
Directory and Resource Administrator

Guida all'installazione

Luglio 2018

Note legali

© Copyright 2007-2018 Micro Focus o una delle sue affiliate.

Le sole garanzie valide per prodotti e servizi di Micro Focus, le sue affiliate e i licenziatari ("Micro Focus") sono specificate nelle dichiarazioni esplicite di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto riportato nel presente documento deve essere interpretato come garanzia aggiuntiva. Micro Focus non sarà da ritenersi responsabile per errori tecnici o editoriali contenuti nel presente documento né per eventuali omissioni. Le informazioni di questo documento sono soggette a modifiche senza preavviso.

Informazioni su questa guida	5
-------------------------------------	----------

1 Introduzione	7
-----------------------	----------

Che cos'è Directory and Resource Administrator	7
Caratteristiche dei componenti di Directory and Resource Administrator	8
Server di amministrazione DRA	8
Console di delega e configurazione	9
Console di gestione account e risorse	9
Console Web	9
Componenti per la generazione di rapporti	9
Motore di workflow	10
Architettura del prodotto	11

2 Installazione e upgrade del prodotto	13
---	-----------

Pianificazione dell'installazione	13
Suggerimenti relativi a risorse provate	13
Porte e protocolli necessari	14
Piattaforme supportate	17
Requisiti del server di amministrazione DRA	18
Requisiti della Console Web e delle estensioni di DRA	21
Requisiti per la generazione di rapporti	22
Requisiti relativi alle licenze	23
Installazione del prodotto	23
Installazione del server di amministrazione DRA	24
Upgrade del prodotto	28
Pianificazione dell'upgrade di DRA	29
Task da eseguire prima dell'upgrade	29
Upgrade del server di amministrazione DRA	32
Esecuzione dell'upgrade delle estensioni REST di DRA	36
Upgrade del contenuto personalizzato	36

3 Configurazione del prodotto	39
--------------------------------------	-----------

Elenco di controllo della configurazione	39
Installazione o upgrade delle licenze	39
Aggiunta di domini gestiti	39
Aggiunta di sottoalberi gestiti	40
Configurazione delle impostazioni di DCOM	40
Configurazione del gruppo Distributed COM Users	41
Configurazione di controller di dominio e server di amministrazione	41

Informazioni su questa guida

La *Guida all'installazione* fornisce informazioni su pianificazione, installazione, gestione delle licenze e configurazione di 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 Directory and Resource Administrator. Per un elenco completo delle pubblicazioni di supporto a questa release, visitare il [sito Web della documentazione](https://www.netiq.com/documentation/directory-and-resource-administrator-92/) (<https://www.netiq.com/documentation/directory-and-resource-administrator-92/>).

Contattare l'assistenza alle vendite

Per informazioni su prodotti, prezzi e funzionalità, rivolgersi al partner locale. In caso d'impossibilità, contattare il team di assistenza alle vendite.

Sedi globali:	www.netiq.com/about_netiq/officelocations.asp
Stati Uniti e Canada:	1-888-323-6768
E-mail:	info@netiq.com
Sito Web:	www.netiq.com

Contattare il supporto tecnico

Per problemi specifici del prodotto, rivolgersi al team del supporto tecnico.

Sedi globali:	www.netiq.com/support/contactinfo.asp
Nord e Sud America:	1-713-418-5555
Europa, Medio Oriente e Africa:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Sito Web:	www.netiq.com/support

Contattare il supporto per la documentazione

NetIQ desidera fornire tutta la documentazione necessaria per indicare le soluzioni più appropriate alle esigenze degli utenti. Per suggerimenti volti a migliorare la documentazione, fare clic su **comment on this topic** (commenti sull'argomento) in fondo a qualsiasi pagina in HTML della documentazione. È inoltre possibile inviare un'e-mail a Documentation-Feedback@netiq.com. La collaborazione degli utenti è una fonte preziosa e saremo lieti di ricevere qualsiasi suggerimento.

Contattare la comunità online di utenti

NetIQ Communities, la comunità online di NetIQ, è una rete collaborativa che connette gli utenti con colleghi ed esperti di NetIQ. È una risorsa che contribuisce ad acquisire la conoscenza approfondita necessaria a sfruttare a pieno il potenziale degli investimenti IT fondamentali, in quanto offre informazioni più immediate, collegamenti e risorse utili e accesso agli esperti di NetIQ. Per ulteriori informazioni, visitare il sito <http://community.netiq.com>.

1 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.

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.

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

L'utilizzo congiunto di DRA ed ExA offre le soluzioni necessarie per il controllo e la gestione di ambienti Active Directory, Microsoft Windows, Microsoft Exchange e Microsoft Office 365.

- ♦ **Supporto per Active Directory, Office 365, Exchange e Skype for Business:** consente la gestione amministrativa di Active Directory, Exchange Server installato localmente, Skype for Business installato localmente, 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 l'automazione dei workflow.

Caratteristiche dei componenti di Directory and Resource Administrator

I componenti di DRA che si utilizzano regolarmente per gestire l'accesso con privilegi sono i server primario e secondario, le console di amministrazione, i componenti di generazione di rapporti e il motore di workflow Aegis che automatizza i processi di workflow.

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

Tipo di utente DRA	Interfacce utente	Server di amministrazione
Amministratore di DRA (la persona che si occuperà della configurazione del prodotto)	Console di delega e configurazione	Server primario
	Funzione di generazione rapporti di DRA Configurazione di Reporting Center (NRC)	Server secondario
	Interfaccia della riga di comando (<i>facoltativo</i>)	
	Provider ADSI di DRA (<i>facoltativo</i>)	
Amministratore occasionale dell'help desk	Console di gestione account e risorse	Server secondario
Amministratore occasionale dell'help desk	Console Web	Qualsiasi server DRA con REST di DRA installato

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, Office 365 e così via).

Console di gestione account e risorse

La console di gestione account e risorse è un'interfaccia utente installabile per gli amministratori aggiunti di DRA, che consente di visualizzare e gestire gli oggetti delegati di domini e servizi connessi.

Console Web

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

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

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

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

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

Componenti per la generazione di rapporti

La funzione di generazione rapporti di DRA include modelli integrati personalizzabili per la gestione di DRA e i dettagli dei domini e sistemi gestiti da DRA:

- ♦ Rapporti sulle risorse per oggetti AD

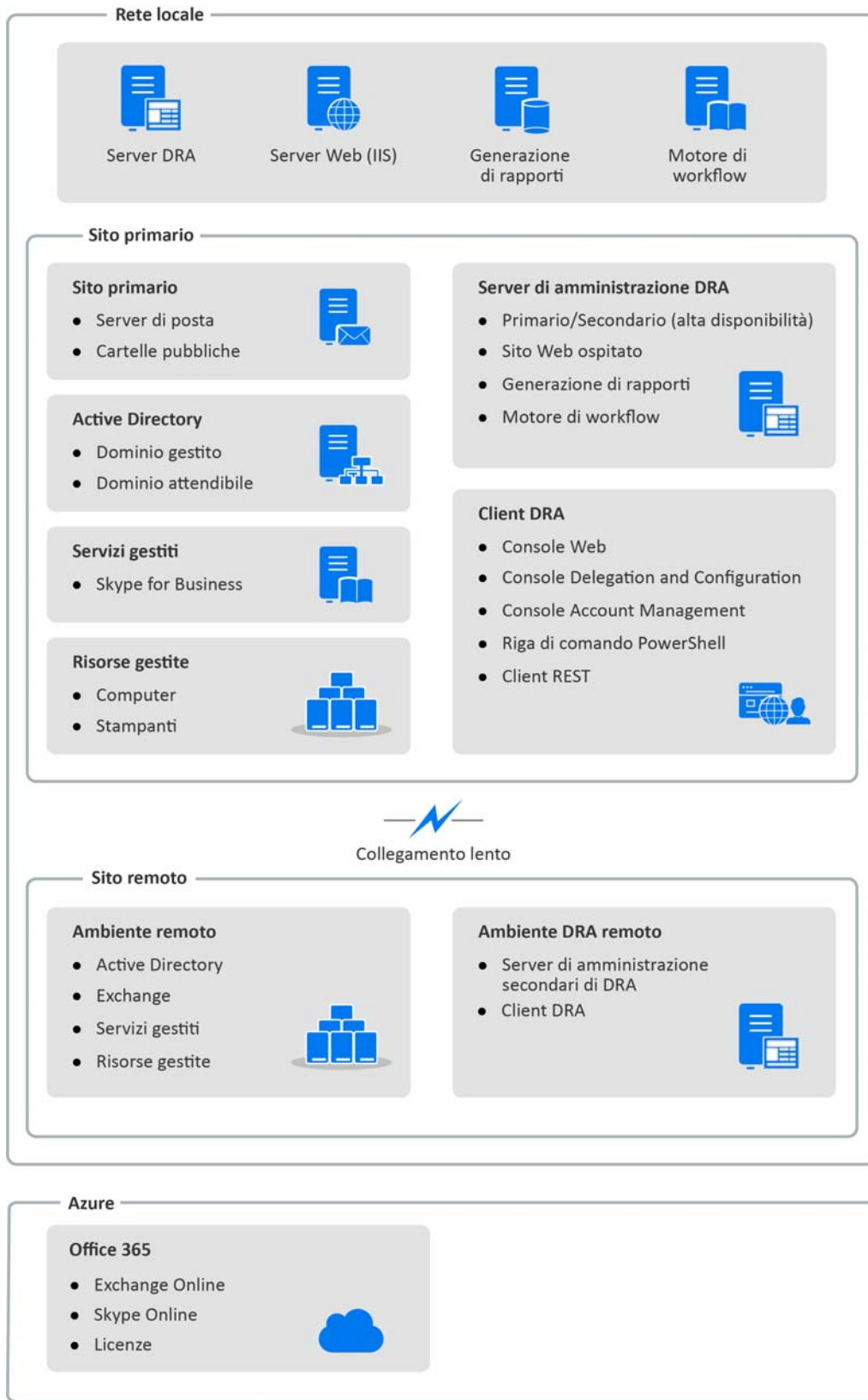
- ♦ Rapporti sui dati degli oggetti AD
- ♦ Rapporti di riepilogo di AD
- ♦ Rapporti di configurazione di DRA
- ♦ Rapporti di configurazione di Exchange
- ♦ Rapporti di Exchange Online di Office 365
- ♦ Rapporti dettagliati sulle tendenze delle attività (per mese, dominio e picco)
- ♦ Rapporti di riepilogo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

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

Motore di workflow

DRA si integra con il motore di workflow Aegis per automatizzare i task di workflow mediante la Console Web, in cui gli amministratori aggiunti possono configurare il server di workflow ed eseguire moduli di automazione dei workflow personalizzati, per poi visualizzare lo stato di tali workflow. Per ulteriori informazioni sul motore di workflow, vedere il [sito della documentazione di DRA \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Architettura del prodotto



2 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.

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	4 CPU (x64)/core 2.0 GHz	16 GB	100 GB
Console Web di DRA	2 CPU (x64)/core 2.0 GHz	8 GB	100 GB
Funzione di generazione rapporti di DRA	4 CPU (x64)/core 2.0 GHz	16 GB	100 GB
Server di workflow DRA	4 CPU (x64)/core 2.0 GHz	16 GB	100 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 (**)

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, client DRA	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 (http://go.microsoft.com/fwlink/?LinkID=46088) (Utilizzo di Distributed COM con firewall) (DCOM)
TCP 50000 *	Bidirezionale	Server di amministrazione DRA	Replica degli attributi e comunicazione fra server DRA e ADAM (LDAP)
TCP 50001 *	Bidirezionale	Server di amministrazione DRA	Replica degli attributi SSL (ADAM)
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
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	Necessari per tutti i server Exchange locali da 2010 a 2013 (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)

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 443, 5986, 5985	In uscita	Microsoft PowerShell	Cmdlet PowerShell nativi (HTTPS) e comunicazione remota di PowerShell
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 denominata.
TCP 8443	Bidirezionale	Server Change Guardian	Cronologia modifiche unificata

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 11192 * **	In uscita	Servizio Host di DRA	Per la comunicazione tra il servizio REST di DRA e il servizio di amministrazione di DRA
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, PowerShell di DRA e il servizio Host 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 (http://go.microsoft.com/fwlink/?LinkID=46088) (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 (http://go.microsoft.com/fwlink/?LinkID=46088) (Utilizzo di Distributed COM con firewall) (DCOM)

Protocollo e porta	Direzione	Destinazione	Utilizzo
TCP 1433	In uscita	Microsoft SQL Server	Archiviazione dei dati di workflow
TCP 8091	In entrata	Console delle operazioni e console di configurazione	Workflow API BSL (TCP)
TCP 8092 **	In entrata	Server di amministrazione DRA	Workflow API BSL (HTTP)
TCP 2219	Localhost	Provider dello spazio dei nomi	Utilizzati dal provider dello spazio dei nomi per eseguire gli adattatori
TCP 9900	Localhost	Correlation Engine	Utilizzati da Correlation Engine per comunicare con il motore di workflow 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 di Directory and Resource Administrator sul sito Web di NetIQ: <https://www.NetIQ.com/support>

Sistema gestito	Prerequisiti
Active Directory	♦ Microsoft Server 2012 ♦ Microsoft Server 2012 R2 ♦ Microsoft Server 2016
Microsoft Exchange	♦ Microsoft Exchange 2010 SP3 (fatta eccezione per le cartelle pubbliche) ♦ Microsoft Exchange 2013 ♦ Microsoft Exchange 2016 ♦ Microsoft Skype Online
Microsoft Office 365	♦ Microsoft Exchange Online ♦ Microsoft Skype Online ♦ Modulo di Windows Azure Active Directory per Windows PowerShell https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ♦ Skype for Business Online, Modulo Windows PowerShell https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype for Business	♦ Microsoft Skype for Business 2015
Cronologia modifiche	♦ Change Guardian 5.0, 5.1

Sistema gestito	Prerequisiti
Browser Web	♦ Microsoft Internet Explorer 11, Edge ♦ Google Chrome ♦ Mozilla Firefox

Requisiti del server di amministrazione DRA

I requisiti del server DRA per account e software sono riportati di seguito.

Requisiti software:

Componente	Prerequisiti
Destinazione di installazione	Sistema operativo del server di amministrazione NetIQ:
Sistema operativo	♦ Microsoft Windows Server 2012, 2012 R2, 2016 ♦ Microsoft Windows 2008 R2 è supportato solo per l'upgrade. Nota: il server deve anche essere un membro di un dominio Microsoft Windows Server nativo supportato. Interfacce DRA per Windows: ♦ Microsoft Windows Server 2012, 2012 R2, 2016 ♦ Microsoft Windows 8.1 (x86 e x64), 10 (x86 e x64)
Programma di installazione	♦ Microsoft .NET Framework 4.5.2 e versioni successive
Server di amministrazione	Directory and Resource Administrator: ♦ Microsoft .NET Framework 4.5.2 e versioni successive ♦ Uno dei programmi seguenti: ♦ Microsoft Visual C++ 2015 (aggiornamento 3) Redistributable Package (x64 e x86) ♦ Microsoft Visual C++ 2017 (aggiornamento 3) Redistributable Package (x64 e x86) ♦ Microsoft Message Queuing ♦ Ruoli di Microsoft Active Directory Lightweight Directory Services ♦ Servizio Registro di sistema remoto avviato Amministrazione di Microsoft Office 365/Exchange Online: ♦ Modulo di Windows Azure Active Directory per Windows PowerShell ♦ Assistente per l'accesso ai Microsoft Online Services per professionisti IT ♦ Skype for Business Online, Modulo Windows PowerShell Per ulteriori informazioni, vedere Piattaforme supportate.

Componente	Prerequisiti
Componenti Web legacy	Server Web: ♦ Microsoft Internet Information Services (IIS) versioni 8.0, 8.5, 10 Componenti di Microsoft IIS: ♦ Microsoft Active Service Pages (ASP) ♦ Microsoft Active Service Pages .NET (ASP .Net) ♦ Servizio ruolo di sicurezza di Microsoft IIS Interfacce DRA per Windows: ♦ Microsoft .NET Framework 4.5.2 ♦ Microsoft Visual C++ 2015 (aggiornamento 3) Redistributable Package (x86)

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 del servizio DRA	Autorizzazioni necessarie per eseguire il servizio di amministrazione NetIQ	♦ Autorizzazioni "Distributed COM Users" ♦ Membro del gruppo Amministratori di AD LDS ♦ Gruppo operatore di account ♦ Gruppi log archivio (OnePointOp ConfigAdms e OnePointOp) Nota: per ulteriori informazioni sull'impostazione di account di accesso ai domini di minimo privilegio, vedere Account di accesso DRA con minimo privilegio.
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 dell'assistente di DRA	Account a cui vengono delegati poteri attraverso DRA	♦ Aggiungere tutti gli account amministratore dell'assistente di DRA al gruppo "Distributed COM Users" affinché possano eseguire la connessione al server DRA da client remoti. 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: assegnare le seguenti autorizzazioni Active Directory all'account di accesso ai domini:

- ♦ Controllo COMPLETO sugli oggetti Utente
- ♦ Controllo COMPLETO sugli oggetti Computer
- ♦ Controllo COMPLETO sugli oggetti Gruppo
- ♦ Controllo COMPLETO sugli oggetti Contatto
- ♦ Controllo COMPLETO sugli oggetti Unità organizzativa
- ♦ Controllo COMPLETO sugli oggetti InetOrgPerson
- ♦ Controllo COMPLETO sugli oggetti Stampante
- ♦ Controllo COMPLETO sugli oggetti Dominio Integrato
- ♦ Controllo COMPLETO sugli oggetti Container
- ♦ Controllo COMPLETO sugli oggetti MsExchSystemObjectContainer
- ♦ Controllo COMPLETO sui gruppi di distribuzione dinamici
- ♦ Controllo COMPLETO sulle cartelle pubbliche

Specificare i seguenti privilegi con l'ambito "Questo oggetto e tutti gli oggetti figlio" per l'account del servizio del dominio:

- ♦ Consenti di creare oggetti Computer
- ♦ Consenti di eliminare oggetti Computer
- ♦ Consenti di creare oggetti Contatto
- ♦ Consenti di eliminare oggetti Contatto
- ♦ Consenti di creare oggetti Gruppo
- ♦ Consenti di eliminare oggetti Gruppo
- ♦ Consenti di eliminare oggetti InetOrgPerson
- ♦ Consenti di creare oggetti Unità organizzativa
- ♦ Consenti di eliminare oggetti Unità organizzativa
- ♦ Consenti di creare oggetti Utente
- ♦ Consenti di eliminare oggetti Utente

- ♦ Consenti di creare gruppi di distribuzione dinamici
- ♦ Consenti di eliminare gruppi di distribuzione dinamici
- ♦ Consenti di creare punto di connessione del servizio
- ♦ Consenti di eliminare punto di connessione del servizio
- ♦ Consenti di creare container
- ♦ Consenti di eliminare container
- ♦ Consenti di creare cartelle pubbliche
- ♦ Consenti di eliminare cartelle pubbliche

Account di accesso tenant di Office 365: assegnare le seguenti autorizzazioni di Active Directory all'account di accesso tenant di Office 365:

- ♦ Amministratore Gestione utenti in Office 365
- ♦ Gestione destinatari in Exchange Online

Account di accesso a Exchange: assegnare il ruolo **Gestione organizzazione** all'account di accesso a Exchange per gestire Exchange 2010.

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

Dopo l'installazione di DRA:

- ♦ Eseguire il comando seguente 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):

```
DraDelObjUtil.exe /domain:<NomeDominioNetbios> /delegate:<Nome account>
```

- ♦ Eseguire il comando seguente per delegare l'autorizzazione a "NetIQReceyleBin OU" dalla cartella di installazione di DRA (si noti che questa operazione può essere eseguita solo dopo aver aggiunto i rispettivi domini che devono essere gestiti tramite DRA):

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

- ♦ Aggiungere l'account prioritario di minimo privilegio al gruppo "Local Administrators" in ciascun computer di cui DRA gestirà le risorse, quali stampanti, servizi, log degli eventi, dispositivi e così via.
- ♦ Concedere all'account prioritario di minimo privilegio le "Autorizzazioni complete" sulle cartelle condivise o DFS in cui viene eseguito il provisioning delle directory Home.
- ♦ Aggiungere l'account prioritario di minimo privilegio al ruolo "Gestione organizzazione" per gestire gli oggetti di Exchange.

Requisiti della Console Web e delle estensioni di DRA

Di seguito sono riportati i requisiti per la Console Web e le estensioni REST.

Requisiti software:

Componente	Prerequisiti
Destinazione di installazione	Sistema operativo: ♦ Microsoft Windows Server 2016, Microsoft Windows 10 con Microsoft IIS 10 ♦ Microsoft Windows Server 2012, 2012 R2 con Microsoft IIS 8.0, 8.5
Servizio Host di DRA	♦ Microsoft .NET Framework 4.5.2 ♦ Server di amministrazione DRA
Endpoint e servizio REST di DRA	♦ Microsoft .NET Framework 4.5.2
Estensioni PowerShell	♦ Microsoft .NET Framework 4.5.2 ♦ PowerShell 4.0
Console Web di DRA	Server Web: ♦ Microsoft Internet Information Server 8.0, 8.5, 10 ♦ WCF di Microsoft Internet Information Services (attivazione) Componenti di Microsoft IIS: ♦ Server Web ♦ Funzioni HTTP comuni ♦ Contenuto statico ♦ Documento di default ♦ Browser di directory ♦ Errori HTTP ♦ Sviluppo di applicazioni ♦ ASP ♦ Integrità e diagnostica ♦ Registrazione HTTP ♦ Monitor richieste ♦ Sicurezza ♦ Autenticazione di base ♦ Prestazioni ♦ Compressione del contenuto statico ♦ Strumenti di gestione del server Web

Requisiti per la generazione di rapporti

Di seguito sono riportati i requisiti per la funzione di generazione rapporti di DRA.

Requisiti software:

Componente	Prerequisiti
Destinazione di installazione	Sistema operativo: ♦ Microsoft Windows Server 2012, 2012 R2, 2016
NetIQ Reporting Center (ver. 3.2)	Database: ♦ Microsoft SQL Server 2012, 2014, 2016 ♦ Microsoft SQL Server Reporting Services Server Web: ♦ Microsoft Internet Information Server 8.0, 8.5, 10 ♦ Componenti di Microsoft IIS: ♦ ASP .NET 4.0 Microsoft .NET Framework 3.5: Anche per tutti i server di amministrazione di DRA che eseguono la connessione alla funzione di generazione rapporti di DRA è necessario .NET Framework 3.5. 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.
Funzione di generazione rapporti di DRA	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.

Dopo aver installato il server di amministrazione, è possibile utilizzare l'utility Health Check per installare la chiave di una licenza di valutazione (License1.lic) che consente di gestire un numero illimitato di account utente e 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.

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.

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 NetIQ 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.
Esecuzione del programma di installazione di DRA	Avviare il programma di installazione di DRA. Nota: per eseguire il programma di installazione in un secondo momento, spostarsi nell'ubicazione in cui è stato estratto il supporto di installazione ed eseguire Setup.exe.
Selezione dei componenti del server di amministrazione NetIQ e della destinazione di installazione	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 NetIQ ♦ Resource Kit di archivio log ♦ NetIQ DRA SDK Componente Web legacy Interfacce utente ♦ Gestione account e risorse ♦ Provider ADSI di DRA ♦ Interfaccia della riga di comando ♦ Delega e configurazione
Verifica 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.
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale.

Passaggio	Dettagli
Selezione della modalità operativa dei server	Selezionare Primary (Primario) per installare il primo server di amministrazione DRA di un set multimaster (nell'installazione vi sarà un solo primario) o Secondary (Secondario) per unire un nuovo server di amministrazione DRA a un set multimaster esistente. Per informazioni sul set multimaster, vedere "Configuring the Multi-Master Set" (Configurazione del set multimaster) nella <i>Directory and Resource Administrator Administrator Guide</i> (Guida all'amministrazione di Directory and Resource Administrator).
Immissione degli account e delle credenziali di installazione	♦ Account del servizio DRA ♦ Gruppo AD LDS ♦ Amministratore di DRA Per ulteriori informazioni, vedere Requisiti del server di amministrazione DRA.
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.
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.

Installazione dei client DRA

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

NetIQDRAUserConsole.mst	Consente di installare la console di gestione account e risorse
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, ad esempio NetIQDRAUserConsole.mst, 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 delle estensioni REST di DRA

Il pacchetto delle estensioni REST di DRA include quattro funzioni:

- ♦ **Servizio host di NetIQ DRA:** gateway utilizzato per comunicare con il servizio di amministrazione di DRA. Questo servizio deve essere eseguito in un computer con il servizio di amministrazione di DRA installato.
- ♦ **Servizio REST ed endpoint di DRA:** forniscono le interfacce RESTful che consentono alla Console Web di DRA e ai client non DRA di richiedere operazioni DRA. Il servizio deve essere eseguito in un computer in cui è installata una console di DRA o il servizio di amministrazione di DRA.
- ♦ **Estensioni PowerShell:** forniscono un modulo PowerShell che consente ai client non DRA di richiedere operazioni DRA mediante cmdlet PowerShell.
- ♦ **Console Web di DRA:** interfaccia Web client utilizzata principalmente dagli amministratori aggiunti e che include anche opzioni di personalizzazione.

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.
Installazione del certificato SSL	Se non è stato già installato nel server Windows, prima di eseguire l'installazione è necessario installare un certificato SSL.
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.
Esecuzione del programma di installazione delle estensioni REST di DRA	Una volta terminata l'estrazione del supporto di installazione dal kit di installazione di DRA, verrà richiesto di avviare il programma di installazione di DRA. Passare all'ubicazione in cui il supporto di installazione è stato estratto, fare clic con il pulsante destro del mouse sul file DRARESTExtensionsInstaller.exe e selezionare Esegui come amministratore .
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale.

Passaggio	Dettagli
Selezione dei componenti e immissione dell'ubicazione di destinazione per l'installazione	Nella finestra di dialogo Seleziona componenti dell'installazione, selezionare tutte le opzioni: servizio Host di DRA, endpoint e servizio REST di DRA, estensioni PowerShell e Console Web di DRA. Accettare l'ubicazione di installazione di default C:\Program Files (x86)\NetIQ\DRA Extensions o specificare un'ubicazione alternativa per l'installazione.
Verifica 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.
Immissione dell'account del servizio da utilizzare per l'esecuzione	Per default, viene visualizzato l'account del servizio esistente dal server DRA. Specificare la password dell'account del servizio. Per ulteriori informazioni sulla configurazione di un account del servizio per il server di amministrazione DRA, vedere Requisiti del server di amministrazione DRA .
Immissione del certificato SSL del servizio REST	Selezionare il certificato SSL che verrà utilizzato per il servizio REST e specificare le porte dei servizi REST e Host.
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.

Installazione del server di workflow

Per informazioni sull'installazione del server di workflow, vedere la [Aegis Administrator Guide](#) (Guida all'amministrazione di Aegis).

Installazione della funzione di generazione rapporti di DRA

Per la funzione di generazione rapporti di DRA è necessario installare due file eseguibili del kit di installazione di NetIQ DRA: NRCSetup.exe e DRAReportingSetup.exe.

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 il prerequisito del programma di installazione di DRA.
Esecuzione del programma di installazione di NetIQ Reporting Center (NRC)	Una volta terminata l'estrazione del supporto di installazione dal kit di installazione di DRA, passare all'ubicazione in cui il supporto è stato estratto ed eseguire NRCSetup.exe.

Passaggi	Dettagli
Selezione del componente NetIQ Reporting Center	Nella finestra di dialogo Seleziona componenti dell'installazione, utilizzare il componente di default "NetIQ Reporting Center" per installare i quattro componenti di NRC.
Immissione dell'ubicazione di destinazione per l'installazione	Accettare l'ubicazione di installazione di default C:\Program Files (x86)\NetIQ\Reporting Center o specificare un'ubicazione alternativa per l'installazione.
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. Importante: .NET Framework 3.5 deve essere installato manualmente nel server di generazione di rapporti prima di installare NRC.
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale.
Installazione del database di configurazione	Utilizzare i valori di default della finestra di dialogo Configuration Database Installation - SQL Server Logon (Installazione del database di configurazione - Accesso a SQL Server) o fornire l'autenticazione SQL per completare l'installazione di NRC. Se si utilizza l'istanza di default per l'installazione di SQL Server, il campo Istanza deve rimanere vuoto.
Esecuzione dell'installazione della funzione di generazione rapporti di DRA	Passare all'ubicazione in cui è stato estratto il supporto d'installazione ed eseguire DRAReportingSetup.exe per installare il componente di gestione per l'integrazione con la funzione di generazione rapporti di DRA.
Accettazione del contratto di licenza EULA	Accettare i termini del contratto di licenza con l'utente finale per completare la procedura di installazione.

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 "Configuring the Multi-Master Set" (Configurazione del set multimaster) nella *Directory and Resource Administrator Administrator Guide* (Guida all'amministrazione di Directory and Resource Administrator).

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 AA (amministratori dell'assistente) utilizzeranno ciascun MMS. Se la maggior parte degli AA utilizzano server o set di server specifici, eseguire prima l'upgrade di tali server nelle ore non di punta.
- ♦ Determinare quali AA necessitano della console di delega e configurazione. È possibile ottenere queste informazioni in uno dei modi seguenti:
 - ♦ Verificare quali AA sono associati ai gruppi AA integrati.
 - ♦ Verificare quali AA sono associati a istanze di 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 assistente ActiveView) e Assistant Admin Groups (Gruppi amministratori assistente).

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

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

Notificare a questi AA 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 di server di amministrazione e interfacce utente (computer client degli AA). 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	<i>Facoltativo:</i> 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.

Nota: Se è necessario ripristinare il backup dell'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.

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 AA 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 AA 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 AA 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 AA 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 AA 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 Avviare l'interfaccia MMC.
- 3 Nel riquadro sinistro espandere **Gestione configurazione**.
- 4 Fare clic su **Server di amministrazione**.
- 5 Nel riquadro destro, selezionare il server di amministrazione primario appropriato per questo set di server.
- 6 Fare clic su **Proprietà**.
- 7 Nella scheda Pianificazione della sincronizzazione, fare clic su **Aggiorna ora**.
- 8 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.

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.

In DRA 9.2 o versioni successive, la configurazione del server di automazione dei workflow viene memorizzata in AD LDS anziché nel registro. Durante l'aggiornamento da DRA 9.1 o versioni precedenti a DRA 9.2 o versioni successive, la configurazione del registro viene automaticamente spostata in AD LDS e replicata in tutti i server secondari.

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

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.
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.
Installazione delle interfacce utente	Installare le interfacce utente per gli amministratori aggiunti.
Upgrade dei server secondari	Eseguire l'upgrade dei server di amministrazione secondari nell'MMS.
Upgrade della funzione di generazione rapporti di DRA	Eseguire l'upgrade della funzione di generazione rapporti di DRA.
Upgrade delle estensioni REST	Eseguire il programma di installazione delle estensioni REST di DRA.
Esecuzione dell'utility Health Check	Eseguire l'utility Health Check installata durante l'upgrade. Risolvere eventuali problemi.

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 degli AA solo dopo aver completato l'upgrade del server di amministrazione primario. Per ulteriori informazioni, vedere [Installazione delle interfacce utente di DRA](#).

Nota: per considerazioni e istruzioni più dettagliate 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 AA 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 AA 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 AA 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 AA 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 AA 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 AA, 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 AA che devono utilizzare il server di amministrazione primario, verificare di aver 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 o il provider ADSI, oppure 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 AA 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 AA.

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 AA, 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 Istruzioni agli AA che utilizzano tale server affinché installino le interfacce utente appropriate, come ad esempio la console di gestione account e risorse.
- 3 Ripetizione dei passaggi 1 e 2 fino a completare l'upgrade dell'MMS.

Prima di eseguire l'upgrade, notificare agli AA 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 AA 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 AA eseguono interfacce utente di cui è stato eseguito l'upgrade, mettere offline eventuali altri server che eseguono versioni precedenti di DRA.

Upgrade dei componenti della funzione di generazione rapporti di DRA

Prima di eseguire l'upgrade della funzione di generazione rapporti di DRA, accertarsi che l'ambiente soddisfi i requisiti minimi di NRC 3.2. Per ulteriori informazioni sui requisiti di installazione e considerazioni sull'upgrade, vedere la *Reporting Center Guide* (Guida di Reporting Center) nel sito della [documentazione di DRA](#).

Passaggi	Dettagli
Disabilitazione del supporto per la funzione di generazione rapporti di DRA	Affinché i servizi di raccolta per la generazione di rapporti non vengano eseguiti durante la procedura di upgrade, disabilitare il supporto per la funzione di generazione rapporti di DRA 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 della funzione di generazione rapporti di DRA	Eseguire DRAReportingSetup.exe dal kit di installazione e seguire le istruzioni della procedura guidata di installazione.
Esecuzione del programma di installazione di NRC	<i>Condizionale:</i> se il servizio Web NRC è installato in un computer diverso, accedere al computer in cui il servizio Web è installato ed eseguire NRCSetup.exe per avviare l'upgrade del servizio Web NRC. Nota: se il database di configurazione è stato installato in un server separato, eseguirne l'upgrade per primo

Passaggi	Dettagli
Esecuzione del programma di installazione di NRC nei computer client	Eseguire NRCSetup.exe in tutti i computer client NRC.
Abilitazione del supporto per la funzione di generazione rapporti di DRA	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 *NetIQ Reporting Center Reporting Guide* (Guida alla generazione dei rapporti di NetIQ Reporting Center) sul sito della [documentazione di DRA](#).

Esecuzione dell'upgrade delle estensioni REST di DRA

Per eseguire l'upgrade della Console Web e delle estensioni REST a Directory and Resource Administrator 9.2, è necessario utilizzare DRA 9.0.1 o versioni successive. Per informazioni sui requisiti, vedere [Requisiti della Console Web e delle estensioni di DRA](#).

Per eseguire l'upgrade della Console Web e delle estensioni di DRA:

- 1 Dopo aver effettuato il download del kit di installazione di DRA, passare all'ubicazione in cui è stato estratto il supporto di installazione, fare clic con il pulsante destro del mouse sul file DRARESTExtensionsInstaller.exe e selezionare **Esegui come amministratore**.
- 2 Seguire le istruzioni della procedura guidata di installazione fino al termine dell'installazione e fare clic su **Fine**.

Per ulteriori informazioni dettagliate sui passaggi della procedura guidata di installazione, fare riferimento ai passaggi per una nuova installazione: [Installazione delle estensioni REST di DRA](#).

Upgrade del contenuto personalizzato

Quando si esegue l'upgrade a una versione più recente di DRA, si desidera mantenere tutte le personalizzazioni effettuate per la Console Web nel server Web. Per semplificare questa operazione, DRA offre l'utility Customization Upgrade, integrata nel programma di installazione delle estensioni REST di DRA. Questa utility viene eseguita automaticamente quando si esegue DRARESTExtensionsInstaller.exe per l'upgrade delle estensioni REST nel server Web. È possibile anche ripetere manualmente l'esecuzione dell'utility dalla directory di installazione di DRA al di fuori dell'installazione.

Parte della procedura dell'utility Customization Upgrade consiste nell'eseguire il backup delle personalizzazioni dell'utente prima di avviare l'upgrade. Durante la procedura di upgrade, l'utility crea un file di log con tutte le modifiche apportate per eseguire l'upgrade e include inoltre un avviso per gli elementi di personalizzazione che non possono essere aggiornati automaticamente.

Come best practice, si consiglia di esaminare il log dopo l'upgrade. Se necessario, è possibile ripristinare le personalizzazioni precedenti all'upgrade copiandole dalla cartella di backup. È inoltre possibile definire il percorso della cartella delle personalizzazioni di cui viene eseguito l'upgrade quando si apre l'utility Customization Upgrade, oppure si può utilizzare il percorso di default, che viene compilato automaticamente.

I percorsi di default per le personalizzazioni di cui viene eseguito l'upgrade e per il backup delle personalizzazioni sono indicati di seguito:

- ♦ Percorso di default della cartella delle personalizzazioni:
C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom
- ♦ Cartella di backup di default:
\$CustomFolderPath\custom_upgrade_\$VERSIONFROM_to_\$VERSIONTO_backup

3 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.

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	<i>Facoltativo:</i> aggiungere altri domini e sottoalberi gestiti a DRA. Per ulteriori informazioni sui domini gestiti, vedere Aggiunta di domini gestiti .
Configurazione delle impostazioni di DCOM	<i>Facoltativo:</i> configurare le impostazioni di DCOM. Per ulteriori informazioni sulle impostazioni di DCOM, vedere Configurazione delle impostazioni di DCOM .

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. Dopo aver installato il server di amministrazione, utilizzare l'utility Health Check per installare il file della chiave di licenza di valutazione (TrialLicense.lic) fornito da NetIQ Corporation.

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.

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 "Configuring Caching" (Configurazione della memorizzazione nella cache) nella *Directory and Resource Administrator Administrator Guide* (Guida all'amministrazione di Directory and Resource Administrator).

Aggiunta di sottoalberi gestiti

Dopo aver installato il server di amministrazione, è possibile aggiungere sottoalberi gestiti da domini Microsoft Windows specifici. È possibile aggiungere eventuali sottoalberi mancanti che si desidera gestire mediante il nodo di configurazione avanzata nella console di delega e configurazione. 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 "Deleted Objects Utility" (Utility Deleted Objects) nella *Directory and Resource Administrator Administrator Guide* (Guida all'amministrazione di Directory and Resource Administrator).

Per ulteriori informazioni sull'impostazione dell'account di accesso, vedere "Specifying Domain Access Accounts" (Specifica di account di accesso ai domini) nella *Directory and Resource Administrator Administrator Guide* (Guida all'amministrazione di Directory and Resource Administrator).

Nota: dopo aver completato l'aggiunta di 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 "Configure Caching" (Configurazione della memorizzazione nella cache) nella *Directory and Resource Administrator Administrator Guide* (Guida all'amministrazione di Directory and Resource Administrator).

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.

Configurazione del gruppo Distributed COM Users

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. Questa appartenenza deve includere l'account del servizio DRA e tutti gli amministratori dell'assistente.

Per configurare il gruppo Distributed COM Users:

- 1 Eseguire l'accesso a un computer client 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 assistente. 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**.

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 Dal menu Start, scegliere **Impostazioni > Sistema e sicurezza > Pannello di controllo**.
- 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 Generale, selezionare **Pacchetto** nell'area 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.