su **Modifica > Modifica**.

7 Immettere `1` nel campo **Dati valore** e fare clic su **OK**.

8 Chiudere l'editor del Registro di sistema.

Per disabilitare la revisione degli eventi:

1 Fare clic su **Start > Esegui**.

2 Digitare `regedit` nel campo **Apri** e fare clic su **OK**.

3 Espandere la chiave di registro seguente: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.

4 Selezionare la chiave `IsNTAuditEnabled`.

5 Fare clic su **Modifica > Modifica**.

6 Immettere `0` nel campo **Dati valore** e fare clic su **OK**.

7 Chiudere l'editor del Registro di sistema.

Integrità della revisione

Affinché tutte le azioni degli utenti vengano sottoposte a revisione, in DRA sono disponibili metodi alternativi di registrazione quando il prodotto non può verificare l'attività di registrazione. Quando si installa DRA, nel registro vengono aggiunti la chiave AuditFailsFilePath e il percorso per consentire le azioni seguenti:

- Se DRA rileva che gli eventi di revisione non vengono più registrati in un archivio dei log, esegue la registrazione di tali eventi in un file locale nel server di amministrazione.
- Se non è possibile scrivere gli eventi di revisione in un file locale, DRA esegue la scrittura nel registro eventi di Windows.
- Se non è possibile scrivere gli eventi di revisione nel registro eventi di Windows, il prodotto esegue la scrittura nel log di DRA.
- Se DRA rileva che gli eventi di revisione non vengono registrati, vengono bloccate anche le operazioni degli utenti.

Per abilitare le operazioni di scrittura quando l'archivio dei log non è disponibile, è necessario impostare anche un valore per la chiave AllowOperationsOnAuditFailure del registro.

Avviso: prestare attenzione quando si modifica il Registro di sistema 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, consultare la Guida dell'Editor del Registro di sistema di Windows.

Per abilitare le operazioni di scrittura:

1. Fare clic su **Start > Esegui**.
2. Digitare `regedit` nel campo **Apri** e fare clic su **OK**.
3. Espandere la chiave di registro seguente: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
4. Fare clic su **Modifica > Nuovo > valore DWORD**.
5. Immettere `AllowOperationsOnAuditFailure` come nome della chiave.
6. Fare clic su **Modifica > Modifica**.
7. Immettere 736458265 nel campo **Dati valore**.
8. Selezionare **Decimale** nel campo **Base** e fare clic su **OK**.
9. Chiudere l'editor del Registro di sistema.

Caratteristiche degli archivi dei log

In DRA i dati relativi all'attività degli utenti vengono registrati in archivi dei log che risiedono nel server di amministrazione. DRA crea partizioni giornaliere degli archivi dei log per memorizzare i dati raccolti e normalizzati nel corso della giornata. Come convenzione di denominazione per le partizioni degli archivi dei log viene utilizzata la data nell'ora locale del server di amministrazione (*AAAAMMGG*).

Se è stato abilitato il servizio di raccolta dei rapporti di gestione, i dati degli archivi dei log vengono esportati in un database SQL Server che funge da origine per i rapporti di gestione di DRA.

Inizialmente, i dati degli archivi dei log vengono conservati di default per un tempo illimitato in DRA. L'archivio dei log può raggiungere una dimensione massima stabilita in fase di installazione sulla base dello spazio disponibile sul disco rigido. Quando l'archivio dei log supera la dimensione massima, i nuovi eventi di revisione non vengono più memorizzati. È possibile impostare un limite di tempo per la permanenza dati, affinché DRA rimuova i dati più vecchi per lasciare spazio ai dati più recenti mediante un processo di pulitura. Prima di abilitare la pulitura, accertarsi di aver predisposto una strategia di backup. È possibile configurare il periodo di permanenza degli archivi dei log mediante l'utility Log Archive Configuration. Per ulteriori informazioni, vedere Modifica delle impostazioni di pulitura degli archivi dei log.

Utilizzo dell'utility Log Archive Viewer

Per visualizzare i dati memorizzati nei file di archivio dei log, utilizzare l'utility Log Archive Viewer. L'utility Log Archive Viewer è disponibile in NetIQ DRA Log Archive Resource Kit (LARK), che è possibile scegliere di installare insieme a DRA. Per ulteriori informazioni, vedere il documento *NetIQ DRA Log Archive Resource Kit Technical Reference* (Riferimento tecnico per NetIQ DRA Log Archive Resource Kit).

Backup dei file di archivio dei log

Un **file di archivio dei log** è una raccolta di blocchi di record. Poiché i file di archivio dei log sono file binari compressi che non risiedono in un database fisico, non è necessario utilizzare Microsoft SQL Server Management Studio per eseguire il backup degli archivi dei log. Se si dispone di un sistema automatico di backup dei file, il backup dei file di archivio dei log viene eseguito automaticamente come per qualsiasi altro file.

Per pianificare la strategia di backup, tenere presenti le best practice seguenti:

- Ogni giorno viene creata una partizione contenente i dati degli eventi relativi al giorno stesso. Quando si abilita la pulitura, il servizio di archiviazione log esegue automaticamente la pulitura dei dati in tali partizioni ogni 90 giorni per default. La strategia di backup deve tenere in considerazione la pianificazione della pulitura per determinare la frequenza dei backup. Quando le partizioni di archiviazione dei log vengono pulite, DRA elimina i file binari. I dati eliminati mediante la pulitura non possono essere recuperati e devono essere ripristinati da un backup. Per ulteriori informazioni, vedere Modifica delle impostazioni di pulitura degli archivi dei log.
- Il backup delle partizioni deve essere eseguito solo quando le partizioni sono chiuse. In condizioni normali, una partizione viene chiusa entro 2 ore dalla mezzanotte del giorno successivo.
- Eseguire il backup e il ripristino delle cartelle delle partizioni e delle relative sottocartelle come un'unica unità. Eseguire il backup del file `VolumeInfo.xml` nell'ambito del backup della partizione.
- Se si desidera ripristinare le partizioni di archivio dei log per i rapporti, verificare che il relativo backup mantenga il formato originale o sia possibile ripristinarlo.
- Quando si configura il processo per il backup dei file di archivio dei log, NetIQ consiglia di escludere le sottocartelle `index_data` e `CubeExport` ubicate nella cartella principale di archivio dei log. Queste sottocartelle contengono dati temporanei e il backup non deve essere eseguito.

Modifica delle impostazioni di pulitura degli archivi dei log

Quando si installa DRA, la pulitura degli archivi dei log è disabilitata per default. Quando si stabiliscono procedure di backup regolari per i file di archivio dei log, è necessario abilitare la pulitura degli archivi dei log per risparmiare spazio su disco. Per modificare il numero di giorni allo scadere dei quali viene eseguita la pulitura delle partizioni di archivio dei log, utilizzare l'utility Log Archive Configuration.

Per modificare il numero di giorni allo scadere dei quali viene eseguita la pulitura delle partizioni di archivio dei log:

1. Eseguire il login al server di amministrazione utilizzando un account che sia membro del gruppo di amministratori locale.
2. Avviare **Log Archive Configuration**nel gruppo di programmi NetIQ Administration.
3. Fare clic su **Log Archive Server Settings** (Impostazioni server archivio log).
4. *Se si desidera abilitare la pulitura delle partizioni,* impostare il valore del campo **Partition Grooming Enabled** (Pulitura partizioni abilitata) su True (Vero).

5 Digitare il numero di giorni per cui si desidera conservare le partizioni di archivio dei log prima della pulitura nel campo **Number of Days before Grooming** (Numero di giorni prima della pulitura).

6 Fare clic su **Apply** (Applica).

7 Fare clic su **Yes** (Sì).

8 Fare clic su **Close** (Chiudi).

9 Individuare il percorso della cartella *NetIQLogArchiveData*\<*Nome partizione*>, generalmente: `C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData`

Se l'attributo "File is ready for archiving" (File pronto per l'archiviazione) dei file o delle cartelle all'interno delle partizioni specificate non è selezionato (nelle proprietà del file o della cartella), è necessario modificare il file di configurazione per abilitare la pulitura degli archivi dei log. Per comprendere perché questo attributo potrebbe essere selezionato o meno, vedere la sezione **Additional Information** (Informazioni aggiuntive) nell'articolo della knowledgebase *How do you configure the data retention period for DRA Logarchival Data?* (Come si configura il periodo di conservazione dei dati per gli archivi dei log DRA?).

Se il valore è	
Selezionato	Fare clic su **Sì** nel messaggio di conferma per riavviare il servizio di archiviazione log di NetIQ Security Manager. **Nota:** se si modifica una qualsiasi impostazione di archiviazione dei log, per rendere effettive le modifiche è necessario riavviare il servizio di archiviazione log.
Non selezionato	Fare clic su **No** nel messaggio di conferma. Vedere Per abilitare il server di archiviazione log di DRA ed eseguire la pulitura dei dati non archiviati:.

Per abilitare il server di archiviazione log di DRA ed eseguire la pulitura dei dati non archiviati:

1 Eseguire localmente il login alla console Windows di ciascun server DRA come membro del gruppo di amministratori locale.

2 Utilizzare un editor di testo per aprire il file `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` e individuare la riga `<Property name="GroomUnarchivedData" value="false" />`.

3 Modificare `"false"` impostando `"true"` e salvare il file.

4 Riavviare il servizio NetIQ DRA LogArchive.

Nota: se si modifica una qualsiasi impostazione di archiviazione dei log, per rendere effettive le modifiche è necessario riavviare il servizio di archiviazione log.

17 Generazione di rapporti

In questa sezione vengono fornite informazioni sulle caratteristiche e sull'abilitazione della funzione di generazione di rapporti di DRA, sulla raccolta dati per i rapporti, sulla raccolta e la generazione di rapporti relativi all'ActiveView Analyzer e sull'accesso ai rapporti integrati.

In DRA sono disabilitate le funzioni e i rapporti non supportati dalla licenza. 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 Activity Detail (Dettagli attività) sono disponibili nella Console di delega e configurazione non appena si installa DRA e forniscono i dettagli più recenti sulle modifiche della rete.

- "Gestione della raccolta dati per la generazione di rapporti" a pagina 177
- "Rapporti integrati" a pagina 179

Gestione della raccolta dati per la generazione di rapporti

DRA Reporting fornisce due metodi per generare rapporti che consentono di visualizzare le ultime modifiche apportate nell'ambiente in uso e di raccogliere ed esaminare le definizioni di account utente, gruppi e risorse di dominio.

Rapporti di dettaglio delle attività

Questi rapporti, accessibili mediante la 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. La funzione di generazione di rapporti consente inoltre di visualizzare i dettagli del modello di sicurezza di DRA, ad esempio le definizioni delle viste ActiveView e dei gruppi di amministratori aggiunti.

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 di attività

Per ulteriori informazioni sulla configurazione della raccolta dati per i rapporti di gestione, vedere Configurazione dei rapporti.

Visualizzazione dello stato dei servizi di raccolta

È possibile visualizzare i dettagli di ciascun servizio di raccolta dati nella scheda Collectors Status (Stato servizi di raccolta).

Per visualizzare lo stato dei servizi di raccolta:

1. Espandere **Configuration Management** (Gestione configurazione) e fare clic su **Update Reporting Service Configuration** (Aggiorna configurazione servizio di generazione rapporti).
2. Nella scheda Collectors Status (Stato servizi di raccolta), fare clic su ciascuna voce per visualizzare ulteriori informazioni sulla raccolta dati, ad esempio quando è stata effettuata l'ultima raccolta e se ha avuto esito positivo.
3. Se non viene visualizzato alcun dato nell'elenco dei server, fare clic su **Refresh** (Aggiorna).

Abilitazione della generazione di rapporti e della raccolta dati

Dopo l'installazione dei componenti di DRA Reporting, abilitare e configurare la raccolta dati per i rapporti affinché sia possibile accedere ai rapporti con Reporting Center.

Per abilitare la generazione di rapporti e la raccolta dati:

1. Passare a **Configuration Management** (Gestione configurazione) > **Update Reporting Service Configuration** (Aggiorna configurazione servizio di generazione rapporti).
2. Nella scheda SQL Server, selezionare **Enable DRA Reporting support** (Abilita supporto per DRA Reporting).
3. Fare clic su **Browse** (Sfoglia) nel campo Server Name (Nome server) e selezionare il computer in cui è installato SQL Server.
4. Nella scheda Credentials (Credenziali), specificare le credenziali appropriate da utilizzare per le interazioni con SQL Server.
5. Se si tratta dello stesso account che può essere utilizzato per creare il database e inizializzare lo schema, selezionare la casella di controllo Use the above credentials for creating a database and initializing the database schema (Usa le credenziali precedenti per creare un database e inizializzare lo schema del database).
6. Se si desidera specificare un account diverso per la creazione di un database, specificare l'account utente e la password nella scheda Admin Credentials (Credenziali amministratore).
7. Fare clic su **OK**.

Per informazioni sulla configurazione specifica dei servizi di raccolta, vedere Configurazione dei rapporti.

Rapporti integrati

I rapporti integrati offrono la possibilità di generare rapporti sulle modifiche degli oggetti, sugli elenchi di oggetti e sui dettagli degli oggetti. Questi rapporti non fanno parte dei servizi DRA Reporting e non è necessaria alcuna configurazione per abilitare la generazione di rapporti di cronologia delle modifiche integrata. Per informazioni su come accedere a questi rapporti, fare riferimento agli argomenti trattati in questa sezione.

Nota: Se DRA è integrato con Change Guardian, è inoltre possibile accedere ai rapporti sulla cronologia delle modifiche per eventi esterni a DRA. Per informazioni su questi tipi di rapporti e sulla configurazione di un server Change Guardian, vedere "Configurare la Cronologia modifiche unificata" a pagina 112.

Generazione di rapporti sulle modifiche degli oggetti

È possibile visualizzare informazioni in tempo reale sulle modifiche degli oggetti nei domini in uso generando rapporti di dettaglio delle attività. Ad esempio, è possibile visualizzare un elenco di modifiche apportate a un oggetto o da un oggetto durante un intervallo di tempo specificato. È anche possibile esportare e stampare i rapporti di dettaglio delle attività.

Per generare rapporti sulle modifiche degli oggetti:

1. Individuare gli oggetti che corrispondono ai propri criteri.
2. Fare clic con il pulsante destro del mouse su un oggetto e selezionare **Reporting (Generazione di rapporti) > Changes made to objectName (Modifiche apportate a nomeOggetto)** o **Reporting (Generazione di rapporti) > Changes made by objectName (Modifiche apportate da nomeOggetto)**.
3. Selezionare le date di inizio e di fine per specificare le modifiche che si desidera visualizzare.
4. *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.

   ---

5. *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.
6. Fare clic su **OK**.

Generazione di rapporti sugli elenchi di oggetti

È possibile esportare o stampare i dati da elenchi di oggetti. Con questa funzione si possono generare rapporti e distribuire informazioni generali sugli oggetti gestiti in modo rapido e semplice.

Quando si esporta un elenco di oggetti, è possibile specificare l'ubicazione, il nome e il formato del file. DRA supporta i formati HTML, CSV e XML, per consentire l'esportazione delle informazioni in applicazioni di database o la pubblicazione di elenchi di risultati in una pagina Web.

Nota: è inoltre possibile selezionare più elementi in un elenco e copiarli in un'applicazione di elaborazione testo, ad esempio Blocco note.

Per generare rapporti su elenchi di oggetti:

1. Individuare gli oggetti che corrispondono ai propri criteri.
2. Per esportare l'elenco di oggetti, fare clic su **Export List** (Esporta elenco) nel menu File.
3. Per stampare l'elenco di oggetti, fare clic su **Print List** (Stampa elenco) nel menu File.
4. Specificare le informazioni appropriate per salvare o stampare l'elenco.

Generazione di rapporti sui dettagli degli oggetti

È possibile esportare o stampare i dati contenuti nelle schede dei dettagli in cui sono elencati gli attributi degli oggetti, come ad esempio le appartenenze a gruppi. Con questa funzione è possibile generare rapporti in modo rapido e semplice e distribuire i dettagli di uso frequente relativi a oggetti specifici.

Quando si esporta una scheda dei dettagli di un oggetto, è possibile specificare l'ubicazione, il nome e il formato del file. DRA supporta i formati HTML, CSV e XML, per consentire l'esportazione delle informazioni in applicazioni di database o la pubblicazione di elenchi di risultati in una pagina Web.

Per generare rapporti sui dettagli degli oggetti:

1. Individuare l'oggetto che corrisponde ai propri criteri.
2. Nel menu View (Visualizza), fare clic su **Details** (Dettagli).
3. Selezionare la scheda appropriata nel riquadro dei dettagli.
4. Per esportare i dettagli dell'oggetto, fare clic sull'elenco **Export Details** (Esporta dettagli) nel menu File.
5. Per stampare i dettagli dell'oggetto, fare clic su **Print Details List** (Stampa elenco dettagli) nel menu File.
6. Specificare le informazioni appropriate per salvare o stampare l'elenco.

VII Funzioni aggiuntive

Le assegnazioni temporanee al gruppo, i gruppi dinamici, la registrazione degli eventi e la password di recupero BitLocker sono funzioni aggiuntive di DRA che è possibile integrare nell'ambiente aziendale.

18 Assegnazioni temporanee al gruppo

DRA consente di creare assegnazioni temporanee al gruppo, così da fornire a utenti autorizzati l'accesso temporaneo alle risorse. Gli amministratori aggiunti possono utilizzare le assegnazioni temporanee al gruppo per inserire utenti in un gruppo di destinazione per un periodo di tempo specifico. Al termine di tale periodo, DRA rimuove automaticamente gli utenti dal gruppo.

Il ruolo Manage Temporary Group Assignments (Gestisci assegnazioni temporanee al gruppo) concede agli amministratori aggiunti i poteri necessari per creare e gestire assegnazioni temporanee al gruppo.

Gli amministratori aggiunti possono solo visualizzare le assegnazioni temporanee al gruppo per cui l'amministratore aggiunto dispone dei poteri per l'aggiunta o la rimozione dei membri.

Per delegare la creazione e la gestione di assegnazioni temporanee al gruppo, utilizzare i poteri seguenti:

- Create Temporary Group Assignments (Crea assegnazioni temporanee al gruppo)
- Delete Temporary Group Assignments (Elimina assegnazioni temporanee al gruppo)
- Modify Temporary Group Assignments (Modifica assegnazioni temporanee al gruppo)
- Reset Temporary Group Assignment State (Ripristina stato assegnazioni temporanee al gruppo)
- View Temporary Group Assignments (Visualizza assegnazioni temporanee al gruppo)
- Add Object to Group (Aggiungi oggetto a un gruppo)
- Remove Object from Group (Rimuovi oggetto da un gruppo)

Il gruppo e gli utenti di destinazione devono appartenere alla stessa vista ActiveView.

Nota

- Non è possibile creare un'assegnazione temporanea al gruppo per un utente che è già membro del gruppo di destinazione. Se si tenta di creare un'assegnazione temporanea al gruppo per un utente che è già membro del gruppo di destinazione, in DRA viene visualizzato un messaggio di avviso e l'assegnazione temporanea dell'utente al gruppo viene impedita.
- Se si crea un'assegnazione temporanea al gruppo per un utente che non è membro del gruppo di destinazione, l'utente viene rimosso dal gruppo quando l'assegnazione temporanea scade.

Esempio:

Bob, il manager delle Risorse umane, notifica a John, amministratore dell'help desk, che l'azienda ha assunto a tempo determinato un dipendente di nome Joe per un periodo di tempo specifico necessario al completamento di un progetto. John effettua i seguenti passaggi:

- Crea un'assegnazione temporanea al gruppo (TGA)
- Aggiunge all'assegnazione TGA un gruppo Risorse umane per i dipendenti temporanei

- Aggiunge Joe come membro del gruppo di dipendenti temporanei
- Imposta la durata dell'assegnazione TGA per un mese (dal 03/07/2019 al 02/08/2019)

Risultato previsto:

Per default, quando l'assegnazione TGA scadrà, Joe verrà rimosso dal gruppo Risorse umane. L'assegnazione TGA sarà disponibile per sette giorni a meno che John non abbia selezionato l'opzione per **Mantenere questa assegnazione temporanea al gruppo per utilizzi futuri**.

Per ulteriori informazioni sulla creazione e l'uso di assegnazioni temporanee al gruppo, vedere la *DRA User Guide* (Guida dell'utente di DRA).

19 Gruppi dinamici di DRA

Un gruppo dinamico è costituito da membri che variano in base a un set prestabilito di criteri che si configurano nelle proprietà del gruppo. È possibile rendere dinamico qualsiasi gruppo, come anche rimuovere tale filtro da qualsiasi gruppo in cui è stato configurato. Questa funzione consente inoltre di aggiungere membri del gruppo a un elenco statico o un elenco di esclusione. I membri del gruppo inseriti in questi elenchi non sono soggetti ai criteri di dinamicità.

Se si ripristina la condizione normale di un gruppo che era stato reso dinamico, tutti i membri eventualmente presenti nell'elenco dei membri statici vengono aggiunti all'appartenenza al gruppo, mentre i filtri di dinamicità e i membri esclusi vengono ignorati. È possibile rendere dinamici i gruppi esistenti oppure creare un nuovo gruppo dinamico sia nella Console di delega e configurazione che nella Console Web.

Per rendere dinamico un gruppo:

1. Individuare il gruppo nella console applicabile.
   - Console di delega e configurazione: passare a **Tutti i miei oggetti gestiti** > **Find Now** (Trova ora).

     Nota: per abilitare Generatore di query, fare clic su **Browse** (Sfoglia) e selezionare un dominio, un container o un'unità organizzativa.

   - Console Web: passare a **Gestione** > **Cerca**.
2. Aprire le proprietà del gruppo e selezionare **Rendi dinamico il gruppo** nella scheda Filtro membri dinamici.
3. Aggiungere gli attributi LDAP e virtuali desiderati per filtrare l'appartenenza al gruppo.
4. Aggiungere eventuali membri statici o esclusi al gruppo dinamico e applicare le modifiche.

Per creare un nuovo gruppo dinamico:

- **Console di delega e configurazione:** fare clic con il pulsante destro del mouse sul dominio o sul nodo secondario in Tutti i miei oggetti gestiti e selezionare **Nuovo** > **Gruppo dinamico**.
- **Console Web:** passare a **Gestione** > **Crea** > **Gruppo dinamico**.

20 Caratteristiche della registrazione eventi

Quando si configura un attributo per un tipo di oggetto e DRA esegue una delle operazioni supportate, tale attributo viene aggiornato (registrato) con le informazioni specifiche di DRA, incluso l'utente che ha eseguito l'operazione. Di conseguenza, AD genera un evento di revisione per la modifica dell'attributo.

Si supponga ad esempio di aver selezionato l'attributo `extensionAttribute1` come attributo utente e di aver configurato la revisione di AD DS. Ogni volta che un amministratore aggiunto aggiorna un utente, DRA aggiorna l'attributo `extensionAttribute1` con i dati di registrazione dell'evento. Ciò significa che insieme agli eventi AD DS per ogni attributo aggiornato dall'amministratore aggiunto (ad esempio descrizione, nome e così via) vi sarà un evento AD DS aggiuntivo per l'attributo `extensionAttribute1`.

Ciascuno di questi eventi contiene un ID di correlazione che è uguale per ogni attributo che è stato modificato durante l'aggiornamento dell'utente. In questo modo, le applicazioni possono associare i dati di registrazione degli eventi agli altri attributi che sono stati aggiornati.

Per i passaggi per l'abilitazione della registrazione degli eventi, vedere Abilitare la registrazione degli eventi in DRA.

Per un esempio di evento AD DS e i tipi di operazione supportati, vedere quanto riportato di seguito:

Evento AD DS

Tutte le volte che DRA esegue un'operazione supportata, nel registro eventi di Sicurezza di Windows appare un evento analogo a quello riportato di seguito.

Nome LDAP:	**`extensionAttribute1`**
Sintassi (OID): 2.5.5.12	2.5.5.12
Valore:	<dra-event **user**="DRDOM300\drauseradmin" **sid**="S-1-5-21-53918190-1560392134-2889063332-1914" **tid**="E0E257E6B4D24744A9B0FE3F86EC7038" **SubjectUserSid**="S-1-5-21-4224976940-2944197837-1672139851-500" **ObjectDN**="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/ >+a+02ROO+bJbhyPbR4leJpKWCGTp/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=

Il valore dell'evento è composto da due parti. La prima è una stringa XML contenente i dati di registrazione dell'evento. La seconda è una firma dei dati che può essere utilizzata per accertare che i dati siano stati effettivamente generati da DRA. Per convalidare la firma, l'applicazione deve disporre della chiave pubblica per la firma.

La stringa XML è costituita dalle informazioni seguenti:

User	Amministratore aggiunto che ha eseguito l'operazione
Sid	SID dell'amministratore aggiunto che ha eseguito l'operazione
Tid	ID della transazione di revisione di DRA per garantire che ogni evento sia univoco
SubjectUserSid	SID dell'account del servizio DRA o dell'account di accesso che ha effettivamente aggiornato AD
ObjectDN	Nome distinto dell'oggetto che è stato modificato

Operazioni supportate

Utente	◆ Crea ◆ Rinomina ◆ Modifica ◆ Clona
Gruppo	◆ Crea ◆ Rinomina ◆ Modifica ◆ Clona
Contatto	◆ Crea ◆ Rinomina ◆ Modifica ◆ Clona
Computer	◆ Crea ◆ Abilita ◆ Disabilita ◆ Rinomina ◆ Modifica
Unità organizzativa	◆ Crea ◆ Rinomina ◆ Clona

21 Password di recupero BitLocker

Microsoft BitLocker memorizza le proprie password di recupero in Active Directory. Grazie alla funzione Password di recupero BitLocker di DRA, è possibile delegare poteri agli amministratori aggiunti per individuare e recuperare le password di BitLocker smarrite 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** ed espandere la struttura ad albero.
2. Nel nodo **Account and Resource Management** (Gestione account e risorse), passare a **Tutti i miei oggetti gestiti** > **Dominio** > **Computer**.
3. Nell'elenco di computer, fare clic con il pulsante destro del mouse sul computer desiderato e selezionare **Proprietà**.
4. Fare clic sulla scheda **Password di recupero BitLocker** per visualizzare la password di recupero BitLocker.
5. Fare clic con il pulsante destro del mouse sulla password di recupero BitLocker, fare clic su **Copia** e incollare il testo nel file di testo o nel foglio di calcolo desiderato.

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.

Nota: Per cercare la password di recupero, l'amministratore aggiunto deve disporre del potere **View BitLocker recovery password** (Visualizza password di recupero BitLocker) sul dominio che contiene gli oggetti Computer delegati.

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

1. Avviare la console di **delega e configurazione** ed espandere la struttura ad albero.
2. Nel nodo **Account and Resource Management** (Gestione account e risorse), passare a **All My Managed Objects** (Tutti i miei oggetti gestiti), fare clic con il pulsante destro del mouse su **Managed Domain** (Dominio gestito) e successivamente su **Find BitLocker Recovery Password** (Trova password di recupero BitLocker).

   Per trovare i primi otto caratteri della password di recupero, vedere 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**.

22 Cestino

È possibile abilitare o disabilitare il Cestino per ciascun dominio Microsoft Windows o per gli oggetti all'interno di tali domini, per controllare la gestione degli account in tutta l'azienda. Se si abilita il Cestino e successivamente si elimina un account utente, un gruppo, un gruppo di distribuzione dinamico, un gruppo dinamico, una casella postale di una risorsa, un contatto o un account computer, il server di amministrazione disabilita l'account selezionato e lo sposta nel container Cestino. Quando l'account viene spostato nel Cestino, non appare più nelle viste ActiveView in cui era incluso. Se si elimina un account utente, un gruppo, un contatto o un account computer quando il Cestino è disabilitato, il server di amministrazione elimina definitivamente l'account selezionato. È possibile disabilitare un Cestino che contiene account eliminati in precedenza. Tuttavia, quando il Cestino è disabilitato, tali account non sono più disponibili nel nodo Cestino.

Assegnazione dei poteri del Cestino

Affinché un amministratore aggiunto possa eliminare definitivamente gli account dal nodo Tutti i miei oggetti gestiti e anche dal Cestino, assegnare il potere corrispondente fra quelli dell'elenco seguente:

- Delete User Account Permanently (Elimina definitivamente account utente)
- Delete Group Permanently (Elimina definitivamente gruppo)
- Delete Computer Permanently (Elimina definitivamente computer)
- Delete Contact Permanently (Elimina definitivamente contatto)
- Delete Dynamic Distribution Group Permanently (Elimina definitivamente gruppo di distribuzione dinamico)
- Delete Dynamic Group Account Permanently (Elimina definitivamente account gruppo dinamico)
- Delete Resource Mailbox Permanently (Elimina definitivamente casella postale risorsa)
- Delete Shared Mailbox Permanently (Elimina definitivamente casella postale condivisa)
- Delete Azure User Account Permanently (Elimina definitivamente account utente Azure)
- Delete Group Managed Service Account Permanently (Elimina definitivamente account del servizio gestito del gruppo)

Se più server di amministrazione gestiscono sottoalberi diversi dello stesso dominio Microsoft Windows, è possibile utilizzare il Cestino per visualizzare eventuali account eliminati da tale dominio indipendentemente da quale server di amministrazione gestisce l'account.

Utilizzo del Cestino

Mediante il Cestino è possibile eliminare definitivamente o ripristinare account, nonché visualizzare le proprietà di account eliminati. È anche possibile cercare account specifici e tenere traccia del numero di giorni di permanenza nel Cestino di un account eliminato. Anche nella finestra delle

proprietà di un dominio selezionato è disponibile la scheda Cestino. Da questa scheda è possibile disabilitare o abilitare il Cestino per tutto il dominio o per oggetti specifici, nonché pianificare una pulizia del Cestino.

Per ripristinare o eliminare in modo rapido e semplice gli account, utilizzare le opzioni **Restore All** (Ripristina tutto) o **Empty Recycle Bin** (Svuota cestino).

Quando si ripristina un account, DRA reintegra l'account con tutte le relative autorizzazioni, le deleghe di poteri, le assegnazioni delle policy, le appartenenze ai gruppi e alle viste ActiveView. Se si elimina definitivamente un account, DRA lo rimuove da Active Directory.

Per garantire l'eliminazione sicura degli account, solo gli amministratori aggiunti che hanno i poteri seguenti possono eliminare definitivamente gli account dal Cestino:

- Delete User Account Permanently (Elimina definitivamente account utente)
- Delete User from Recycle Bin (Elimina utente dal Cestino)
- Delete Group Account Permanently (Elimina definitivamente account gruppo)
- Delete Group from Recycle Bin (Elimina gruppo dal Cestino)
- Delete Computer Account Permanently (Elimina definitivamente account computer)
- Delete Computer from Recycle Bin (Elimina computer dal Cestino)
- Delete Contact Account Permanently (Elimina definitivamente account contatto)
- Delete Contact from Recycle Bin (Elimina contatto dal Cestino)
- Delete Dynamic Distribution Group Permanently (Elimina definitivamente gruppo di distribuzione dinamico)
- Delete Dynamic Distribution Group from Recycle Bin (Elimina gruppo di distribuzione dinamico dal Cestino)
- Delete Dynamic Group Permanently (Elimina definitivamente gruppo dinamico)
- Delete Dynamic Group from Recycle Bin (Elimina gruppo dinamico dal Cestino)
- Delete Resource Mailbox Permanently (Elimina definitivamente casella postale risorsa)
- Delete Resource Mailbox from Recycle Bin (Elimina casella postale risorsa dal Cestino)
- Delete Shared Mailbox Permanently (Elimina definitivamente casella postale condivisa)
- Delete Shared Mailbox from Recycle Bin (Elimina casella postale condivisa dal Cestino)
- View all Recycle Bin Objects (Visualizza tutti gli oggetti del Cestino)

Per ripristinare un account dal Cestino, gli amministratori aggiunti devono disporre dei poteri seguenti nell'unità organizzativa contenente l'account:

- Restore User From Recycle Bin (Ripristina utente dal Cestino)
- Restore Group from Recycle Bin (Ripristina gruppo dal Cestino)
- Restore Dynamic Distribution Group from Recycle Bin (Ripristina gruppo di distribuzione dinamico dal Cestino)
- Restore Dynamic Group from Recycle Bin (Ripristina gruppo dinamico dal Cestino)
- Restore Resource Mailbox from Recycle Bin (Ripristina casella postale risorsa dal Cestino)
- Restore Shared Mailbox from Recycle Bin (Ripristina casella postale condivisa dal Cestino)
- Restore Computer from Recycle Bin (Ripristina computer dal Cestino)

- Restore Contact from Recycle Bin (Ripristina contatto dal Cestino)
- View all Recycle Bin Objects (Visualizza tutti gli oggetti del Cestino)

Nota

- Se si elimina un account amministratore aggiunto spostandolo nel Cestino, in DRA vengono comunque visualizzate le assegnazioni a ruoli e viste ActiveView dell'account. Invece di visualizzare il nome dell'account amministratore aggiunto eliminato, viene visualizzato l'identificatore di sicurezza (SID). Prima di eliminare definitivamente l'account amministratore aggiunto, è possibile rimuovere le assegnazioni.
- Dopo l'eliminazione dell'account utente dal Cestino, DRA elimina la home directory.
- Se si elimina un utente che dispone di una licenza di Office 365, l'account utente viene spostato nel Cestino e la licenza rimossa. Se successivamente si ripristina l'account utente, anche la licenza di Office 365 viene ripristinata.

VIII Personalizzazione dei client

È possibile personalizzare il client di delega e configurazione e la Console Web. Per i client è necessario eseguire l'accesso fisicamente o in remoto e disporre delle credenziali dell'account. Per la Console Web, invece, sono necessari l'URL del server e le credenziali dell'account per eseguire il login da un browser Web.

23 Client di delega e configurazione

In questa sezione vengono fornite informazioni utili per personalizzare il client di delega e configurazione. In particolare viene descritto come creare in DRA pagine delle proprietà personalizzate, come creare strumenti personalizzati che possono essere eseguiti su computer client e server della rete e come personalizzare la configurazione dell'interfaccia utente.

Personalizzazione delle pagine delle proprietà

È possibile personalizzare ed estendere la Console di delega e configurazione implementando proprietà personalizzate. Le proprietà personalizzate consentono di aggiungere proprietà di account e OU proprietarie, come estensioni dello schema di Active Directory e attributi virtuali, a finestre specifiche delle procedure guidate e delle proprietà. Queste estensioni consentono di personalizzare DRA in base alle proprie esigenze specifiche. Tramite la procedura guidata New Custom Page (Nuova pagina personalizzata) nella Console di delega e configurazione, è possibile creare in modo rapido e semplice una pagina personalizzata per estendere l'interfaccia utente appropriata.

Se gli amministratori aggiunti necessitano di poteri univoci per gestire in modo sicuro la pagina personalizzata, è inoltre possibile creare e delegare poteri personalizzati. Potrebbe ad esempio essere necessario limitare la gestione degli account utente alle sole proprietà incluse nella pagina personalizzata. Per ulteriori informazioni, vedere Implementazione di poteri personalizzati.

Caratteristiche delle pagine delle proprietà personalizzate

Le estensioni dell'interfaccia utente sono pagine personalizzate che DRA visualizza nelle finestre appropriate di procedure guidate e proprietà. È possibile configurare pagine personalizzate per esporre attributi di Active Directory, estensioni dello schema e attributi virtuali nella Console di delega e configurazione.

Quando si seleziona un qualsiasi attributo di Active Directory, un'estensione dello schema o un attributo virtuale supportato, è possibile utilizzare le pagine personalizzate nei modi seguenti:

- Per limitare la gestione degli amministratori aggiunti a un set ben definito e controllato di proprietà. Il set di proprietà può includere *proprietà standard* ed estensioni dello schema. Le proprietà standard sono gli attributi di Active Directory esposti di default tramite la console di gestione di account e risorse.
- Per esporre attributi di Active Directory diversi dalle proprietà standard gestite da DRA.
- Per estendere la Console di delega e configurazione in modo da includere le proprietà proprietarie.

È inoltre possibile configurare le modalità di visualizzazione e applicazione di queste proprietà in DRA. Ad esempio, è possibile definire i controlli dell'interfaccia utente con valori di default delle proprietà.

In DRA le pagine personalizzate vengono applicate a tutti gli oggetti gestiti applicabili dell'azienda. Ad esempio, se si crea una pagina personalizzata per aggiungere estensioni dello schema di Active Directory alla finestra Group Properties (Proprietà gruppo), DRA applica le proprietà della pagina a ogni gruppo gestito in un dominio che supporta le estensioni dello schema specificate. Ciascuna pagina personalizzata deve includere un set univoco di proprietà. Non è possibile aggiungere un attributo di Active Directory a più di una pagina personalizzata.

Le singole finestre o le schede dell'interfaccia utente esistente non possono essere disabilitate. Un amministratore aggiunto può selezionare un valore della proprietà tramite l'interfaccia utente di default o una pagina personalizzata. DRA applica il valore di selezione più recente per una proprietà.

In DRA è disponibile un audit trail completo per le proprietà personalizzate e nel log degli eventi applicazione vengono registrati i dati seguenti:

- Modifiche apportate alle pagine personalizzate

  Importante: è necessario configurare manualmente la revisione dei log delle applicazioni Windows. Per ulteriori informazioni, vedere Abilitazione e disabilitazione della revisione dei registri eventi di Windows per DRA.

- Creazione ed eliminazione di pagine personalizzate
- Estensioni dello schema, attributi di Active Directory e attributi virtuali esposti inclusi nelle pagine personalizzate

È inoltre possibile eseguire rapporti sull'attività di modifica per controllare le modifiche di configurazione apportate alle proprietà personalizzate.

Le pagine personalizzate devono essere implementate e modificate dal server di amministrazione primario. Durante la sincronizzazione, DRA replica le configurazioni delle pagine personalizzate in tutto il set multimaster. Per ulteriori informazioni, vedere Configurazione del set multimaster.

Pagine personalizzate supportate

La creazione di pagine personalizzate consente di selezionare un set di proprietà di Active Directory, estensioni dello schema o attributi virtuali per esporre tali proprietà come scheda personalizzata. È possibile creare i tipi di pagine personalizzate elencati di seguito:

Pagina personalizzata dell'utente

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà utente
- Procedura guidata di creazione utente
- Procedura guidata di clonazione utente

Pagina personalizzata del gruppo

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà del gruppo
- Procedura guidata di creazione gruppo
- Procedura guidata di clonazione gruppo

Pagina personalizzata del computer

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà del computer
- Procedura guidata di creazione computer

Pagina personalizzata del contatto

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà del contatto
- Procedura guidata di creazione contatto
- Procedura guidata di clonazione contatto

Pagina personalizzata dell'unità organizzativa

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà dell'OU
- Procedura guidata di creazione OU
- Procedura guidata di clonazione OU

Pagina personalizzata della casella postale risorsa

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà della casella postale risorsa
- Procedura guidata di creazione casella postale risorsa
- Procedura guidata di clonazione casella postale risorsa

Pagina personalizzata del gruppo di distribuzione dinamico

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà del gruppo di distribuzione dinamico

- Procedura guidata di creazione gruppo di distribuzione dinamico
- Procedura guidata di clonazione gruppo di distribuzione dinamico

Pagina personalizzata della casella postale condivisa

Consente di visualizzare schede personalizzate nelle finestre seguenti:

- Finestra delle proprietà della casella postale condivisa
- Procedura guidata di creazione casella postale condivisa
- Procedura guidata di clonazione casella postale condivisa

Controlli supportati per le proprietà personalizzate

Quando si aggiunge un attributo di Active Directory, un'estensione dello schema o un attributo virtuale a una pagina personalizzata, è inoltre possibile configurare il controllo dell'interfaccia utente mediante il quale gli amministratori aggiunti immettono il valore della proprietà. Ad esempio, è possibile specificare i valori delle proprietà nei modi seguenti:

- Definendo gli intervalli di valori specifici
- Impostando i valori di default delle proprietà
- Indicando se una proprietà è obbligatoria

È inoltre possibile configurare il controllo dell'interfaccia utente per visualizzare informazioni proprietarie o istruzioni. Ad esempio, se si definisce un intervallo specifico per il numero di identificazione di un dipendente, è possibile configurare l'etichetta di controllo della casella di testo affinché visualizzi **Specificare il numero di identificazione del dipendente (da 001 a 100)**.

Ciascun controllo dell'interfaccia utente fornisce il supporto solo per un attributo di Active Directory, un'estensione dello schema o un attributo virtuale. Configurare i controlli seguenti dell'interfaccia utente in base al tipo di proprietà:

Tipo di attributo di Active Directory	Controlli supportati nell'interfaccia utente
Booleano	Casella di controllo
Data	Controllo di calendario
Numero intero	Casella di testo (default) Elenco di selezione
Stringa	Casella di testo (default) Elenco di selezione Selettore oggetti
Stringa multivalore	Elenco di selezione

Utilizzo delle pagine personalizzate

È possibile creare pagine personalizzate dal nodo User Interface Extensions (Estensioni interfaccia utente). Dopo aver creato la pagina, è possibile aggiungere o rimuovere le proprietà degli attributi di AD e disabilitare o eliminare la pagina. Per ogni personalizzazione che si desidera configurare, creare una pagina personalizzata e assegnare il potere o il ruolo appropriato all'amministratore aggiunto. Per l'utilizzo delle pagine personalizzate, valutare le best practice seguenti:

1. Affinché DRA riconosca gli attributi di Active Directory, gli attributi di estensione dello schema o gli attributi virtuali, riavviare il servizio NetIQ Administration Service in ciascun server di amministrazione.
2. Identificare il tipo di pagina personalizzata che si intende creare e le proprietà che si desidera vengano gestite dagli amministratori aggiunti mediante la pagina stessa. È possibile selezionare qualsiasi attributo di Active Directory, inclusi gli attributi di estensione dello schema e quelli delle procedure guidate e delle finestre delle proprietà esistenti in DRA o un qualsiasi attributo virtuale creato. Tuttavia, ciascuna pagina personalizzata deve includere un set univoco di proprietà. Non è possibile aggiungere un attributo di Active Directory a più di una pagina personalizzata.

   Le pagine personalizzate non sostituiscono l'interfaccia utente esistente. Per ulteriori informazioni, vedere Caratteristiche delle pagine delle proprietà personalizzate e Pagine personalizzate supportate.
3. Stabilire in che modo gli amministratori aggiunti dovranno specificare le proprietà. Ad esempio, si potrebbe voler limitare l'impostazione di una proprietà specificata a soli tre valori possibili. È possibile definire un controllo appropriato dell'interfaccia utente per ciascuna proprietà. Per ulteriori informazioni, vedere Controlli supportati per le proprietà personalizzate.
4. Stabilire se gli amministratori aggiunti necessitano di informazioni proprietarie o istruzioni per gestire correttamente le proprietà. Ad esempio, stabilire se Active Directory impone una sintassi per il valore della proprietà, come un nome distinto (DN) o un percorso LDAP.
5. Stabilire l'ordine in cui le proprietà devono essere visualizzate nella pagina personalizzata. È possibile modificare l'ordine di visualizzazione in qualsiasi momento.
6. Stabilire in che modo la pagina personalizzata deve essere utilizzata in DRA. Ad esempio, è possibile aggiungere una pagina personalizzata dell'utente alla procedura guidata New User (Nuovo utente) e alla finestra User Properties (Proprietà utente).
7. Utilizzare la scheda Assegnazioni del riquadro dei dettagli Amministratore aggiunto per verificare che gli amministratori aggiunti dispongano dei poteri appropriati per il set di oggetti corretto. Se sono stati creati poteri personalizzati per la pagina personalizzata, delegare i poteri agli amministratori aggiunti appropriati.
8. Stabilire se gli amministratori aggiunti necessitano di un potere personalizzato per gestire le proprietà della pagina. Ad esempio, se si aggiunge una pagina personalizzata alla finestra User Properties (Proprietà utente), delegando il potere *Modify All User Properties* (Modifica tutte le proprietà utente), l'amministratore aggiunto potrebbe acquisire eccessivo potere. Creare tutti i poteri personalizzati necessari per implementare la pagina personalizzata. Per ulteriori informazioni, vedere Implementazione di poteri personalizzati.
9. In base alle scelte effettuate nei passaggi precedenti, creare le pagine personalizzate appropriate.
10. Distribuire agli amministratori aggiunti appropriati (ad esempio all'help desk) le informazioni relative alle pagine personalizzate delle proprietà che sono state implementate.

Per implementare la personalizzazione delle proprietà, è necessario disporre dei poteri inclusi nel ruolo DRA Administration (Amministrazione DRA). Per ulteriori informazioni sulle pagine personalizzate, vedere Caratteristiche delle pagine delle proprietà personalizzate.

Creazione di pagine personalizzate delle proprietà

È possibile creare proprietà personalizzate diverse mediante la creazione di pagine personalizzate differenti. Le nuove pagine personalizzate sono abilitate di default.

Quando si crea una pagina personalizzata, è possibile disabilitarla. Le pagine personalizzate disabilitate non appaiono nell'interfaccia utente. Se si creano più pagine personalizzate, può essere opportuno disabilitarle in attesa di aver completato e provato le personalizzazioni.

Nota: gli account computer ereditano gli attributi di Active Directory dagli account utente. Se si estende lo schema di Active Directory includendo attributi aggiuntivi per gli account utente, è possibile selezionare tali attributi quando si crea una pagina personalizzata per gestire gli account computer.

Per creare una pagina personalizzata delle proprietà:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **User Interface Extensions** (Estensioni interfaccia utente).
2. Nel menu Task, fare clic su **New** (Nuovo) e scegliere la voce di menu appropriata per la pagina personalizzata che si desidera creare.
3. Nella scheda General (Generale), digitare il nome della pagina personalizzata e fare clic su **OK**. Se si desidera disabilitare la pagina, deselezionare la casella di controllo **Enabled** (Abilitato).
4. Per ciascuna proprietà che si desidera includere nella pagina personalizzata, effettuare le operazioni seguenti:
   - **4a** Nella scheda Proprietà fare clic su **Add** (Aggiungi).
   - **4b** Per selezionare una proprietà, fare clic su **Browse** (Sfoglia).
   - **4c** Nel campo **Control label** (Etichetta controllo), digitare il nome della proprietà da utilizzare in DRA come etichetta per il controllo dell'interfaccia utente. Verificare che l'etichetta di controllo sia facile da comprendere e descrittiva. È anche possibile includere istruzioni, intervalli di valori validi ed esempi di sintassi.
   - **4d** Selezionare il controllo appropriato per l'interfaccia utente nel menu **Control type** (Tipo di controllo).
   - **4e** Selezionare in quale posizione della Console di delega e configurazione si desidera visualizzare la pagina personalizzata.
   - **4f** Per specificare attributi aggiuntivi, quali la lunghezza minima o i valori di default, fare clic su **Advanced** (Avanzate).
   - **4g** Fare clic su **OK**.
5. Per modificare l'ordine di visualizzazione delle proprietà nella pagina personalizzata in DRA, selezionare la proprietà desiderata e fare clic su **Sposta su** o **Sposta giù**.
6. Fare clic su **OK**.

Modifica delle proprietà personalizzate

È possibile modificare una pagina personalizzata modificando le proprietà personalizzate.

Per modificare le proprietà personalizzate:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **User Interface Extensions** (Estensioni interfaccia utente).
2. Nel riquadro dell'elenco, selezionare la pagina personalizzata che si desidera.
3. Nel menu Task, fare clic su **Properties** (Proprietà).
4. Modificare le proprietà e le impostazioni desiderate della pagina personalizzata.
5. Fare clic su **OK**.

Identificazione degli attributi di Active Directory gestiti con le pagine personalizzate

È possibile identificare rapidamente le proprietà di Active Directory, le estensioni dello schema o gli attributi virtuali che vengono gestiti mediante una pagina personalizzata specifica.

Per identificare le proprietà di Active Directory gestite mediante pagine personalizzate:

1. Passare al nodo **Configuration Management** (Gestione configurazione) > **User Interface Extensions** (Estensioni interfaccia utente).
2. Nel riquadro dell'elenco, selezionare la pagina personalizzata che si desidera.
3. Nel riquadro dei dettagli, fare clic sulla scheda **Properties** (Proprietà). Per visualizzare il riquadro dei dettagli, fare clic su **Details** (Dettagli) nel menu View (Visualizza).
4. Per verificare le modalità di visualizzazione e applicazione di una proprietà in DRA, selezionare l'attributo di Active Directory, l'estensione dello schema o l'attributo virtuale appropriato nell'elenco e fare clic sull'icona **Proprietà**.

Abilitazione, disabilitazione ed eliminazione di pagine personalizzate

Quando si abilita una pagina personalizzata, la pagina personalizzata viene aggiunta alle procedure guidate e alle finestre associate. Per specificare in quali procedure guidate e finestre visualizzare una pagina personalizzata, modificare le proprietà della pagina personalizzata.

Nota: affinché in ciascuna pagina personalizzata appaia un set univoco di proprietà, le pagine personalizzate che contengono proprietà visibili in altre pagine personalizzate non vengono abilitate in DRA.

Quando si disabilita una pagina personalizzata, la pagina personalizzata viene rimossa dalle relative procedure guidate e finestre. DRA non elimina la pagina personalizzata. Per essere certi che una pagina personalizzata non venga mai visualizzata nell'interfaccia utente, eliminarla.

Quando si elimina una pagina personalizzata, la pagina personalizzata viene rimossa dalle relative procedure guidate e finestre. Non è possibile ripristinare una pagina personalizzata eliminata. Per rimuovere temporaneamente una pagina personalizzata dall'interfaccia utente, disabilitarla.

Per abilitare, disabilitare o eliminare una pagina personalizzata, passare al nodo **Configuration Management** (Gestione configurazione) > **User Interface Extensions** (Estensioni interfaccia utente) e selezionare l'azione desiderata nel menu Task o nel menu di scelta rapida.

Interfaccia della riga di comando

L'interfaccia della riga di comando consente di accedere a potenti funzionalità di amministrazione del prodotto e applicarle utilizzando comandi o file batch. Con l'interfaccia della riga di comando è possibile generare un comando per implementare modifiche su più oggetti.

Ad esempio, se è necessario trasferire le home directory di 200 dipendenti in un nuovo server, è possibile utilizzare l'interfaccia della riga di comando e immettere il seguente comando singolo per modificare tutti i 200 account utente:

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

Questo comando istruisce DRA affinché modifichi il campo della home directory di ciascuno dei 200 account utente dei gruppi HOU_SALES e HOU_MIS, impostando \\HOU2\USERS*id_utente*. Per eseguire questo task con gli strumenti di amministrazione nativi di Microsoft Windows, è necessario effettuare come minimo 200 azioni separate.

Nota: lo strumento dell'interfaccia della riga di comando diventerà obsoleto nelle versioni future, poiché verranno aggiunte ulteriori funzioni in PowerShell.

Strumenti personalizzati

Gli strumenti personalizzati possono essere utilizzati per richiamare qualsiasi applicazione da eseguire su computer client e server della rete tramite la selezione di un account Active Directory gestito in DRA.

In DRA sono supportati due tipi di strumenti personalizzati:

- Strumenti personalizzati che avviano utility desktop comuni, ad esempio Microsoft Office
- Strumenti personalizzati creati e distribuiti in ciascun computer client DRA

È possibile creare uno strumento personalizzato che avvia una scansione antivirus in tutti i computer in cui è installato il client DRA. È inoltre possibile creare uno strumento personalizzato che avvia un'applicazione o uno strumento esterno che richiede a DRA di aggiornare periodicamente uno script. Questi aggiornamenti periodici possono essere modifiche della configurazione o della regola di business. Dopo gli aggiornamenti periodici, DRA replica gli strumenti personalizzati dal server di amministrazione primario a eventuali server di amministrazione secondari e computer client DRA.

Per comprendere come gli strumenti personalizzati vengono replicati nel set multimaster di server, vedere Replica di file.

Creazione di strumenti personalizzati

È possibile creare strumenti personalizzati nel server primario di DRA utilizzando l'associazione a un oggetto Active Directory specifico o a tutti gli oggetti Active Directory visualizzati nella procedura guidata di creazione dello strumento personalizzato. Viene quindi eseguita la replica nei server secondari dell'MMS e nei client DRA mediante la replica dei file.

Un nuovo strumento personalizzato crea, se necessario, un menu e un sottomenu per richiamare in DRA l'operazione da eseguire su uno o più oggetti Active Directory.

È possibile delegare poteri agli amministratori aggiunti affinché possano creare ed eseguire strumenti personalizzati, nonché accedere all'applicazione ed eseguirla.

Durante la creazione di uno strumento personalizzato, è necessario immettere i parametri come descritto di seguito.

Scheda Generale

1. **Nome:** consente di specificare il nome dello strumento desiderato.
2. **Menu e sottomenu:** per creare una voce di menu per un nuovo strumento personalizzato, immettere il titolo del menu nel campo **Menu and Submenu Structure** (Struttura menu e sottomenu). Quando si crea uno strumento personalizzato e si seleziona l'oggetto, nel menu Task, nel menu di scelta rapida e nella barra degli strumenti di DRA viene visualizzata la voce di menu dello strumento personalizzato utilizzando la struttura di menu e sottomenu specificata.

   Struttura di esempio di menu e sottomenu: digitare il nome della voce di menu, una barra rovesciata (\) e il nome della voce di sottomenu.

   Per creare un tasto di scelta rapida: digitare una e commerciale (&) prima del nome della voce di menu.

   a. Esempio: `SendEmail\ApproveAction` --- `SendEmail` è il menu e `ApproveAction` è il sottomenu con la prima lettera "A" di `ApproveAction` che funge da tasto di scelta rapida.
3. **Enabled (Abilitato):** selezionare questa casella di controllo per attivare lo strumento personalizzato.
4. **Description (Descrizione):** è possibile aggiungere la descrizione desiderata.
5. **Comment (Commento):** è possibile aggiungere eventuali commenti necessari allo strumento personalizzato.

Scheda Supported Objects (Oggetti supportati)

Selezionare l'oggetto o tutti gli oggetti AD desiderati a cui lo strumento personalizzato creato deve essere associato.

Le opzioni per gli strumenti personalizzati attualmente supportate sono: Dominio gestito, Container, Utenti, Contatti, Gruppi, Computer, Unità organizzativa e Published Printers (Stampanti pubblicate).

Nota: altri oggetti di recente introduzione come Casella postale risorsa, Gruppo dinamico ed Exchange Dynamic Group (Gruppo dinamico Exchange) non sono supportati dagli strumenti personalizzati.

Scheda Application Settings (Impostazioni applicazione)

Location of the application (Ubicazione dell'applicazione): è necessario specificare il percorso/ubicazione in cui l'applicazione è installata, sia copiando e incollando il percorso esatto dell'applicazione che utilizzando l'opzione **Insert** (Inserisci).

Lo stesso percorso deve esistere già su tutti i server DRA nell'MMS. Se necessario, è possibile utilizzare Replica di file per effettuare l'upload di un file e replicarlo in un percorso utilizzabile sui server MMS prima di creare un nuovo strumento personalizzato.

È inoltre possibile utilizzare le variabili di DRA, le variabili di ambiente e i valori del registro per specificare l'ubicazione di un'applicazione esterna nel campo Location of the application (Ubicazione dell'applicazione). Per utilizzare queste variabili, fare clic su **Insert** (Inserisci) e selezionare la variabile che si desidera utilizzare.

Dopo aver inserito la variabile, digitare una barra rovesciata (\) e specificare la parte restante del percorso dell'applicazione, incluso il nome del relativo file eseguibile.

Esempi:

- *Esempio 1:* per specificare l'ubicazione di un'applicazione esterna che verrà eseguita dallo strumento personalizzato, selezionare la variabile di ambiente {%PROGRAMFILES%} e specificare la parte restante del percorso dell'applicazione nel campo Location of the application (Ubicazione dell'applicazione): {%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe

  ---

  Nota: in DRA è disponibile come esempio il valore del Registro di sistema della directory di installazione di Office. Per specificare come valore una chiave del Registro di sistema che contiene un percorso, utilizzare la sintassi seguente: {HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}

- *Esempio 2:* per specificare l'ubicazione di un file script personalizzato che verrà eseguito dallo strumento personalizzato, selezionare la variabile di DRA {Percorso_File_Replicati_DRA} e specificare la parte restante del percorso del file script nel campo Location of the application (Ubicazione dell'applicazione): {Percorso_File_Replicati_DRA}\cscript.vbs; dove {Percorso_File_Replicati_DRA} è il percorso del file replicato o la cartella {DirInstallazioneDRA}\FileTransfer\Replicate nel server di amministrazione.

  Nota: prima di creare lo strumento personalizzato, effettuare l'upload del file script nel server di amministrazione primario utilizzando la funzione di replica dei file. La funzione di replica dei file esegue l'upload del file script nella cartella {DirInstallazioneDRA} \FileTransfer\Replicate nel server di amministrazione primario.

- *Esempio 3:* per specificare l'ubicazione dell'utility di DRA che verrà eseguita dallo strumento personalizzato, selezionare la variabile di DRA {Percorso_Applicazione_DRA} e specificare la parte restante del percorso nel campo Location of the application (Ubicazione dell'applicazione): {Percorso_Applicazione_DRA}\DRADiagnosticUtil.exe, dove {Percorso_Applicazione_DRA} è l'ubicazione in cui è installato DRA.
- *Esempio 4:* è sufficiente copiare e incollare l'ubicazione dell'applicazione insieme al nome del file dell'applicazione con l'estensione.

Parametri da trasferire all'applicazione: per definire un parametro da trasferire a un'applicazione esterna, copiare e incollare oppure digitare uno o più parametri nel campo Parameters to pass to the application (Parametri da trasferire all'applicazione). In DRA sono disponibili parametri che è possibile utilizzare nel campo Parameters to pass to the application (Parametri da trasferire all'applicazione). Per utilizzare questi parametri, fare clic su Insert (Inserisci) e selezionare il parametro o i parametri che si desidera utilizzare. Quando si fornisce una proprietà dell'oggetto come parametro, accertarsi che l'amministratore aggiunto disponga dell'autorizzazione di lettura necessaria per la proprietà dell'oggetto oltre al potere *Execute Custom Tools* (Esegui strumenti personalizzati) per eseguire lo strumento personalizzato.

Esempi:

- *Esempio 1:*per trasferire i nomi di gruppo e dominio come parametri a un'applicazione esterna o uno script, selezionare i parametri Object Property Name (Nome proprietà oggetto) e Domain Property Name (Nome proprietà dominio) e specificare i nomi dei parametri nel campo Parameters to pass to the application field (Parametri da trasferire all'applicazione): `"{Object.Name}" "{Domain.$McsName}"`
- *Esempio 2:* per trasferire il parametro di input "ipconfig" per l'applicazione "C:\Windows\SysWOW64\cmd.exe", digitare semplicemente `"{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}"` nel campo.

Directory where the application will run (Directory in cui verrà eseguita l'applicazione): si tratta dell'ubicazione in cui l'applicazione deve essere eseguita nel computer client o server. È necessario trasferire il percorso in cui l'applicazione deve essere eseguita. È inoltre possibile utilizzare l'opzione Insert (Inserisci) nello stesso modo in cui si trasferisce il parametro per il campo Location of the application (Ubicazione dell'applicazione). Il significato degli altri parametri di questa scheda è implicito e non necessita di spiegazioni.

Personalizzazione dell'interfaccia utente

Sono disponibili svariate opzioni per personalizzare la configurazione della Console di delega e configurazione. La maggior parte di queste opzioni offre la possibilità di nascondere, mostrare o riconfigurare funzioni nei vari riquadri delle funzioni dell'applicazione. È possibile anche nascondere o mostrare la barra degli strumenti, personalizzare il titolo dell'applicazione e aggiungere, rimuovere o riordinare le colonne. Tutte le opzioni di personalizzazione sono disponibili nel menu **View** (Visualizza).

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 opzioni appropriate e fare clic su **OK**. Per ulteriori informazioni, fare clic sull'icona **?**.

Personalizzazione delle colonne dell'elenco

È possibile selezionare le proprietà degli oggetti che vengono visualizzati nelle colonne degli elenchi di DRA. Questa funzione flessibile permette di personalizzare l'interfaccia utente, ad esempio gli elenchi dei risultati delle ricerche, per soddisfare al meglio le esigenze amministrative specifiche dell'azienda. Ad esempio, è possibile impostare le colonne per visualizzare il nome di login dell'utente o il tipo di gruppo, così da individuare in modo rapido ed efficiente i dati necessari e ordinarli.

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**.

24 Client Web

Nel client Web, è possibile personalizzare le proprietà degli oggetti, i moduli di Workflow Automation e il branding dell'interfaccia utente. Se implementate correttamente, le personalizzazioni di proprietà e workflow contribuiscono ad automatizzare i task degli amministratori aggiunti durante la gestione degli oggetti e l'invio di workflow automatizzati.

Personalizzazione delle pagine delle proprietà

È possibile personalizzare in base al tipo di oggetto i moduli delle proprietà degli oggetti che gli amministratori aggiunti utilizzano nei loro ruoli di gestione di Active Directory. A tale scopo è necessario creare e personalizzare nuove pagine degli oggetti basate sui tipi integrati in DRA. È anche possibile modificare le proprietà dei tipi di oggetti integrati.

Gli oggetti delle proprietà sono chiaramente definiti nell'elenco Personalizzazione > 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 come amministratore 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'utilizzo dei gestori personalizzati, vedere la sezione Aggiunta di gestori personalizzati.

Definizione di filtri personalizzati

È possibile utilizzare i filtri per personalizzare le informazioni visualizzate per ciascun tipo di oggetto aggiungendo il campo **Browser oggetti gestiti** a una pagina delle proprietà. Quando si configurano le impostazioni dei campi, è possibile aggiungere filtri alle impostazioni tramite la scheda Opzioni browser oggetti gestiti. Definendo filtri personalizzati, è possibile limitare le informazioni visualizzate nei browser degli oggetti per gli amministratori aggiunti. Gli amministratori aggiunti possono visualizzare solo gli oggetti che soddisfano le condizioni del filtro definite.

Per definire un filtro, abilitare la casella di controllo **Specifica filtri oggetto** nella scheda Opzioni browser oggetti gestiti. Per ciascuna condizione del filtro, specificare il tipo di oggetto, l'attributo da filtrare, la condizione del filtro e il valore dell'attributo da utilizzare per filtrare le informazioni. Quando si creano più filtri per lo stesso tipo di oggetto, questi vengono combinati con l'operatore AND. Con tutti i filtri predefiniti nel Browser degli oggetti gestiti, gli amministratori aggiunti possono eseguire l'operazione di ricerca.

Nota

- Per definire i filtri è possibile utilizzare solo gli attributi memorizzati nella cache.
- Se si crea un gestore personalizzato utilizzando uno script personalizzato per il filtro personalizzato, è necessario anche definire manualmente il filtro personalizzato nella scheda **Opzioni browser oggetti gestiti** per il funzionamento del gestore personalizzato.

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 come amministratore di DRA.

2 Accedere ad **Amministrazione** > **Personalizzazione** > **Pagine delle proprietà**.

3 Fare clic su + **Crea**.

4 Creare il modulo iniziale delle proprietà dell'oggetto definendo il nome dell'azione, l'icona, il tipo dell'oggetto e la configurazione dell'operazione.

   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.

5 Personalizzare il nuovo modulo in base alle esigenze. Vedere la sezione Personalizzazione di una pagina delle proprietà di un oggetto.

Personalizzazione dei moduli di richiesta

Quando vengono creati o modificati, i moduli di richiesta vengono salvati sul server Web. L'amministratore DRA può gestirli da **Amministrazione** > **Personalizzazione** > **Richieste**. Gli amministratori aggiunti possono gestirli da **Task** > **Richieste**. Questi moduli sono utili per inviare workflow automatizzati che vengono creati nel server di Workflow Automation. I creatori di moduli utilizzano queste richieste per automatizzare e migliorare ulteriormente i task di gestione degli oggetti.

È possibile aggiungere e modificare proprietà dei moduli e gestori personalizzati esistenti. Il comportamento dell'interfaccia per l'aggiunta e la personalizzazione delle proprietà nei moduli di Workflow Automation è generalmente analogo a quello della personalizzazione delle proprietà dell'oggetto, a eccezione delle opzioni di configurazione del workflow e dei controlli per gli utenti che possono utilizzare il modulo. Per ulteriori informazioni su come aggiungere e modificare le proprietà, aggiungere gestori personalizzati e comprendere Workflow Automation, vedere gli argomenti trattati di seguito.

- Personalizzazione delle pagine delle proprietà (Client Web)
- Aggiunta di gestori personalizzati
- Workflow automatizzato

Aggiunta di gestori personalizzati

In DRA i gestori personalizzati vengono utilizzati affinché gli attributi delle proprietà interagiscano fra di loro per completare task di workflow e per le personalizzazioni di caricamento e invio in un workflow, una proprietà o un modulo di creazione.

Gestori personalizzati delle proprietà

Alcuni esempi di gestori personalizzati delle proprietà includono:

- interrogazione del valore di altri campi
- aggiornamento dei valori dei campi
- attivazione/disattivazione dello stato di sola lettura di un campo
- visualizzazione o occultamento di campi in base alle variabili configurate

Gestori di caricamento pagina

In genere, i gestori di caricamento pagina eseguono l'inizializzazione e vengono utilizzati principalmente nelle pagine delle proprietà personalizzate. Vengono eseguiti solo la prima volta che viene selezionata una pagina e, nel caso delle pagine delle proprietà, vengono eseguiti dopo il caricamento dei dati dal server.

Gestori di caricamento modulo

I gestori di caricamento modulo eseguono generalmente controlli di inizializzazione. Vengono eseguiti solo una volta durante il caricamento iniziale del modulo. Nel caso delle pagine delle proprietà, vengono eseguiti prima che il server venga sottoposto a query per le proprietà dell'oggetto selezionato.

Gestori di invio modulo

I gestori di invio modulo permettono di eseguire alcuni tipi di convalida ed eventualmente annullare l'invio del modulo in caso di errori.

Nota: Come best practice, evitare di configurare i gestori di modifica nella pagina e i gestori dei moduli che modificano i valori dei campi presenti in pagine (schede) diverse da quelle in cui viene creato il gestore. In questo scenario, i dati presenti in una pagina diversa da quella del gestore non verranno caricati finché l'amministratore aggiunto non accederà a tale pagina, il che può essere in conflitto con il valore impostato dal gestore di modifica.

Per esempi dettagliati sull'utilizzo di gestori personalizzati e personalizzazioni nella Console Web, fare riferimento alle sezioni “Web Console Customization” (Personalizzazione della Console Web) e “Workflow Customization” (Personalizzazione del workflow) nel riferimento *Product Customization* (Personalizzazione del prodotto) nella pagina della documentazione DRA.

Per ulteriori informazioni sul comportamento dei gestori personalizzati e su come crearli, vedere i seguenti argomenti:

- “Passaggi di base per la creazione di un gestore personalizzato” a pagina 212
- “Abilitazione di JavaScript personalizzato” a pagina 215
- “Utilizzo dell'editor di script” a pagina 215
- “Informazioni sull'esecuzione del gestore personalizzato” a pagina 216

Passaggi di base per la creazione di un gestore personalizzato

Prima di creare un gestore personalizzato, assicurarsi che JavaScript personalizzato sia abilitato nella configurazione della console. Per ulteriori informazioni, vedere Abilitazione di JavaScript personalizzato.

La procedura riportata di seguito inizia da una pagina preselezionata del gestore personalizzato. Per arrivare a tale punto, è necessario passare a diversi gestori nel modo seguente:

- Gestori personalizzati delle proprietà dell'oggetto: fare clic sull'icona di modifica in un campo delle proprietà.

- Gestori di caricamento pagina: selezionare le proprietà della pagina. Ad esempio, **Generale** > **Altre opzioni** > **Proprietà**.
- Gestori di caricamento modulo e di invio modulo: fare clic sul pulsante **Proprietà modulo** in un modulo di workflow selezionato, in una pagina Crea oggetto o in una pagina Modifica proprietà.

Creazione di un gestore personalizzato:

1. Selezionare la scheda del gestore appropriata in base alla proprietà o alla pagina che si sta personalizzando:
   - Gestori personalizzati
   - Gestori di caricamento pagina
   - Gestori caricamento modulo
   - Gestori invio modulo
2. Abilitare la pagina del gestore  ed eseguire una delle seguenti operazioni:
   - **Gestore personalizzato del campo delle proprietà:**
     1. Selezionare un orario di esecuzione. In genere viene utilizzata la seconda opzione.

        L'orario di esecuzione controlla quando i gestori di modifica vengono eseguiti in risposta all'input dell'utente. Tenere presente che questa impostazione non si applica quando il valore del campo viene aggiornato da un altro gestore personalizzato tramite l'interfaccia draApi.fieldValues.
     2. Fare clic su **+ Aggiungi** e scegliere un gestore personalizzato dal menu **Aggiungi gestore personalizzato**.
   - **Gestore della pagina o del modulo:** fare clic su **+ Aggiungi** e scegliere un gestore personalizzato dal menu **Aggiungi gestore personalizzato**.

   Nota: In genere è probabile che sia sufficiente un solo gestore personalizzato ma è possibile usarne più di uno. I gestori multipli vengono eseguiti sequenzialmente nell'ordine elencato. Se si desidera modificare l'ordine dei gestori o ignorare un gestore non necessario, è possibile aggiungere API di controllo del flusso nello script.

   ---
3. Sarà necessario configurare ciascun gestore personalizzato aggiunto alla pagina. Le opzioni di configurazione variano in base al tipo di gestore. L'editor di script include una Guida integrata e l'assistenza per il completamento dinamico del codice Intellisense che fa riferimento anche agli snippet della Guida. Per ulteriori informazioni sull'utilizzo di queste funzionalità, vedere Utilizzo dell'editor di script.

   È possibile creare tipi di gestori personalizzati.

   - **Gestori di query LDAP o REST:**
     1. Se si desidera basare la propria query su valori statici, è necessario definire le **informazioni di connessione** e i **parametri della query**.

        Nota: Per le query LDAP, è possibile richiedere un tipo di autenticazione specifico nelle impostazioni di Informazioni di connessione:

        - **Account di default:** esegue l'autenticazione con un login al server DRA.

- **Account prioritario dominio gestito:** esegue l'autenticazione ad Active Directory tramite l'account prioritario del dominio gestito esistente.
- **Account prioritario LDAP:** esegue l'autenticazione tramite un account prioritario LDAP a differenza di un account di dominio da un dominio gestito. Per utilizzare questa opzione, è innanzitutto necessario abilitare l'account nella Console di delega e configurazione. Per ulteriori informazioni, vedere Abilitare l'autenticazione prioritaria LDAP.

Se si desidera che la query sia dinamica, immettere i valori segnaposto nei campi obbligatori. Questa operazione è necessaria affinché il gestore venga eseguito. Lo script sovrascriverà i valori segnaposto.

Nota: È anche possibile configurare le intestazioni e i cookie per la query REST.

---

2. In Azione pre-query, utilizzare l'editor di script per scrivere codice JavaScript personalizzato che verrà eseguito prima dell'invio della query. Questo script dispone dell'accesso a tutte le informazioni sulla connessione e ai parametri di query ed è in grado di apportare modifiche in modo da personalizzare la query. Ad esempio, impostare i parametri di query in base ai valori immessi dall'utente nel modulo.
3. Nell'Azione post-query, includere script per elaborare i risultati della query. I task comuni includono il controllo di errori, l'aggiornamento dei valori del modulo in base ai risultati restituiti e la convalida dell'univocità dell'oggetto in base al numero di oggetti restituiti dalla query.

- **Script:** Inserire codice JavaScript personalizzato per creare lo script.
- **Query DRA:** Specificare il payload JSON nella scheda Parametri query. Il formato del payload deve corrispondere alla chiave VarSet o alle coppie di valori che verranno inviate al server DRA. Analogamente alle query REST e LDAP, è possibile specificare un'Azione pre-query che può essere utilizzata per modificare il payload prima che venga inviato al server e un'Azione post-query per elaborare i risultati.
- **Gestori delle caselle del messaggio:** Una volta definite le proprietà della finestra del messaggio, è inoltre possibile scrivere i segmenti JavaScript per l'**Azione prima della visualizzazione** e l'**Azione dopo la chiusura**.

  Queste azioni sono facoltative. L'Azione prima della visualizzazione consente di personalizzare qualsiasi proprietà della casella di messaggio prima che venga visualizzata all'utente, l'Azione dopo la chiusura viene utilizzata per elaborare la selezione del pulsante dell'utente ed eseguire eventuale logica aggiuntiva sulla base della selezione.

4 Fare clic su **OK** per salvare il gestore.

Per esempi dettagliati sull'utilizzo di gestori personalizzati e personalizzazioni nella Console Web, fare riferimento alle sezioni “Web Console Customization” (Personalizzazione della Console Web) e “Workflow Customization” (Personalizzazione del workflow) nel riferimento *Product Customization* (Personalizzazione del prodotto) nella pagina della documentazione DRA

Abilitazione di JavaScript personalizzato

Per motivi di sicurezza, JavaScript personalizzato è disabilitato per default. L'abilitazione di JavaScript personalizzato consente agli amministratori di scrivere frammenti di codice JavaScript che verranno eseguiti dalla Console Web senza variazioni. È consigliabile abilitare questa eccezione solo se si comprendono e si accettano i rischi correlati.

Per abilitare le personalizzazioni per includere codice JavaScript personalizzato:

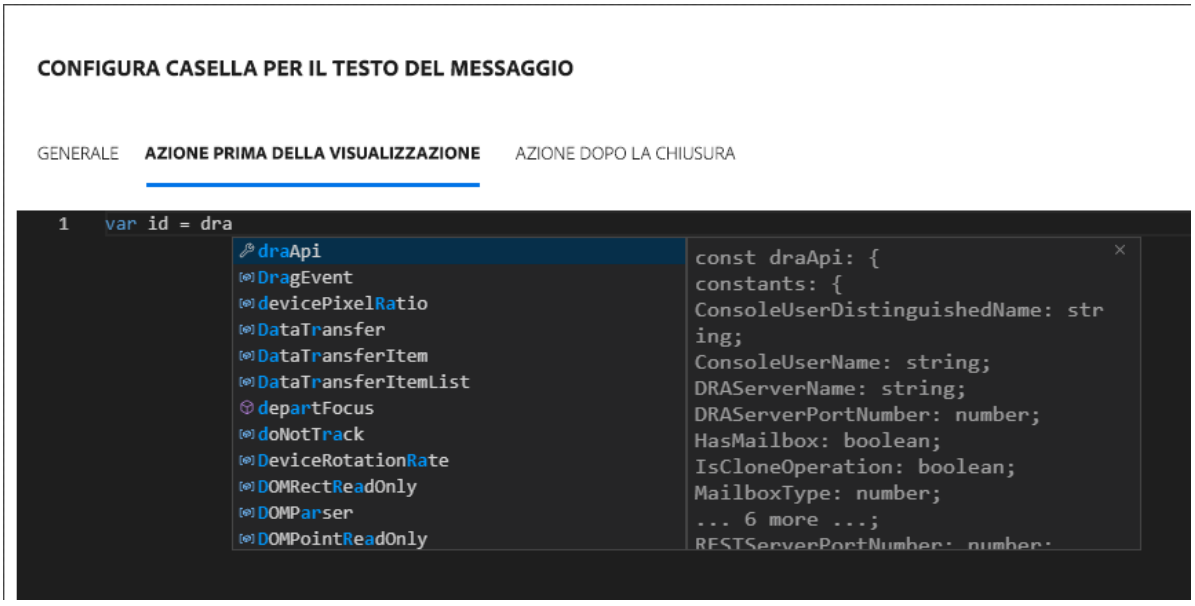
1. Passare all'ubicazione `C:\ProgramData\NetIQ\DRARESTProxy`.
2. Aprire il file `restProxy.config`.
3. Aggiungere `allowCustomJavaScript = "true"` all'elemento `<consoleConfiguration>`.

Utilizzo dell'editor di script

L'editor di script consente di digitare in formato libero e di incollare i metodi JavaScript mediante le API di DRA per la creazione di gestori personalizzati in DRA. L'editor include il completamento dinamico del codice Intellisense e un pannello a comparsa della Guida che assiste l'utente nella scrittura dello script.

Completamento del codice Intellisense

Intellisense nell'editor di script fornisce snippet di completamento del codice selezionabili, completamento tramite tasto Tab e pannelli a comparsa dei riepiloghi API con descrizioni delle API.



Nota: Il completamento del codice Intellisense è dinamico. Ciò significa che può fornire opzioni di sintassi in base al tipo di gestore per il quale si sta definendo lo script ma memorizza anche le stringhe precedentemente immesse dall'utente che vengono incluse nei prompt.

Guida dell'editor di script

Quando si fa clic sull'opzione GUIDA nell'editor di script, viene visualizzato un pannello in cui vengono illustrate le finalità generali delle API dei gestori personalizzati, dove vengono utilizzate e in cui vengono elencate le API con le descrizioni delle rispettive funzioni in base al tipo di API:

- Le API globali includono:
  - Accesso ai moduli
  - Controllo del flusso
  - Costanti
- Le API per le caselle del messaggio includono:
  - Azione prima della visualizzazione
  - Azione dopo la chiusura
- Le API per le query includono:
  - Risultati della query
  - Query DRA
  - Query LDAP
  - Query REST

Informazioni sull'esecuzione del gestore personalizzato

DRA consente di personalizzare il comportamento dei moduli Web in diversi punti del ciclo di vita dell'esecuzione dei moduli mediante i gestori personalizzati. Ciascun tipo di gestore personalizzato dispone di una finestra di esecuzione specifica che, a sua volta, influisce sull'ambito dei dati dell'oggetto disponibili durante l'esecuzione della personalizzazione, come indicato di seguito:

1. *Gestori di caricamento modulo*. Vengono eseguiti quando il modulo viene caricato prima della raccolta degli attributi dell'oggetto a cui è connesso il modulo. Questi gestori non hanno accesso ai valori degli attributi per l'oggetto di destinazione.
2. *Gestori di caricamento pagina*. DRA esegue i gestori di caricamento pagina la prima volta che si accede a una pagina di un modulo. A questi gestori è garantito l'accesso ai valori degli attributi per l'oggetto di destinazione contenuti in tale pagina.
3. *Gestori degli attributi*. DRA esegue i gestori degli attributi quando si accede al valore di un attributo nel modulo. Inoltre, è possibile configurare ciascun attributo del modulo in modo da eseguire i propri gestori personalizzati in uno dei tre punti specifici durante l'interazione dell'utente: (1) immediatamente (quando l'attributo acquisisce lo stato attivo), (2) quando l'attributo perde lo stato attivo o (3) dopo un determinato periodo di tempo dalla perdita dello stato attivo dell'attributo.
4. *Gestori di invio modulo*. I gestori di invio modulo vengono eseguiti quando il modulo viene salvato o le modifiche vengono applicate al modulo.

Personalizzazione del branding dell'interfaccia utente

È possibile personalizzare la barra del titolo della console Web di DRA con il proprio titolo e la propria immagine del logo. La posizione di questi elementi è direttamente a destra del nome del prodotto DRA. Poiché questa posizione viene utilizzata anche per la navigazione di più alto livello, dopo il login gli elementi vengono nascosti dai collegamenti di tale navigazione. Tuttavia, la scheda del browser continuerà a visualizzare il titolo personalizzato.

Per personalizzare il branding della Console Web di DRA:

1. Eseguire il login alla Console Web come amministratore di DRA.
2. Passare ad **Amministrazione** > **Configurazione** > **Branding**.
3. Se si aggiunge un'immagine del logo aziendale, salvare l'immagine del logo sul server Web in `inetpub\wwwroot\DRAClient\assets`.
4. Se applicabile, aggiornare la configurazione per i riquadri Titolo e Login.

   Se si desidera aggiungere un avviso per gli amministratori aggiunti durante il login, attivare il pulsante **Mostra una notifica obbligatoria durante il login**. Aggiornare la configurazione di questa notifica e fare clic su **ANTEPRIMA** per visualizzare l'aspetto della notifica durante il login.
5. Una volta completate le modifiche, fare clic su **Salva**.

IX Strumenti e utility

Queste sezioni contengono informazioni relative alle utility ActiveView Analyzer, Diagnostic, Deleted Object, Health Check e Recycle Bin incluse in DRA.

25 Utility ActiveView Analyzer

Ogni vista ActiveView di DRA contiene una o più regole, che vengono applicate agli oggetti Active Directory (AD) gestiti da un set multimaster DRA. L'utility ActiveView Analyzer viene utilizzata per controllare il tempo di elaborazione di ciascuna regola ActiveView di DRA dal momento in cui viene applicata agli oggetti AD all'interno di un'operazione DRA specifica. Durante un'operazione DRA, il server DRA confronta gli oggetti di destinazione dell'operazione con ciascuna regola in ogni vista ActiveView. DRA crea successivamente un elenco dei risultati contenente tutte le regole corrispondenti. ActiveView Analyzer calcola il tempo impiegato per l'elaborazione di ciascuna regola dal momento in cui viene applicata a un'operazione DRA.

Queste informazioni consentono di diagnosticare i problemi relativi alle viste ActiveView verificando la presenza di anomalie nel tempo di elaborazione della vista ActiveView, compreso il tempo richiesto per elaborare viste ActiveView inutilizzate. L'utility semplifica anche la ricerca di viste ActiveView duplicate.

Dopo aver eseguito una raccolta dati e visualizzato un rapporto, potrebbe essere necessario modificare le regole di una o più viste ActiveView.

È possibile accedere all'utility ActiveView Analyzer da qualsiasi server di amministrazione DRA. Tuttavia, l'utility ActiveView deve essere eseguita nel server di amministrazione in cui si verifica il problema.

Per accedere all'utility ActiveView Analyzer, eseguire il login al server di amministrazione con i privilegi del ruolo di amministrazione DRA e dal menu Start accedere a **NetIQ Administration** (Amministrazione NetIQ) > **ActiveView Analyzer Utility** (Utility ActiveView Analyzer). È inoltre possibile avviare `ActiveViewAnalyzer. exe` dal percorso di installazione di DRA `Program Files (x86)\NetIQ\DRA\X64`.

Utilizzare questa utility per eseguire le seguenti operazioni:

- Raccogliere dati sulle viste ActiveView
- Generare un rapporto dell'analizzatore

Esempio

Paul, un amministratore aggiunto, notifica a Bob, un amministratore DRA, che la creazione di utenti richiede più tempo del solito. Bob decide di avviare l'analizzatore ActiveView sull'oggetto utente di Paul, quindi chiede a Paul di creare un utente. Al termine della raccolta, Bob genera un rapporto di analisi e nota che la regola denominata Share MBX impiega 50ms per l'enumerazione. Bob identifica la vista ActiveView che contiene la regola e dopo averla modificata, osserva che il problema è stato risolto.

Avvio di una raccolta dati ActiveView

Con l'utility ActiveView Analyzer, è possibile raccogliere dati sulle viste ActiveView dalle azioni eseguite su di esse dagli amministratori aggiunti. Questi dati possono quindi essere visualizzati in un rapporto dell'analizzatore. Per raccogliere i dati, è necessario specificare l'amministratore aggiunto oggetto della raccolta e avviare una raccolta ActiveView.

Nota: l'amministratore aggiunto per il quale si desidera eseguire la raccolta dati deve essere connesso allo stesso server DRA in cui viene eseguito l'analizzatore.

Per avviare una raccolta ActiveView:

1. Fare clic su **Start** > **NetIQ Administration** (Amministrazione NetIQ) > **ActiveView Analyzer Utility** (Utility ActiveView Analyzer).
2. Nella pagina ActiveView Analyzer, specificare quanto segue:
   - 2a **Target DRA Server (Server DRA di destinazione):** il server DRA che raccoglie i dati sulle prestazioni delle operazioni dell'amministratore aggiunto.
   - 2b **Target Assistant Administrator (Amministratore aggiunto di destinazione):** fare clic su Sfoglia e selezionare un amministratore aggiunto per il quale si desidera raccogliere i dati.
   - 2c **Monitoring Duration (Durata del monitoraggio):** specificare il numero totale di ore necessarie per raccogliere i dati dell'analizzatore. Una volta trascorso il periodo di tempo specificato, la raccolta dei dati verrà interrotta.
3. Fare clic su **Start Collection** (Avvia raccolta) per raccogliere i dati ActiveView.

   Una volta avviata la raccolta di dati ActiveView, l'utility cancella i dati esistenti e visualizza lo stato più recente.
4. (Facoltativo) È possibile interrompere manualmente la raccolta dati prima della scadenza della durata pianificata e generare comunque un rapporto. Fare clic su **Stop Collection** (Interrompi raccolta) per interrompere la registrazione delle operazioni degli amministratori aggiunti nelle viste ActiveView.
5. (Facoltativo) Per ottenere lo stato più recente, fare clic su **Collection Status** (Stato raccolta).

Importante: se si interrompe la raccolta e si modifica l'amministratore aggiunto o si riavvia una raccolta dati per lo stesso amministratore aggiunto, ActiveView Analyzer cancella i dati esistenti. Nel database è possibile registrare i dati dell'analizzatore di un solo amministratore aggiunto per volta.

Generazione di un rapporto dell'analizzatore

Prima di generare un rapporto dell'analizzatore, accertarsi di avere interrotto la raccolta dei dati.

Nella pagina ActiveView Analyzer viene visualizzato l'elenco delle operazioni eseguite dall'amministratore aggiunto. Per generare un rapporto dell'analizzatore:

1. Fare clic su **Select Report** (Seleziona rapporto), quindi scegliere il rapporto che si desidera visualizzare.

2 Fare clic su **Generate Report** (Genera rapporto) per generare un rapporto di analisi con i dettagli sulle operazioni di ActiveView, ad esempio gli oggetti AD interessati dall'operazione, la gestione da parte di ActiveView degli oggetti elencati, con o senza corrispondenza e la durata per l'elaborazione di ciascuna regola ActiveView.

   Questo rapporto permette di analizzare quali regole necessitano di più tempo per eseguire le operazioni, affinché sia possibile decidere se devono essere modificate o eliminate dalle rispettive viste ActiveView.

3 (Facoltativo) Spostarsi col mouse sulla griglia, fare clic con il pulsante destro del mouse e utilizzare il menu di copia per copiare il rapporto negli Appunti. Negli Appunti, è possibile incollare le intestazioni di colonna e i dati in un'altra applicazione, ad esempio Blocco note o Excel.

Identificazione delle prestazioni degli oggetti

Per identificare le prestazioni di tutti gli oggetti gestiti mediante una vista ActiveView o una regola:

1 Avviare la Console di delega e configurazione.

2 Passare a **Delegation Management** (Gestione delega) e fare clic su **Manage ActiveViews** (Gestisci viste ActiveView).

3 Eseguire una ricerca per individuare una vista ActiveView specifica.

   Qui è possibile trovare la regola o l'oggetto che presenta un problema e apportare modifiche.

   - Fare doppio clic sulla vista ActiveView e selezionare **Rules** (Regole) per elencare le regole. È possibile modificare una regola specifica dal menu di scelta rapida.
   - Fare clic con il pulsante destro del mouse sulla vista ActiveView e selezionare **Show Managed Objects** (Mostra oggetti gestiti) per elencare gli oggetti. Per modificare un oggetto, selezionare **Proprietà** dal menu di scelta rapida.

4 Apportare le modifiche alla regola o all'oggetto gestito e verificare che tali modifiche siano in grado di risolvere il problema.

26 Utility Diagnostic

L'utility Diagnostic raccoglie le informazioni dal server di amministrazione per facilitare la diagnostica di eventuali problemi di DRA. Si utilizza per fornire file di log al rappresentante del Supporto tecnico. L'utility Diagnostic offre un'interfaccia con procedure guidate per impostare i livelli di log e raccogliere le informazioni di diagnostica.

È possibile accedere all'utility Diagnostic da qualsiasi computer del server di amministrazione. Tuttavia, l'utility Diagnostic deve essere eseguita nel server di amministrazione in cui si verifica il problema.

Per accedere all'utility Diagnostic, eseguire il login al computer server di amministrazione utilizzando un account amministratore con diritti di amministratore locale e aprire l'utility dal gruppo di programmi di amministrazione di NetIQ nel menu Start di Windows.

Per ulteriori informazioni sull'uso di questa utility, contattare il Supporto tecnico.

27 Utility Deleted Objects

Questa utility consente di abilitare il supporto per l'aggiornamento incrementale della cache degli account per un dominio specifico quando l'account di accesso al dominio non è un amministratore. Se l'account di accesso al dominio non dispone delle autorizzazioni di lettura per il container Oggetti eliminati del dominio, DRA non può eseguire l'aggiornamento incrementale della cache degli account.

Questa utility consente di eseguire le operazioni seguenti:

- Verificare che l'account utente o il gruppo specificato disponga delle autorizzazioni di lettura per il container Oggetti eliminati nel dominio specificato
- Delegare o rimuovere le autorizzazioni di lettura per un account utente o gruppo specificato
- Delegare a un account utente o rimuovere il diritto utente per i dati del servizio di sincronizzazione directory
- Visualizzare le impostazioni di sicurezza per il container Oggetti eliminati

È possibile eseguire il file dell'utility Deleted Objects (`DraDelObjsUtil.exe`) dalla cartella `Program Files (x86)\NetIQ\DRA` nel server di amministrazione.

Autorizzazioni necessarie per l'utility Deleted Objects

Per utilizzare questa utility, è necessario disporre delle autorizzazioni seguenti:

Operazione	Autorizzazione necessaria
Verificare le autorizzazioni dell'account	Autorizzazioni di lettura per il container Oggetti eliminati
Delegare autorizzazioni di lettura per il container Oggetti eliminati	Autorizzazioni di amministratore nel dominio in cui si trova il container Oggetti eliminati
Delegare il diritto utente per dati del servizio di sincronizzazione directory	Autorizzazioni di amministratore nel dominio in cui si trova il container Oggetti eliminati
Rimuovere le autorizzazioni precedentemente delegate	Autorizzazioni di amministratore nel dominio in cui si trova il container Oggetti eliminati
Visualizzare le impostazioni di sicurezza per il container Oggetti eliminati	Autorizzazioni di lettura per il container Oggetti eliminati

Sintassi per l'utility Deleted Objects

```
DRADELOBJSUTIL /DOMAIN:NOMEDOMINIO [/DC:NOMECOMPUTER] {/
DELEGATE:NOMEACCOUNT | /VERIFY:NOMEACCOUNT | /REMOVE:NOMEACCOUNT | /
DISPLAY [/RIGHT]}
```

Opzioni dell'utility Deleted Objects

È possibile specificare le opzioni seguenti:

/DOMAIN:*dominio*	Consente di specificare il nome NETBIOS o DNS del dominio in cui si trova il container Oggetti eliminati.
/SERVER:*nomecomputer*	Consente di specificare il nome o l'indirizzo IP del controller del dominio specificato.
/DELEGATE:*nomeaccount*	Consente di delegare autorizzazioni all'account utente o al gruppo specificato.
/REMOVE:*nomeaccount*	Consente di rimuovere le autorizzazioni precedentemente delegate all'account utente o al gruppo specificato
/VERIFY:*nomeaccount*	Consente di verificare le autorizzazioni dell'account utente o del gruppo specificato.
/DISPLAY	Consente di visualizzare le impostazioni di sicurezza del container Oggetti eliminati nel dominio specificato.
/RIGHT	Garantisce che l'account utente o il gruppo specificato disponga del diritto utente per i dati del servizio di sincronizzazione directory. È possibile utilizzare l'opzione per delegare o verificare questo diritto. Il diritto utente per i dati del servizio di sincronizzazione directory consente all'account di leggere tutti gli oggetti e le proprietà di Active Directory.

Nota

- Se il nome dell'account utente o del gruppo che si desidera specificare contiene uno spazio, racchiudere il nome dell'account tra virgolette. Ad esempio, se si desidera specificare il gruppo Houston IT, digitare "Houston IT".
- Quando si specifica un gruppo, utilizzare il nome precedente a Windows 2000 per il gruppo.

Esempi relativi all'utility Deleted Objects

Gli esempi seguenti illustrano alcuni comandi esemplificativi per gli scenari più comuni.

Esempio 1

Per verificare che l'account utente `MYCOMPANY\JSmith` disponga delle autorizzazioni di lettura per il container Oggetti eliminati nel dominio `hou.mycompany.com`, immettere:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Esempio 2

Per delegare le autorizzazioni di lettura per il container Oggetti eliminati nel dominio MYCOMPANY al gruppo MYCOMPANY\DraAdmins, immettere:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Esempio 3

Per delegare autorizzazioni di lettura per il container Oggetti eliminati e il diritto utente per i dati del servizio di sincronizzazione directory nel dominio MYCOMPANY all'account utente MYCOMPANY\JSmith, immettere:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Esempio 4

Per visualizzare le impostazioni di sicurezza per il container Oggetti eliminati nel dominio hou.mycompany.com utilizzando il controller di dominio HQDC, immettere:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Esempio 5

Per rimuovere le autorizzazioni di lettura per il container Oggetti eliminati nel dominio MYCOMPANY dal gruppo MYCOMPANY\DraAdmins, immettere:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 Utility Health Check

L'utility Health Check di DRA è un'applicazione autonoma inclusa nel kit di installazione di DRA. Si utilizza dopo l'installazione, nonché prima e dopo l'upgrade per verificare, convalidare e ottenere informazioni sullo stato dei componenti e dei processi per il server DRA, il sito Web di DRA e i client DRA. È inoltre possibile utilizzarla per installare o aggiornare una licenza del prodotto, per eseguire il backup dell'istanza AD LDS prima di eseguire un upgrade del prodotto, per visualizzare le descrizioni dei controlli e per correggere i problemi o identificare le azioni da intraprendere per correggere i problemi e quindi eseguire una nuova convalida.

L'utility Health Check è disponibile nella cartella del programma DRA dopo l'esecuzione del programma di installazione `NetIQAdminInstallationKit.msi`.

È possibile eseguire l'utility Health Check in qualsiasi momento eseguendo il file `NetIQ.DRA.HealthCheckUI.exe`. All'apertura dell'applicazione, è possibile scegliere di eseguire un'operazione specifica, effettuare controlli su componenti specifici o effettuare controlli su tutti i componenti. Di seguito sono illustrate alcune funzioni dell'utility Health Check:

Funzione	Azioni utente
Selezionare tutto o deselezionare tutto	Utilizzare la barra degli strumenti o le opzioni del menu File per **selezionare** o **deselezionare** tutti gli elementi da controllare, oppure selezionare le singole caselle di controllo per eseguire controlli specifici.
Eseguire controlli selezionati	Utilizzare la barra degli strumenti oppure l'opzione del menu File per eseguire i controlli selezionati (tutti o specifici).
Salvare o scrivere i risultati	Utilizzare la barra degli strumenti o l'opzione del menu File per creare e salvare un rapporto dettagliato dei controlli eseguiti.
Eseguire un controllo	Selezionare il titolo di un elemento per visualizzare la descrizione del controllo, quindi fare clic sull'icona della barra degli strumenti per eseguire il controllo. Ad esempio, per eseguire una delle operazion seguentii: ◆ Convalida della licenza (installazione o aggiornamento di una licenza del prodotto) ◆ Backup dell'istanza AD LDS (esecuzione del backup dell'istanza AD LDS) ◆ Replica (convalida del database di replica)
Correggere il problema	Selezionare il titolo di un elemento e utilizzare l'opzione della barra degli strumenti quando un controllo ha esito negativo. Se eseguendo nuovamente il controllo il problema non viene corretto, la descrizione dovrebbe includere informazioni o azioni che è possibile utilizzare per risolvere il problema.

29 Utility Recycle Bin

Questa utility consente di abilitare il supporto per il Cestino quando si gestisce un sottoalbero di un dominio. Se l'account di accesso al dominio non dispone delle autorizzazioni sul container nascosto NetIQRecycleBin nel dominio specificato, DRA non è in grado di spostare gli account eliminati nel Cestino.

Nota: dopo aver utilizzato questa utility per abilitare il Cestino, eseguire un aggiornamento completo della cache degli account affinché il server di amministrazione applichi la modifica.

Questa utility consente di eseguire le operazioni seguenti:

- Verificare che l'account specificato disponga delle autorizzazioni di lettura per il container NetIQRecycleBin nel dominio specificato
- Delegare autorizzazioni di lettura a un account specificato
- Visualizzare le impostazioni di sicurezza per il container NetIQRecycleBin

Autorizzazioni necessarie per l'utility Recycle Bin

Per utilizzare questa utility, è necessario disporre delle autorizzazioni seguenti:

Operazione	Autorizzazione necessaria
Verificare le autorizzazioni dell'account	Accesso con autorizzazioni di lettura per il container NetIQRecycleBin
Delegare autorizzazioni di lettura per il container NetIQRecycleBin	Autorizzazioni di amministratore nel dominio specificato
Visualizzare le impostazioni di sicurezza per il container NetIQRecycleBin	Accesso con autorizzazioni di lettura per il container NetIQRecycleBin

Sintassi dell'utility Recycle Bin

```
DRARECYCLEBINUTIL /DOMAIN:NOMEDOMINIO [/DC:NOMECOMPUTER] {/
DELEGATE:NOMEACCOUNT | /VERIFY:NOMEACCOUNT | /DISPLAY}
```

Opzioni dell'utility Recycle Bin

Mediante le opzioni seguenti è possibile configurare l'utility Recycle Bin:

/DOMAIN:dominio Consente di specificare il nome NETBIOS o DNS del dominio in cui si trova il Cestino.

/SERVER:*nomecomputer*	Consente di specificare il nome o l'indirizzo IP del controller del dominio specificato.
/DELEGATE:*nomeaccount*	Consente di delegare autorizzazioni all'account specificato.
/VERIFY:*nomeaccount*	Consente di verificare le autorizzazioni dell'account specificato.
/DISPLAY	Consente di visualizzare le impostazioni di sicurezza del container NetIQRecycleBin nel dominio specificato.

Esempi relativi all'utility Recycle Bin

Gli esempi seguenti illustrano alcuni comandi esemplificativi per gli scenari più comuni.

Esempio 1

Per verificare che l'account utente `MYCOMPANY\JSmith` disponga delle autorizzazioni di lettura per il container NetIQRecycleBin nel dominio `hou.mycompany.com`, immettere:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Esempio 2

Per delegare le autorizzazioni di lettura per il container NetIQRecycleBin nel dominio `MYCOMPANY` al gruppo `MYCOMPANY\DraAdmins`, immettere:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Esempio 3

Per visualizzare le impostazioni di sicurezza per il container NetIQRecycleBin nel dominio `hou.mycompany.com` utilizzando il controller di dominio `HQDC`, immettere:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

A Appendice

In questa appendice vengono fornite informazioni sui servizi DRA e su come risolvere i problemi relativi al servizio REST di DRA.

Servizi DRA

In questa tabella vengono fornite informazioni sui servizi DRA. Ciò consente agli amministratori DRA di decidere se possono disabilitare un servizio in modo sicuro senza influire sulle funzionalità DRA.

Servizio DRA	Descrizione	Sicuro da disabilitare
NetIQ Administration Service (Servizio di amministrazione NetIQ)	Questo servizio esegue tutte le operazioni DRA e gestisce i processi interni del server DRA.	No
Servizio Revisione di NetIQ DRA	Questo servizio gestisce le richieste di Cronologia modifiche unificata dalla console Web. Quando si disabilita questo servizio: ◆ La funzionalità di DRA non viene influenzata. ◆ Sarà possibile generare rapporti di Cronologia modifiche unificata dalla Console di delega e configurazione. ◆ Non sarà possibile generare rapporti di Cronologia modifiche unificata dalla console Web.	Sì
Servizio Cache di NetIQ DRA	Questo servizio funge da cache permanente per il server di amministrazione NetIQ.	No
Servizio Core di NetIQ DRA	Questo servizio genera rapporti per le console DRA e pianifica i lavori di Active Directory, Office365, DRA e del servizio di raccolta risorse. Quando si disabilita questo servizio: ◆ La funzionalità di DRA non viene influenzata. ◆ I lavori del servizio di raccolta non verranno eseguiti, quindi i dati per i rapporti NRC non verranno raccolti. ◆ Non sarà possibile generare rapporti di Cronologia modifiche unificata da alcuna console DRA.	Sì

Servizio DRA	Descrizione	Sicuro da disabilitare
Archivio log di NetIQ DRA	Questo servizio memorizza tutti gli eventi di revisione di DRA in modo sicuro per fornire supporto alla generazione di rapporti di revisione.	No
Servizio Replica di NetIQ DRA	Questo servizio supporta la funzione Assegnazione temporanea al gruppo (TGA, Temporary Group Assignment) di DRA. Le assegnazioni temporanee al gruppo non saranno disponibili nei server DRA in cui il servizio è stato rimosso o arrestato.	Sì
Servizio Rest di NetIQ DRA	La console Web e i client PowerShell utilizzano questo servizio per comunicare con il server di amministrazione NetIQ.	No
Memorizzazione sicura di NetIQ DRA	Questo servizio gestisce l'istanza AD LDS di DRA in cui è memorizzata la configurazione di DRA. Inoltre, replica questi dati di configurazione nella configurazione di MMS.	No
Servizio Skype di NetIQ DRA	Questo servizio gestisce tutti i task di Skype. Quando si disabilita questo servizio: ◆ La funzionalità di DRA non viene influenzata. ◆ Le operazioni Skype non verranno elaborate.	Sì

Risoluzione dei problemi relativi ai servizi REST di DRA

Questa sezione contiene informazioni per la risoluzione dei problemi relativi ai seguenti argomenti:

- “Gestione dei certificati per le estensioni REST di DRA” a pagina 236
- “Gestione degli errori dal server DRA” a pagina 237
- “Ogni comando PowerShell restituisce un errore PSInvalidOperation” a pagina 238
- “Registrazione della traccia WCF” a pagina 238

Gestione dei certificati per le estensioni REST di DRA

Il servizio endpoint DRA richiede un'associazione di certificato sulla porta di comunicazione. Durante l'installazione, il programma di installazione eseguirà i comandi per associare la porta al certificato. In questa sezione viene descritto come convalidare l'associazione e come aggiungere o rimuovere un'associazione, in base alle necessità.

Informazioni di base

Porta di default del servizio endpoint: 8755

ID app per le estensioni REST di DRA: 8031ba52-3c9d-4193-800a-d620b3e98508

Hash certificato: visualizzato nella pagina SSL Certificates (Certificati SSL) di Gestione IIS

Controllo delle associazioni esistenti

In una finestra CMD, eseguire il seguente comando: `netsh http show sslcert`

Verrà visualizzato un elenco di associazioni di certificato per il computer in uso. Cercare l'ID app delle estensioni REST di DRA nell'elenco. Il numero di porta deve corrispondere alla porta di configurazione. L'hash del certificato deve corrispondere all'hash del certificato visualizzato in Gestione IIS.

```
IP:port                 : 0.0.0.0:8755
Certificate Hash        : d095304df3d3c8eecf64c25df7931414c9d8802c
Application ID          : {8031ba52-3c9d-4193-800a-d620b3e98508}
Certificate Store Name  : (null)
Verify Client Certificate Revocation    : Enabled
Verify Revocation Using Cached Client Certificate Only    : Disabled
Usage Check             : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout   : 0
Ctl Identifier          : (null)
Ctl Store Name          : (null)
DS Mapper Usage         : Disabled
Negotiate Client Certificate    : Disabled
```

Rimozione di un'associazione

Per rimuovere un'associazione esistente, immettere il seguente comando in una finestra CMD:

```
netsh http delete sslcert ipport=0.0.0.0:9999
```

Dove 9999 è il numero di porta da rimuovere. Il comando `netsh` visualizza un messaggio che indica che il certificato SSL è stato rimosso correttamente.

Aggiunta di un'associazione

Per aggiungere una nuova associazione, immettere il seguente comando in una finestra CMD:

```
netsh http add sslcert ipport=0.0.0.0:9999 certhash=[HashValue]
appid={8031ba52-3c9d-4193-800a-d620b3e98508}
```

Dove 9999 corrisponde al numero di porta del servizio endpoint e `[HashValue]` corrisponde al valore hash del certificato visualizzato in Gestione IIS.

Gestione degli errori dal server DRA

Se si verifica un errore durante la creazione di un oggetto abilitato per la posta, vedere quanto segue:

EnableEmail restituisce un messaggio di errore dell'operazione

Quando si crea un oggetto abilitato per la posta o si chiama uno degli endpoint EnableEmail, è possibile che venga restituito un errore dal server DRA, ad esempio "*Server failed to complete the requested operation workflow successfully. Operation UserEnableEmail failed*" (Il server non è

riuscito a completare correttamente il workflow dell'operazione richiesta. Operazione UserEnableEmail non riuscita). Ciò può essere causato dall'inclusione di una proprietà `mailNickname` nel payload che non è conforme alla policy definita sul server.

Rimuovere la proprietà `mailNickname` dal payload e fare in modo che il server DRA generi il valore dell'alias e-mail in base alla policy definita.

Ogni comando PowerShell restituisce un errore PSInvalidOperation

Quando il servizio REST di DRA è associato a un certificato autofirmato, i cmdlet PowerShell restituiscono il seguente errore:

```
Get-DRAServerInfo: One or more errors occurred.
An error occurred while sending the request.
The underlying connection was closed: Could not establish trust
relationship for the SSL/TLS secure channel.
The remote certificate is invalid according to the validation procedure.
```

Per ciascun comando, è necessario includere il parametro `-IgnoreCertificateErrors`. Per sopprimere anche il messaggio di conferma, aggiungere il parametro `-Force`.

Registrazione della traccia WCF

Se le richieste REST generano errori che non possono essere risolti tramite l'analisi dei log del servizio REST, potrebbe essere necessario aumentare il livello di registrazione della traccia WCF in modo da visualizzare i dettagli sulla modalità di trasferimento della richiesta nel livello WCF. Il volume di dati generati da questo livello di traccia può essere significativo, pertanto il livello di registrazione fornito è impostato su "Critical, Error" (Critico, Errore).

Ad esempio, questa impostazione può essere utile se le richieste generano eccezioni di valore nullo anche se si inviano gli oggetti nel payload. Un altro caso è quello in cui REST non risponde.

Per aumentare il livello di registrazione della traccia WCF, è necessario modificare il file di configurazione per il servizio in fase di esame. È probabile che le eccezioni del payload possano essere evinte dall'esame del log di traccia WCF per il servizio REST.

Procedura per l'abilitazione della registrazione dettagliata

1. In Esplora file di Windows, passare alla cartella di installazione delle estensioni di DRA. In genere, il percorso è `C:\Program Files (x86)\NetIQ\DRA`.
2. Aprire il file `NetIQ.DRA.RestService.exe.config`.
3. Individuare l'elemento `<source>` nel seguente percorso XML: `<system.diagnostics><sources>`.
4. Nell'elemento di origine, modificare il valore dell'attributo `switchValue` da `"Critical, Error"` (Critico, Errore) a `"Verbose, ActivityTracing"` (Dettagliato, Traccia attività).
5. Salvare il file e riavviare il servizio Rest di NetIQ DRA.

EnableEmail restituisce un messaggio di errore dell'operazione

I dati di traccia WCF sono scritti in formato proprietario. È possibile leggere il file traces.svslog mediante l'utility SvcTraceViewer.exe. Ulteriori informazioni su questa utility sono disponibili qui: