NetIQ Directory and Resource Administrator

Guida all'installazione

Giugno 2021

Note legali

Sommario

Informazioni su questa guida

La *Guida all'installazione* fornisce informazioni su pianificazione, installazione, gestione delle licenze e configurazione di NetIQ Directory and Resource Administrator (DRA) e i relativi componenti integrati.

Contiene inoltre indicazioni sulla procedura di installazione e informazioni per decidere come installare e configurare DRA correttamente.

Destinatari

Questa guida fornisce informazioni per chi desidera installare DRA.

Documentazione aggiuntiva

Questa guida fa parte del set di documentazione di NetIQ 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 (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Informazioni di contatto

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

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

Introduzione

Prima di installare e configurare tutti i componenti di NetIQ 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

NetIQ Directory and Resource Administrator (DRA) 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, nonché di Exchange Online e Skype for Business Online.
- **Controlli differenziati dei privilegi di accesso di utenti e amministratori:** la tecnologia ActiveView brevettata delega solo i privilegi necessari a svolgere le funzioni corrispondenti a responsabilità specifiche e offre protezione contro l'escalation dei privilegi.
- **Console Web personalizzabile:** l'approccio intuitivo consente a personale non tecnico di eseguire task amministrativi in modo facile e sicuro mediante funzionalità e accesso limitati (e assegnati).
- **Revisioni e rapporti dettagliati delle attività:** offre un record di revisione completo di tutte le attività eseguite con il prodotto. Memorizza i dati a lungo termine e in modo sicuro, consentendo di dimostrare ai revisori (ad esempio PCI DSS, FISMA, HIPAA e NERC CIP) l'adozione di processi per il controllo degli accessi ad AD.
- **Automazione dei processi IT:** permette di automatizzare i workflow di svariati task, quali provisioning e deprovisioning, azioni di utenti e caselle postali, applicazione delle policy e task di self-service controllati, aumentando l'efficienza aziendale e riducendo le operazioni manuali e ripetitive.
- **Integrità operativa:** impedisce modifiche errate o dannose che incidono sulle prestazioni e la disponibilità di sistemi e servizi, fornendo un controllo differenziato degli accessi agli amministratori e gestendo l'accesso a sistemi e risorse.

- **Applicazione dei processi:** preserva l'integrità dei processi chiave di gestione delle modifiche per migliorare la produttività, ridurre gli errori, risparmiare tempo e aumentare l'efficienza amministrativa.
- **Integrazione con Change Guardian:** consente la revisione degli eventi generati in Active Directory al di fuori di DRA e di Workflow Automation.

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:

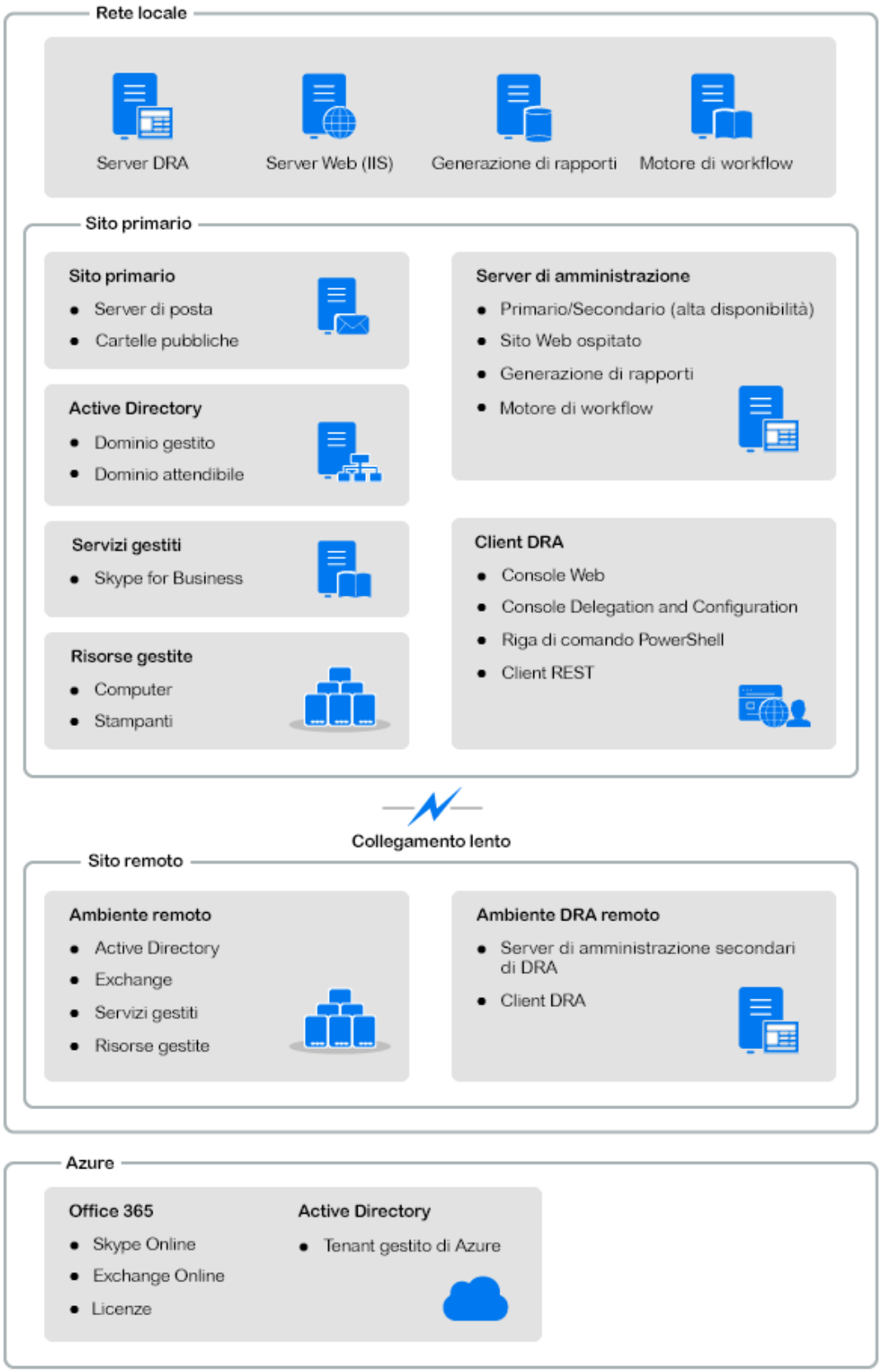
- Rapporti risorse per gli oggetti Active Directory
- Rapporti sui dati oggetto di Active Directory
- Rapporti di riepilogo di Active Directory
- Rapporti di configurazione di DRA
- Rapporti di configurazione di Exchange
- Rapporti di Exchange Online di Office 365
- Rapporti dettagliati sulle tendenze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

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 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 di 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 versione 1.0.1 o 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 Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype for Business	◆ Microsoft Skype for Business 2015
Cronologia modifiche	◆ Change Guardian 5.1 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

Requisiti del server di amministrazione DRA e della console Web

I componenti DRA richiedono i seguenti software e account:

- “Requisiti software” a pagina 23
- “Dominio server” a pagina 24
- “Requisiti degli account” a pagina 24
- “Account di accesso DRA con minimo privilegio” a pagina 26

Requisiti software

Componente	Prerequisiti
Destinazione di installazione	**Sistema operativo del server di amministrazione NetIQ:**
Sistema operativo	◆ Microsoft Windows Server 2012 R2, 2016, 2019 **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
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 ◆ URL Rewrite Module for IIS ◆ Estensione Application Request Routing di Microsoft Internet Information Services **Nota:** L'endpoint e il servizio REST di DRA vengono installati con il server di amministrazione. **Amministrazione di Microsoft Office 365/Exchange Online:** ◆ Modulo di Windows Azure Active Directory per Windows PowerShell ◆ Modulo Windows PowerShell ◆ Modulo PowerShell per Exchange Online V2 ◆ 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 8.0, 8.5, 10 ◆ URL Rewrite Module for IIS ◆ Estensione Application Request Routing di Microsoft Internet Information Services

Dominio server

Componente	Sistemi operativi
Server DRA	◆ 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

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 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)

Nota

- Per 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

Account di accesso tenant di Azure: assegnare le seguenti autorizzazioni di Azure Active Directory all'account di accesso tenant di Azure:

- 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

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

Componente	Prerequisiti
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 8.0, 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 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.
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.
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.

Importante

- Se nella versione DRA precedente è stata installata la console Account and Resource Management (ARM), la console ARM verrà rimossa durante l'upgrade.
- Quando si esegue l'upgrade del server DRA da una versione DRA 9.x, tutti i tenant gestiti vengono rimossi da DRA. Per continuare a utilizzare i tenant con Azure, è necessario aggiungerli dopo l'upgrade. Per informazioni sull'aggiunta dei tenant, vedere "Creazione di un'applicazione Azure e aggiunta di un tenant di Azure" nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).
- Poiché Exchange 2010 non è supportato in DRA 10.1, Exchange viene disabilitato durante l'upgrade da DRA 9.x. Per continuare a eseguire le operazioni di Exchange dopo l'upgrade, disabilitare e riabilitare l'opzione **Enable Exchange Policy** (Abilita policy Exchange) nella Console di delega e configurazione. Per reimpostare la policy, è necessario "applicare" entrambe le modifiche.

  Per informazioni sulla configurazione delle policy, vedere “Abilitazione di Microsoft Exchange” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

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.

Passaggi	Dettagli
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 42
- “Sincronizzazione del set di server di una versione precedente di DRA” a pagina 43
- “Backup del registro del server di amministrazione” a pagina 43

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: L'installazione dell'upgrade del server DRA apporta le seguenti modifiche durante l'upgrade del server DRA da una versione DRA 9.x a una versione DRA 10.x:

- Sposta le configurazioni dell'utente del server di Workflow Automation e UCH dalla Console Web alla Console di delega e configurazione.
- Rimuove il componente Web precedente dal server.
- Rimuove tutti i tenant gestiti.

  Per informazioni sull'aggiunta di tenant, vedere "Configurazione dei tenant di Azure" nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).
- Se nella versione precedente è stata installata la console di gestione di account e risorse, durante l'upgrade a una versione DRA 10.x, la console di gestione di account e risorse viene rimossa.
- Durante l'upgrade di MMS, viene eseguito prima l'upgrade del server primario, seguito dai server secondari. Per la corretta replica delle assegnazioni temporanee al gruppo nel server secondario, eseguire manualmente la **Pianificazione della sincronizzazione multimaster** o attendere l'esecuzione pianificata.

- Poiché Exchange 2010 non è supportato in DRA 10, Exchange viene disabilitato durante l'upgrade da DRA 9.x. Per continuare a eseguire le operazioni di Exchange dopo l'upgrade, disabilitare e riabilitare l'opzione **Enable Exchange Policy** (Abilita policy Exchange) nella Console di delega e configurazione. Per reimpostare la policy, è necessario "applicare" entrambe le modifiche.

  Per informazioni sulla configurazione delle policy, vedere “Abilitazione di Microsoft Exchange” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

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).

Passaggi	Dettagli
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 Configurazione del prodotto

In questo capitolo si descrivono i passaggi e le procedure di configurazione da eseguire se si installa Directory and Resource Administrator per la prima volta.

6 Elenco di controllo della configurazione

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

Passaggi	Dettagli
Applicazione 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.
Apertura della Console di delega e configurazione	Utilizzando l'account del servizio DRA, accedere a un computer in cui è installata la Console di delega e configurazione. Aprire la console.
Aggiunta del primo dominio gestito a DRA	Aggiungere il primo dominio gestito a DRA. **Nota:** è possibile iniziare a delegare i poteri al termine dell'aggiornamento iniziale completo dell'account.
Aggiunta di domini e sottoalberi gestiti	*Facoltativo:* aggiungere altri domini e sottoalberi gestiti a DRA. Per ulteriori informazioni sui domini gestiti, vedere Aggiunta di domini gestiti.
Configurazione delle impostazioni di DCOM	*Facoltativo:* configurare le impostazioni di DCOM. Per ulteriori informazioni sulle impostazioni di DCOM, vedere Configurazione delle impostazioni di DCOM.
Configurazione dei controller di dominio e dei server di amministrazione	Configurare il computer client in cui viene eseguita la Console di delega e configurazione per ciascun controller di dominio e ciascun server di amministrazione. Per ulteriori informazioni, vedere Configurazione di controller di dominio e server di amministrazione.
Configurazione dei servizi DRA per una gMSA	*Facoltativo:* configurare i servizi DRA per un Group Managed Service Account (gMSA). Per ulteriori informazioni, vedere Configurazione dei servizi DRA per un account del servizio gestito del gruppo.

7 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.

8 Aggiunta di domini gestiti

Dopo aver installato il server di amministrazione, è possibile aggiungere domini gestiti, server o workstation. Quando si aggiunge il primo dominio gestito, è necessario eseguire l'accesso utilizzando l'account del servizio DRA in un computer in cui è installata la Console di delega e configurazione. È inoltre necessario disporre dei diritti amministrativi all'interno del dominio, ad esempio i diritti concessi al gruppo Domain Administrators. Per aggiungere domini gestiti e computer dopo aver installato il primo dominio gestito, è necessario disporre dei poteri appropriati, ad esempio quelli inclusi nel ruolo integrato Configure Servers and Domains (Configura server e domini).

Nota: dopo aver completato l'aggiunta di domini gestiti, verificare che le pianificazioni degli aggiornamenti della cache degli account per tali domini siano corrette. Per ulteriori informazioni sulla modifica della pianificazione degli aggiornamenti della cache degli account, vedere “Configurazione della memorizzazione nella cache” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

---

9 Aggiunta di sottoalberi gestiti

Dopo aver installato il server di amministrazione, è possibile aggiungere sottoalberi gestiti o mancanti da domini Microsoft Windows specifici. Queste funzioni vengono eseguite nella Console di delega e configurazione dal nodo **Configuration Management** (Gestione configurazione) > **Managed Domains** (Domini gestiti). Per aggiungere sottoalberi gestiti dopo aver installato 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). Per verificare che l'account di accesso 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.

Per ulteriori informazioni sull'uso di questa utility, vedere “Utility Deleted Objects” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Per ulteriori informazioni sull'impostazione dell'account di accesso, vedere “Definizione di account di accesso ai domini” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

Nota: Dopo aver aggiunto i sottoalberi gestiti, verificare che le pianificazioni degli aggiornamenti della cache degli account per i domini corrispondenti siano corrette. Per ulteriori informazioni sulla modifica della pianificazione degli aggiornamenti della cache degli account, vedere “Configurazione della memorizzazione nella cache” nella *DRA Administrator Guide* (Guida all'amministrazione di DRA).

---

10 Configurazione delle impostazioni di DCOM

Se non si è consentito al programma di installazione di eseguire la configurazione di DCOM, configurare le impostazioni di DCOM nel server di amministrazione primario.

Se si è scelto di non configurare Distributed COM durante la procedura di installazione di DRA, è necessario aggiornare l'appartenenza al gruppo Distributed COM Users per includere tutti gli account utente che utilizzano DRA. Tale appartenenza deve includere l'account di servizio DRA, tutti gli amministratori aggiunti e l'account usato per gestire i servizi DRA REST, DRA Host e DRA Admin.

Per configurare il gruppo Distributed COM Users:

1. Eseguire l'accesso a un computer di amministrazione DRA come amministratore di DRA.
2. Avviare la Console di delega e configurazione. Se la console non esegue automaticamente la connessione al server di amministrazione, stabilire la connessione manualmente.

   Nota: potrebbe non essere possibile eseguire la connessione al server di amministrazione se il gruppo Distributed COM Users non contiene alcun account Amministratore aggiunto. In questo caso, configurare il gruppo Distributed COM Users tramite lo snap-in Utenti e computer di Active Directory. Per ulteriori informazioni sull'utilizzo dello snap-in Utenti e computer di Active Directory, visitare il sito Web di Microsoft.

   ---
3. Nel riquadro a sinistra, espandere **Account and Resource Management** (Gestione account e risorse).
4. Espandere **Tutti i miei oggetti gestiti**.
5. Espandere il nodo di ciascun dominio in cui si dispone di un controller di dominio.
6. Fare clic sul container **Integrato**.
7. Cercare il gruppo Distributed COM Users.
8. Nell'elenco dei risultati della ricerca, fare clic sul gruppo **Distributed COM Users**.
9. Fare clic su **Membri** nel riquadro inferiore e successivamente su **Aggiungi membri**.
10. Aggiungere utenti e gruppi che utilizzeranno DRA. Assicurarsi di aggiungere a questo gruppo l'account del servizio DRA.
11. Fare clic su **OK**.

11 Configurazione di controller di dominio e server di amministrazione

Dopo aver configurato il computer client in cui viene eseguita la Console di delega e configurazione, è necessario configurare ciascun controller di dominio e ciascun server di amministrazione.

Per configurare controller di dominio e server di amministrazione:

1. Nel menu Start, passare a **Pannello di controllo** > **Sistema e sicurezza**.
2. Aprire Strumenti di amministrazione e successivamente Servizi componenti.
3. Espandere **Servizi componenti** > **Computer** > **Computer locale** > **Config DCOM**.
4. Selezionare **MCS OnePoint Administration Service** in Administration Server (Server di amministrazione).
5. Nel menu Azioni, fare clic su **Proprietà**.
6. Nella scheda General (Generale), selezionare **Packet** (Pacchetto) nell'area Authentication Level (Livello di autenticazione).
7. Nella scheda sicurezza, selezionare **Personalizza** nell'area Autorizzazioni di accesso, quindi fare clic su **Modifica**.
8. Verificare che il gruppo Distributed COM Users sia disponibile. Se non è disponibile, aggiungerlo. Se il gruppo Tutti è disponibile, rimuoverlo.
9. Verificare che il gruppo Distributed COM Users disponga delle autorizzazioni di accesso locale e remoto.
10. Nella scheda Sicurezza, selezionare **Personalizza** nell'area Autorizzazioni di esecuzione e attivazione, quindi fare clic su **Modifica**.
11. Verificare che il gruppo Distributed COM Users sia disponibile. Se non è disponibile, aggiungerlo. Se il gruppo Tutti è disponibile, rimuoverlo.
12. Verificare che il gruppo Distributed COM Users disponga delle autorizzazioni seguenti:
    - Avvio locale
    - Avvio remoto
    - Attivazione locale
    - Attivazione remota
13. Applicare le modifiche.

12 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 DB cache 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.

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