

NetIQ® eDirectory™ 8.8 SP8

Guida alle novità

Settembre 2013



Note legali

QUESTA DOCUMENTAZIONE E IL SOFTWARE IVI DESCRITTO SONO FORNITI SU LICENZA E SONO SOGGETTI AI TERMINI DI TALE CONTRATTO O DI UN'ESCLUSIONE DI GARANZIA. A ECCEZIONE DI QUANTO STABILITO ESPRESSAMENTE IN TALE CONTRATTO DI LICENZA O ESCLUSIONE DI GARANZIA, NETIQ CORPORATION FORNISCE LA PRESENTE DOCUMENTAZIONE E IL SOFTWARE CHE VI È DESCRITTO "COME È" SENZA GARANZIA DI ALCUN TIPO, ESPRESSA O IMPLICITA, INCLUSE, MA NON LIMITATE A, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ O IDONEITÀ A UN PARTICOLARE SCOPO. IN ALCUNI STATI NON È CONSENTITO STIPULARE ESCLUSIONI DI GARANZIA ESPRESSE O IMPLICITE RELATIVAMENTE A DETERMINATE TRANSAZIONI. LA PRESENTE ESCLUSIONE POTREBBE QUINDI NON ESSERE APPLICABILE.

Per maggiore chiarezza, qualsiasi modulo, adattatore o altro materiale simile ("Modulo") viene concesso su licenza in base ai termini e alle condizioni del contratto di licenza con l'utente finale relativo alla versione pertinente del prodotto o del software NetIQ cui è correlato o con il quale interagisce. Mediante l'accesso, la copia o l'utilizzo di un modulo l'utente conferma di accettare termini del contratto di licenza. Se l'utente non accetta i termini del contratto di licenza con l'utente finale, questi non è autorizzato a utilizzare, accedere o copiare un modulo ed è inoltre tenuto a distruggere tutte le copie del modulo e contattare NetIQ per ricevere ulteriori istruzioni.

La documentazione e il software che vi è descritto non possono essere noleggiati, venduti o donati senza disporre di previa autorizzazione scritta di NetIQ Corporation, eccetto nei casi consentiti dalla legge. Eccetto come stabilito espressamente nel contratto di licenza nell'esclusione di garanzia, nessuna parte di questa documentazione o del software che vi è descritto può essere riprodotta, memorizzata in un sistema di ripristino o trasmessa in qualsiasi forma o mezzo, sia esso elettronico o meccanico, senza disporre di previa autorizzazione scritta di NetIQ Corporation. Alcune aziende, nomi e dati presenti nella documentazione vengono utilizzati solo a scopo illustrativo e potrebbero non avere alcun riscontro reale.

La documentazione potrebbe includere alcune inesattezze tecniche o errori tipografici. Periodicamente vengono apportate delle modifiche alle informazioni contenute. Tali modifiche potrebbero essere introdotte nelle nuove edizioni della documentazione. NetIQ Corporation potrebbe apportare dei miglioramenti o delle modifiche al software descritto nella documentazione in qualsiasi momento.

Diritti limitati del governo degli Stati Uniti: se il software e la documentazione sono stati acquistati da o per conto del governo degli Stati Uniti o da un fornitore principale diretto o indiretto a qualsiasi livello del governo degli Stati Uniti, conformemente all'articolo 48 C.F.R. 227.7202-4 (per gli acquisti realizzati dal DOD, Department of Defense - Dipartimento della Difesa) e gli articoli 48 C.F.R. 2.101 e 12.212 (per gli acquisti non realizzati dal DOD), i diritti del governo relativi a software e documentazione, inclusi quelli relativi a utilizzo, modifica, riproduzione, rilascio, esecuzione, visualizzazione o divulgazione del software o della documentazione, saranno soggetti interamente ai diritti e ai limiti di licenza commerciale previsti nel contratto di licenza.

© 2013 NetIQ Corporation e le sue consociate. Tutti i diritti riservati.

Per informazioni sui marchi di fabbrica di NetIQ, vedere <https://www.netiq.com/company/legal/>.

Sommario

Informazioni sulla Guida e la raccolta di documentazione	7
Informazioni su NetIQ Corporation	9
1 Funzioni e miglioramenti del Service Pack 8	11
1.1 Miglioramenti alla scalabilità	11
1.1.1 Controllo dei processi in background	11
1.1.2 Processo di sincronizzazione delle partizioni	11
1.1.3 Replica asincrona	12
1.1.4 Replica basata su policy	12
1.1.5 Necrologio	12
1.1.6 Rilevamento del conteggio dei necrologi e del conteggio della cache delle modifiche tramite iMonitor	12
1.1.7 Distributed Reference Links (DRL)	12
1.1.8 Memorizzazione nella cache degli eventi di registro	13
1.1.9 Supporto di SSD (Solid State Disks)	13
1.1.10 ACR (Determinazione costi riferimenti avanzata)	13
1.1.11 Intervallo di aggiornamento del login	13
1.2 Miglioramenti a LDAP	13
1.2.1 Controllo delle modifiche permissivo	14
1.2.2 Supporto orario generalizzato	14
1.2.3 Controllo di eliminazione sottoalberi	14
1.3 Supporto IPv6	14
1.4 Miglioramenti ai controlli	15
2 Piattaforme supportate per l'installazione di eDirectory	17
2.1 Piattaforme obsolete	17
2.2 Il test su Linux	17
2.3 Windows	18
3 Miglioramenti all'installazione e all'upgrade	19
3.1 Formati di pacchetti multipli per l'installazione di eDirectory 8.8	20
3.2 Installazione di eDirectory 8.8 in un'ubicazione personalizzata	20
3.2.1 Specifica di un'ubicazione personalizzata per i file di applicazione	20
3.2.2 Specifica di un'ubicazione personalizzata per i file di dati	21
3.2.3 Specifica di un'ubicazione personalizzata per i file di configurazione	21
3.3 Installazione non radice	22
3.4 Supporto migliorato per le installazioni sui cluster a elevata disponibilità	22
3.5 Conformità agli standard	22
3.5.1 Conformità a FHS	23
3.5.2 Conformità a LSB	24
3.6 Controlli sullo stato del server	24
3.6.1 Necessità dei controlli dello stato	24
3.6.2 Cos'è che garantisce la stabilità dello stato di un server?	24
3.6.3 Esecuzione dei controlli dello stato	24
3.6.4 Tipi di controlli dello stato	25
3.6.5 Categorizzazione dello stato	26
3.6.6 File di log	27
3.7 Integrazione di SecretStore con eDirectory	28

3.8	Installazione di eDirectory Instrumentation	28
3.9	Ulteriori informazioni	28
4	Backup e ripristino di NICI	29
5	Utility ndspasstore	31
6	Istanze multiple	33
6.1	Esigenza di istanze multiple	33
6.2	Scenari di esempio per l'installazione di istanze multiple	33
6.3	Utilizzo di istanze multiple	34
6.3.1	Pianificazione della configurazione	34
6.3.2	Configurazione di istanze multiple	34
6.4	Gestione di istanze multiple	35
6.4.1	Utility ndsmanage	35
6.4.2	Identificazione di un'istanza specifica	38
6.4.3	Chiamata di un'utility per un'istanza specifica	39
6.5	Scenario di esempio per più istanze	39
6.5.1	Pianificazione della configurazione	39
6.5.2	Configurazione delle istanze	39
6.5.3	Richiamo di un'utility per un'istanza	40
6.5.4	Elenco delle istanze	40
6.6	Ulteriori informazioni	40
7	Autenticazione a eDirectory tramite SASL-GSSAPI	41
7.1	Concetti	41
7.1.1	Cos'è Kerberos?	41
7.1.2	Cos'è SASL?	42
7.1.3	Cos'è GSSAPI?	42
7.2	Come funziona GSSAPI con eDirectory?	42
7.3	Configurazione di GSSAPI	43
7.4	In che modo LDAP utilizza GSSAPI?	44
7.5	Termini utilizzati comunemente	44
8	Applicazione di password universali che rilevano la distinzione tra maiuscole e minuscole	45
8.1	Esigenza di password in grado di rilevare la distinzione tra maiuscole e minuscole	46
8.2	Come far sì che la password rilevi la distinzione tra maiuscole e minuscole	46
8.2.1	Prerequisiti	46
8.2.2	Come fare in modo che la password rilevi la distinzione tra maiuscole e minuscole	47
8.2.3	Gestione delle password che rilevano la distinzione tra maiuscole e minuscole	47
8.3	Aggiornamento dei client Novell e delle utility esistenti	47
8.3.1	Migrazione alle password in grado di rilevare la distinzione tra maiuscole e minuscole	48
8.4	Esclusione dei client Novell esistenti dall'accesso al server eDirectory 8.8	49
8.4.1	Esigenza di impedire ai client Novell esistenti l'accesso al server eDirectory 8.8	49
8.4.2	Gestione delle configurazioni di login NDS	49
8.4.3	Operazioni sulla partizione	53
8.4.4	Applicazione di password in grado di rilevare la distinzione tra maiuscole e minuscole in un albero misto	53
8.5	Ulteriori informazioni	54

9	Supporto di Criteri password di Microsoft Windows Server 2008	55
9.1	Creazione di criteri password Windows Server 2008	55
9.2	Gestione dei Criteri password di Windows Server 2008	55
9.3	Ulteriori informazioni	56
10	Sincronizzazione con priorità	57
10.1	Esigenza di Sincronizzazione con priorità	57
10.2	Utilizzo di Sincronizzazione con priorità	58
10.3	Ulteriori informazioni	58
11	Cifratura dei dati	59
11.1	Cifratura degli attributi	59
11.1.1	Esigenza di attributi cifrati	59
11.1.2	Come cifrare gli attributi	60
11.1.3	Accesso agli attributi cifrati	60
11.2	Cifratura della replica	60
11.2.1	Esigenza della replica cifrata	60
11.2.2	Abilitazione della replica cifrata	60
11.3	Ulteriori informazioni	61
12	Prestazioni dell'inoltro di massa	63
13	Plug-in ICE di iManager ICE	65
13.1	Aggiunta dello schema mancante	65
13.1.1	Aggiungi schema da un file	65
13.1.2	Add Schema from a Server (Aggiungi schema a un server)	66
13.2	Confronto dello schema	66
13.2.1	Confronta file dello schema	67
13.2.2	Confronta schema tra server e file	67
13.3	Genera file dell'ordine	67
13.4	Ulteriori informazioni	67
14	Backup basato su LDAP	69
14.1	Esigenza del backup basato su LDAP	69
14.2	Ulteriori informazioni	69
15	Elenco LDAP Richiedi diritti effettivi	71
15.1	Esigenza dell'interfaccia dell'elenco Richiedi diritti effettivi LDAP	71
15.2	Ulteriori informazioni	71
16	Gestione della registrazione degli errori in eDirectory 8.8	73
16.1	Livelli di sicurezza dei messaggi	73
16.1.1	Fatale	73
16.1.2	Avviso	73
16.1.3	Errore	74
16.1.4	Informazioni	74
16.1.5	Debug	74
16.2	Configurazione della registrazione degli errori	74
16.2.1	Il test su Linux	75

16.2.2	Windows	75
16.3	Messaggi DSTrace	77
16.3.1	Il test su Linux	77
16.3.2	Windows	78
16.4	Filtraggio dei messaggi di iMonitor	80
16.5	Filtraggio dei messaggi SAL	80
16.5.1	Configurazione dei livelli di gravità	80
16.5.2	Impostazione del percorso del file di log	81
17	Utility bulkload offline: Idif2dib	83
17.1	Esigenza di Idif2dib	83
17.2	Ulteriori informazioni	83
18	Backup di eDirectory Backup con SMS	85
19	Revisione LDAP	87
19.1	Esigenza della revisione LDAP	87
19.2	Utilizzo della revisione LDAP	87
19.3	Ulteriori informazioni	88
20	Revisione con XDASv2	89
21	Varie	91
21.1	Segnalazione di dump della cache di iMonitor	91
21.2	Supporto di Microsoft Large Integer Syntax in iManager	91
21.3	Memorizzazione nella cache degli oggetti di sicurezza	92
21.4	Miglioramento delle prestazioni della ricerca nei sottoalberi	92
21.5	Modifiche a Localhost	93
21.6	Gestione di 256 file in Solaris	93
21.7	Gestione della memoria in Solaris	93
21.8	Gruppi nidificati	93

Informazioni sulla Guida e la raccolta di documentazione

Nella *Guida alle novità* vengono presentate le nuove funzioni di NetIQ eDirectory.

Per la versione più recente della *Guida alle novità di NetIQ eDirectory 8.8 SP8*, vedere il sito Web della [documentazione online di NetIQ eDirectory 8.8](#).

Destinatari

Questa guida è destinata agli amministratori di rete.

Altre informazioni incluse nella raccolta di documentazione

La raccolta di documentazione contiene le risorse seguenti:

Guida all'amministrazione di XDASv2

Descrive come configurare e utilizzare XDASv2 per il controllo di eDirectory e NetIQ Identity Manager.

Guida all'installazione

Descrive come installare eDirectory ed è destinata agli amministratori di rete.

Guida all'amministrazione

Descrive come gestire e configurare eDirectory.

Guida alla soluzione dei problemi

Descrive come risolvere i problemi relativi a eDirectory.

Guida all'ottimizzazione per piattaforme Linux

Descrive come analizzare e ottimizzare eDirectory per le piattaforme Linux al fine di ottenere prestazioni migliori in tutte le installazioni.

Le guide sono disponibili sul [sito Web della documentazione di NetIQ eDirectory 8.8](https://www.netiq.com/documentation/edir88/) (<https://www.netiq.com/documentation/edir88/>).

Per informazioni sull'utility di gestione eDirectory, vedere [NetIQ iManager 2.7 Administration Guide](https://www.netiq.com/documentation/imanager/) (<https://www.netiq.com/documentation/imanager/>) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

Informazioni su NetIQ Corporation

NetIQ Corporation è una società globale di software per le aziende, focalizzata su tre problematiche costanti dell'ambiente aziendale - cambiamento, complessità e rischio - e che offre soluzioni utili per gestirle.

Il nostro punto di vista

Adattamento al cambiamento e gestione della complessità: sfide ben note

Fra tutte le sfide da affrontare, queste sono forse le variabili principali che impediscono il controllo necessario a misurare, monitorare e gestire in modo sicuro gli ambienti informatici fisici, virtuali e cloud.

Erogazione migliore e più rapida dei servizi aziendali di importanza critica

Siamo convinti del fatto che le nostre soluzioni per assicurare il massimo controllo possibile alle organizzazioni IT siano il solo percorso verso un'erogazione tempestiva ed economica dei servizi. Il costante processo di cambiamento delle organizzazioni e la maggiore complessità intrinseca delle tecnologie necessarie per gestirlo continueranno ad esercitare pressioni sempre più forti.

La nostra filosofia

Vendiamo soluzioni intelligenti e non semplice software

Al fine di poter garantire un controllo affidabile, prima di tutto ci dedichiamo a comprendere le situazioni reali in cui le organizzazioni IT operano quotidianamente. Questo approccio è il solo che consenta di sviluppare soluzioni IT pratiche e intelligenti, capaci di garantire risultati misurabili e comprovati, e che ci gratifica molto di più della semplice vendita di software.

Il successo degli utenti è il nostro stimolo

Il fulcro attorno al quale ruota la nostra attività aziendale è il successo degli utenti. Dall'ideazione del prodotto alla sua installazione, non dimentichiamo mai l'esigenza di poter contare su soluzioni IT funzionanti e che si integrino alla perfezione con i prodotti esistenti, fornendovi supporto costante e formazione successiva all'installazione oltre che, tanto per cambiare, essendo un partner con cui è veramente facile collaborare. In sintesi: il successo degli utenti è il nostro successo.

Le nostre soluzioni

- ♦ Governance di identità e accessi
- ♦ Gestione degli accessi
- ♦ Gestione sicurezza
- ♦ Gestione di sistemi e applicazioni

- ♦ Gestione dei carichi di lavoro
- ♦ Gestione servizio

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
Email:	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
Email:	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 inviare suggerimenti di miglioramento, fare clic su **comments on this topic** (commenti su questo argomento) in fondo a qualsiasi pagina nelle versioni in HTML della documentazione pubblicata sul sito Web www.netiq.com/documentation. 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

La comunità online di NetIQ, Qmunity, è una rete collaborativa che unisce utenti 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 Funzioni e miglioramenti del Service Pack 8

In questo capitolo viene fornita una panoramica delle funzioni e dei miglioramenti inclusi in eDirectory 8.8 SP8.

1.1 Miglioramenti alla scalabilità

Per garantire una sincronizzazione dei dati e un'elaborazione dei necrologi più rapide, nonché una ridotta occupazione della memoria nell'elaborazione degli eventi di registro, in eDirectory 8.8 SP8 sono inclusi i miglioramenti alla scalabilità citati nelle sezioni seguenti.

In questa versione, alcuni processi in background sono stati riprogettati in modo da soddisfare ambienti dinamici più grandi. Ciò include l'ottimizzazione dei processi di background esistenti e l'offerta di opzioni di configurazione per ottimizzare i sistemi in modo appropriato all'ambiente in uso.

1.1.1 Controllo dei processi in background

Gli amministratori possono controllare il processo in background configurando le seguenti policy Impostazioni di ritardo processi in background nella finestra Impostazioni del processo in background in NetIQ iMonitor:

- ♦ **CPU:** specifica la percentuale massima di risorse del computer e la durata massima dell'inattività dello stesso processo (sincronizzazione di partizioni, eliminazione, o necrologio).
- ♦ **Limite di hardware:** specifica un'impostazione di ritardo statica per i singoli processi di sincronizzazione di partizioni, eliminazione e necrologio.

Per informazioni sulla configurazione di processi in background, vedere [“Configuring Background Processes \(Configurazione dei processi in background\)”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.1.2 Processo di sincronizzazione delle partizioni

Per aumentare i thread creati per consentire la replica contemporanea nel massimo numero di server possibile, è possibile utilizzare il processo di sincronizzazione delle partizioni per impostare manualmente il numero massimo di thread creati. Questa impostazione può essere applicata a tutte le partizioni di un server.

Per informazioni sulla configurazione del processo di sincronizzazione delle partizioni, vedere [“Manually Configuring Synchronization Threads”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.1.3 Replica asincrona

Per ridurre il tempo richiesto per la replica, le operazioni indicate di seguito devono essere eseguite in parallelo:

- ◆ Elaborazione della cache delle modifiche
- ◆ Invio di pacchetti a un server remoto

La nuova opzione **Impostazioni Sincronizzazione asincrona in uscita (millisecondi)** consente di evitare di sovraccaricare il server ricevente. Per impostazione predefinita, questa opzione è disattivata. La configurazione dipende dall'ambiente a disposizione. Quando si attiva questa opzione, impostarla su 100, quindi regolarla verso l'alto o verso il basso secondo necessità.

Per informazioni sulla configurazione della sincronizzazione in uscita asincrona, vedere [“Configuring Asynchronous Outbound Synchronization”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.1.4 Replica basata su policy

Gli amministratori ora possono creare una policy (file XML) per specificare la modalità di replica delle modifiche. Tale soluzione può essere utile se viene distribuito un anello di replica a più ubicazioni. Se la policy contiene un errore di ortografia o di sintassi, la replica ritorna al metodo predefinito.

Per ulteriori informazioni, vedere [“Policy Based Replication”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.1.5 Necrologio

Un necrologio generato a causa dell'eliminazione, della ridenominazione o dello spostamento di oggetti viene elaborato più rapidamente rispetto a quanto avveniva nelle precedenti versioni di eDirectory. Ad esempio, un aggiornamento che nelle versioni precedenti richiedeva cinque cicli, ora potrebbe richiedere solo due cicli.

Inoltre, il processo del necrologio ora può essere eseguito parallelamente al processo di sincronizzazione delle partizioni.

1.1.6 Rilevamento del conteggio dei necrologi e del conteggio della cache delle modifiche tramite iMonitor

iMonitor consente di visualizzare il numero di oggetti con necrologi in ogni stato. Inoltre, consente di visualizzare il numero di oggetti nella cache delle modifiche di una partizione quando si visualizza un oggetto di partizione tramite iMonitor in un dato server. In tal modo è possibile monitorare ulteriormente lo stato della sincronizzazione e dell'elaborazione dei necrologi.

1.1.7 Distributed Reference Links (DRL)

Per ottimizzare l'elaborazione dei necrologi, in eDirectory non vengono più utilizzati gli attributi DRL:

- ◆ UsedBy
- ◆ ObitUsedBy

1.1.8 Memorizzazione nella cache degli eventi di registro

Il sistema degli eventi di registro viene modificato in modo da consentire l'uso di una combinazione di memoria e disco per gestire gli eventi nella coda. In tal modo si riduce notevolmente la crescita della memoria del processo ndsd.

I miglioramenti agli eventi di registro includono:

- ♦ **Memorizzazione nella cache**

Quando la coda degli eventi di registro cresce e supera un determinato punto della memoria (32 MB = max. di blocchi di 8 x 4 MB), eDirectory comincia a utilizzare una cache sul disco rigido.

- ♦ **Variabili**

Gli eventi di registro includono le seguenti variabili che possono essere configurate dagli utenti:

- ♦ NDS_EVENT_DISK_CACHE
- ♦ NDS_EVENT_DISK_CACHE_DIR

- ♦ **Compressione**

Il miglioramento della compressione consente di ridurre al minimo le dimensioni dei dati sul disco rigido. Il rapporto di compressione è approssimativamente di 20:1.

1.1.9 Supporto di SSD (Solid State Disks)

Questa versione supporta SSD di classe Enterprise per operazioni IO migliorate.

1.1.10 ACR (Determinazione costi riferimenti avanzata)

In questa versione, l'ARC è abilitata per impostazione predefinita.

Per ulteriori informazioni, vedere "[Advanced Referral Costing](#)" nella *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.1.11 Intervallo di aggiornamento del login

La nuova opzione Intervallo per disabilitazione aggiornamento login consente agli amministratori di specificare un intervallo di tempo (in secondi) durante il quale eDirectory non aggiorna gli attributi di login.

Nota: Questa opzione si applica solo ai login NDS (NetIQ Directory Services).

Per ulteriori informazioni, vedere "[Controlling and Configuring the DS Agent](#)" in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.2 Miglioramenti a LDAP

In questa versione sono inclusi i seguenti miglioramenti a LDAP:

1.2.1 Controllo delle modifiche permissivo

Questa opzione consente di estendere l'operazione di modifica LDAP corrente. Se si tenta di eliminare un attributo che non esiste o di aggiungere un qualsiasi valore a un attributo esistente, l'operazione viene eseguita senza che venga visualizzato alcun messaggio di errore.

Per ulteriori informazioni, vedere *“Configuring Permissive Modify Control”* nella *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.2.2 Supporto orario generalizzato

L'opzione Generalized Time Support (Supporto orario generalizzato) consente di visualizzare l'ora nel formato AAAAMMGGHHmmSS.0Z.

È opportuno notare che 0Z indica il supporto delle frazioni di secondo come in Active Directory. Dal momento che eDirectory non supporta la visualizzazione delle frazioni di secondo, questa opzione visualizza 0 per evitare di interrompere la funzionalità in un ambiente coesistente.

Per ulteriori informazioni, vedere *“Configuring Generalized Time Support”* nella *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

1.2.3 Controllo di eliminazione sottoalberi

Questa versione supporta il controllo di eliminazione dei sottoalberi che consente l'eliminazione di qualsiasi oggetto contenitore. In precedenza, era possibile eliminare solo gli oggetti foglia. Tuttavia, il controllo di eliminazione dei sottoalberi non supporta l'eliminazione dei contenitori di partizioni.

1.3 Supporto IPv6

Questa versione supporta le reti IPv4 e IPv6. Per impostazione predefinita, IPv6 viene abilitato automaticamente quando si installa eDirectory. Se si esegue l'aggiornamento da una versione precedente di eDirectory, è necessario abilitare manualmente il supporto IPv6.

eDirectory 8.8 SP8 supporta le seguenti modalità IPv6:

- ◆ Doppio stack
- ◆ Tunneling
- ◆ IPv6 puro

eDirectory 8.8 SP8 non supporta i seguenti tipi di indirizzi IPv6:

- ◆ Indirizzi locali di collegamento
- ◆ Indirizzi IPv6 mappati a IPv4
- ◆ Indirizzi IPv6 compatibili con IPv4

eDirectory 8.8 SP8 supporta i seguenti formati di indirizzamento:

- ◆ [::]
- ◆ [::1]
- ◆ [2015::12]
- ◆ [2015::12]:524

1.4 Miglioramenti ai controlli

In questa versione è stato migliorato il controllo XDAS grazie al supporto dell'indirizzo IP del client negli eventi.

2 Piattaforme supportate per l'installazione di eDirectory

eDirectory 8.8 SP8 è una versione multipiattaforma che ha come obiettivo il miglioramento della stabilità di eDirectory.

2.1 Piattaforme obsolete

In eDirectory 8.8 SP8 le piattaforme seguenti non sono supportate:

- ♦ NetWare
- ♦ eDirectory a 32 e 64 bit in Solaris
- ♦ eDirectory a 32 bit in AIX
- ♦ eDirectory a 32 bit in Linux
- ♦ eDirectory a 32 bit in Windows

2.2 Il test su Linux

È necessario installare eDirectory su una delle seguenti piattaforme:

- ♦ SLES 11 SP1, SP2 e SP3 a 64 bit
- ♦ SLES 10 SP4 a 64 bit
- ♦ RHEL 5.7, 5.8 e 5.9
- ♦ RHEL 6.2, 6.3 e 6.4

È possibile eseguire questi sistemi operativi in modalità virtuale su uno dei seguenti hypervisor:

- ♦ VMware ESXi
- ♦ Xen (su SLES 10 e SLES 11 e i relativi Support Pack)

Nota: eDirectory 8.8 SP8 è supportato sul servizio di virtualizzazione SLES 10 XEN che esegue il sistema operativo guest SLES 10. I seguenti aggiornamenti sono disponibili sul [sito Web NetIQ Update \(https://update.novell.com\)](https://update.novell.com):

- ♦ SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
- ♦ Aggiornamenti SLES10

Per registrare e aggiornare SUSE Linux Enterprise 10, fare riferimento a [Registrazione di SUSE Linux Enterprise con NetIQ Customer Center \(http://www.suse.com/products/register.html\)](http://www.suse.com/products/register.html).

Dopo aver installato l'aggiornamento più recente, accertarsi che il livello di patch minimo dell'aggiornamento installato sia 3.0.2_09763-0.8.

-
- ♦ Windows Server 2008 R2 Virtualization con Hyper-V

Per determinare la versione di SUSE Linux in esecuzione, vedere il file `/etc/SuSE-release`.

Assicurarsi di applicare le patch glibc più recenti scaricandole dal sito Web [Red Hat Errata \(http://rhn.redhat.com/errata\)](http://rhn.redhat.com/errata). La versione minima richiesta della libreria glibc è la 2.1.

2.3 Windows

È necessario installare eDirectory su una delle seguenti piattaforme:

- ♦ Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) e relativi Service Pack
- ♦ Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) e relativi Service Pack
- ♦ Windows Server 2012

Importante

- ♦ Per installare eDirectory 8.8 SP8 su Windows Server 2008 R2 è necessario utilizzare un account dotato di diritti amministrativi.
 - ♦ Le versioni desktop di Windows non sono supportate.
-

3 Miglioramenti all'installazione e all'upgrade

In questo capitolo vengono discussi le nuove funzioni e i miglioramenti con l'installazione e l'upgrade di NetIQ eDirectory 8.8.

Nella tabella seguente sono elencate le nuove funzioni e specificate le piattaforme sulle quali sono supportate.

Funzione	Linux	Windows
Formati di pacchetto multipli per l'installazione di eDirectory 8.8	✓	✗
Installazione ubicazione personalizzata per i file delle applicazioni	✓	✓
Installazione ubicazione personalizzata per i file di dati	✓	✓
Installazione ubicazione personalizzata per i file di configurazione	✓	✗
Installazione non radice	✓	✗
Supporto migliorato per installazioni su cluster a elevata disponibilità	✓	✓
Conformità a FHS	✓	✗
Conformità a LSB	✓	✗
Controlli dello stato del server	✓	✓
Integrazione SecretStore	✓	✓
Installazione di eDirectory Instrumentation	✓	✓

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ Sezione 3.1, "Formati di pacchetti multipli per l'installazione di eDirectory 8.8", a pagina 20
- ♦ Sezione 3.2, "Installazione di eDirectory 8.8 in un'ubicazione personalizzata", a pagina 20
- ♦ Sezione 3.3, "Installazione non radice", a pagina 22
- ♦ Sezione 3.4, "Supporto migliorato per le installazioni sui cluster a elevata disponibilità", a pagina 22
- ♦ Sezione 3.5, "Conformità agli standard", a pagina 22
- ♦ Sezione 3.6, "Controlli sullo stato del server", a pagina 24
- ♦ Sezione 3.7, "Integrazione di SecretStore con eDirectory", a pagina 28

- ♦ [Sezione 3.8, “Installazione di eDirectory Instrumentation”](#), a pagina 28
- ♦ [Sezione 3.9, “Ulteriori informazioni”](#), a pagina 28

3.1 Formati di pacchetti multipli per l'installazione di eDirectory 8.8

Linux consente di scegliere tra vari formati file durante l'installazione di eDirectory 8.8 sull'host. I formati file sono elencati nella tabella di seguito.

Tipo di utente e ubicazione di installazione	Il test su Linux
Utente root	
ubicazione di default	RPM
Ubicazione personalizzata	Tarball
Utente nonroot	
Ubicazione personalizzata	Tarball

Per ulteriori informazioni sull'installazione mediante tarball, fare riferimento a [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guida all'installazione di NetIQ eDirectory 8.8 SP8).

3.2 Installazione di eDirectory 8.8 in un'ubicazione personalizzata

eDirectory 8.8 offre la flessibilità di installare file dell'applicazione, file di dati e file di configurazione in un'ubicazione a scelta.

Uno degli scenari per l'installazione di eDirectory 8.8 in un'ubicazione personalizzata si verifica quando si dispone di una versione precedente di eDirectory installata sull'host e si desidera testare eDirectory 8.8 prima di effettuare l'aggiornamento. In tal modo è possibile disporre della configurazione eDirectory esistente senza problemi e anche testare questa nuova versione. È quindi possibile decidere se mantenere la versione esistente o eseguire l'upgrade a eDirectory 8.8.

Nota: SLP e il subagente SNMP vengono installati nelle ubicazioni predefinite.

In questa sezione viene spiegato come installare i diversi file in un'ubicazione personalizzata:

- ♦ [Sezione 3.2.1, “Specificazione di un'ubicazione personalizzata per i file di applicazione”](#), a pagina 20
- ♦ [Sezione 3.2.2, “Specificazione di un'ubicazione personalizzata per i file di dati”](#), a pagina 21
- ♦ [Sezione 3.2.3, “Specificazione di un'ubicazione personalizzata per i file di configurazione”](#), a pagina 21

3.2.1 Specificazione di un'ubicazione personalizzata per i file di applicazione

Durante l'installazione di eDirectory, è possibile installare i file di applicazione in un'ubicazione a scelta.

Il test su Linux

Per installare eDirectory 8.8 in un'ubicazione personalizzata, è possibile utilizzare il file di installazione tarball e decomprimere eDirectory 8.8 in un'ubicazione a scelta.

Windows

È possibile specificare un'ubicazione personalizzata per i file di applicazione durante la procedura guidata di installazione persino prima di eDirectory 8.8.

3.2.2 Specifica di un'ubicazione personalizzata per i file di dati

Durante la configurazione di eDirectory, è possibile salvare i file di dati in un'ubicazione a scelta. I file di dati includono le directory `data`, `dib` e `log`.

Il test su Linux

Per configurare i file di dati in un'ubicazione personalizzata, è possibile utilizzare l'opzione `-d` o `-D` dell'utilità `ndsconfig`.

Opzione	Descrizione
<code>-d custom_location</code>	Consente di creare la directory <code>DIB</code> (il database eDirectory) nel percorso indicato. Nota: Questa opzione era presente anche prima di eDirectory 8.8.
<code>-D custom_location</code>	Consente di creare le directory <code>data</code> (contiene dati quali i pid e gli ID socket), <code>dib</code> e <code>log</code> nel percorso indicato.

Windows

In Windows verrà richiesto di immettere il percorso `DIB` durante l'installazione. Immettere un percorso a scelta.

3.2.3 Specifica di un'ubicazione personalizzata per i file di configurazione

Durante la configurazione di eDirectory, è possibile selezionare il percorso in cui si desidera salvare i file di configurazione.

Il test su Linux

Per configurare il file di configurazione `nds.conf` in un'altra ubicazione, utilizzare l'opzione `--config-file` dell'utilità `ndsconfig`.

Per installare gli altri file di configurazione (ad esempio `modules.conf`, `ndsimon.conf` e `ice.conf`) in un'altra ubicazione, effettuare le seguenti operazioni:

- 1 Copiare tutti i file di configurazione nella nuova ubicazione.
- 2 Impostare la nuova ubicazione immettendo la stringa seguente:

```
ndsconfig set n4u.nds.configdir custom_location
```

Windows

Non è possibile specificare un'ubicazione personalizzata per i file di configurazione in Windows.

3.3 Installazione non radice

eDirectory 8.8 e le versioni successive supportano l'installazione e la configurazione di server eDirectory da parte di un utente nonroot. Le versioni precedenti di eDirectory possono essere installate e configurate solo da un utente root con una singola istanza di eDirectory in esecuzione su un host.

Con eDirectory 8.8 o versione superiore, qualsiasi utente nonroot può utilizzare una build tarball per installare eDirectory. Possono essere presenti più istanze di installazioni binarie di eDirectory da parte dello stesso utente o di utenti diversi. Tuttavia, persino per le installazioni utente nonroot, i servizi a livello di sistema, come NICI (Novell International Cryptographic Infrastructure), SNMP e SLP possono essere installati solo con privilegi radice. NICI è un componente obbligatorio, mentre SNMP e SLP sono componenti facoltativi per la funzionalità eDirectory. Inoltre, con un'installazione di pacchetto, l'utente root può installare una sola istanza.

Dopo l'installazione, un utente nonroot può configurare istanze server di eDirectory utilizzando la propria installazione tarball singola oppure un'installazione binaria. Ciò significa che su un singolo host possono essere in esecuzione più istanze del server eDirectory poiché ogni utente, radice o non radice, può configurare più istanze del server eDirectory su un singolo host mediante un'installazione di pacchetto o tarball. Per ulteriori dettagli sulla funzione Multiple Instances (Istanze multiple), fare riferimento a [“Multiple Instances”](#) e [“Upgrading Multiple Instances”](#) in *NetIQ eDirectory 8.8 SP8 Installation Guide* (Guida all'installazione di NetIQ eDirectory 8.8 SP8).

L'installazione non radice e la configurazione si applicano solo alle piattaforme Linux. Per ulteriori informazioni sull'installazione non radice e sulla configurazione, fare riferimento a [“Nonroot User Installing eDirectory 8.8”](#) in *NetIQ eDirectory 8.8 SP8 Installation Guide* (Guida all'installazione di NetIQ eDirectory 8.8 SP8).

3.4 Supporto migliorato per le installazioni sui cluster a elevata disponibilità

eDirectory 8.8 SP8 semplifica l'installazione e la gestione di eDirectory sui cluster sia Linux che Windows, migliorando il supporto della gestione in cluster e l'abilitazione dell'elevata disponibilità. eDirectory fornisce inoltre disponibilità elevata attraverso la sincronizzazione della replica, che può essere combinata con la gestione in cluster per ottenere un livello maggiore di disponibilità.

Per ulteriori informazioni sull'installazione di eDirectory nei cluster, vedere [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guida all'installazione di NetIQ eDirectory 8.8 SP8).

3.5 Conformità agli standard

eDirectory 8.8 è compatibile con i seguenti standard:

- ♦ [Sezione 3.5.1, “Conformità a FHS”, a pagina 23](#)
- ♦ [Sezione 3.5.2, “Conformità a LSB”, a pagina 24](#)

3.5.1 Conformità a FHS

Per evitare i conflitti di file con altri file di applicazioni di prodotto, eDirectory 8.8 segue lo standard FHS (Filesystem Hierarchy Standard). Questa funzione è disponibile solo su Linux.

In eDirectory questa struttura di directory viene seguita solo se si è scelto di eseguire l'installazione nell'ubicazione di default. Se è stata scelta un'ubicazione personalizzata, la struttura di directory sarà *custom_location/default_path*.

Se, ad esempio, si sceglie di eseguire l'installazione nella directory eDir88, la stessa struttura di directory sarà seguita nella directory eDir88, come la documentazione man sarà installata nella directory `/eDir88/opt/novell/man`.

Nella tabella seguente è elencata la modifica nella struttura di directory:

Tipi di file archiviati nella directory	Nome e percorso della directory
Binari eseguibili e script di shell statici	<code>/opt/novell/eDirectory/bin</code>
Binari eseguibili per utilizzo root	<code>/opt/novell/eDirectory/sbin</code>
Binari di librerie statiche o dinamiche	<code>/opt/novell/eDirectory/lib</code>
File di configurazione	<code>/etc/opt/novell/eDirectory/conf</code>
Dati dinamici di runtime di lettura/scrittura come DIB	<code>/var/opt/novell/eDirectory/data</code>
File di log	<code>/var/opt/novell/eDirectory/log</code>
Documentazione man di Linux	<code>/opt/novell/man</code>

Esportare le variabili ambientali

Con l'implementazione di FHS in eDirectory 8.8, è necessario aggiornare le variabili ambientali di percorso ed esportarle. Tale operazione crea i seguenti problemi:

- ♦ È necessario ricordare tutti i percorsi esportati, in modo che ogni volta che si apre una shell, è necessario esportarli cominciare a utilizzare le utility.
- ♦ Se si desidera utilizzare più set di file binari, è necessario aprire più shell oppure modificare con una certa frequenza il percorso dei set di file binari.

Per risolvere il problema, è possibile utilizzare lo script `/opt/novell/eDirectory/bin/ndspath` nel modo indicato di seguito:

- ♦ Aggiungere lo script `ndspath` come prefisso all'utility ed eseguire l'utility desiderata nel modo descritto di seguito:

```
custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```
- ♦ Esportare i percorsi nella shell come descritto di seguito:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```
- ♦ Dopo aver immesso il comando indicato in precedenza, eseguire le utility nel modo normale. Chiamare lo script nel profilo, nel `bashrc` o in script simili. Pertanto, ogni volta che si esegue il login o si apre una shell, è possibile cominciare a utilizzare le utility direttamente.

3.5.2 Conformità a LSB

eDirectory 8.8 ora è conforme a LSB (Linux Standard Base). LSB inoltre suggerisce la conformità a FHS. Tutti i pacchetti eDirectory in Linux hanno come prefisso *novell*. Ad esempio, NDSserv ora è *novell-NDSserv*.

3.6 Controlli sullo stato del server

eDirectory 8.8 introduce i controlli dello stato del server che consentono di stabilire se lo stato del server è sicuro prima dell'aggiornamento.

I controlli dello stato del server vengono eseguiti per default con ogni upgrade e si verificano prima dell'effettivo upgrade del pacchetto. Tuttavia, è anche possibile eseguire lo strumento di diagnostica *ndscheck* per eseguire i controlli dello stato.

3.6.1 Necessità dei controlli dello stato

Nelle precedenti versioni di eDirectory, durante l'upgrade non veniva verificato lo stato del server prima di procedere all'operazione. Se lo stato era instabile, l'operazione di upgrade aveva esito negativo e lo stato di eDirectory non era coerente. In alcuni casi, probabilmente, non era possibile ripristinare le impostazioni precedenti all'upgrade.

Questo nuovo strumento di controllo dello stato risolve il problema, consentendo di garantire che il server sia pronto per l'upgrade.

3.6.2 Cos'è che garantisce la stabilità dello stato di un server?

L'utility di controllo dello stato del server esegue [controlli di stato](#) specifici per garantire la stabilità dell'albero. Lo stato dell'albero viene dichiarato stabile quando tutti questi controlli di stato hanno esito positivo.

3.6.3 Esecuzione dei controlli dello stato

È possibile eseguire i controlli di stato in due modi:

- ♦ [“Esecuzione dei controlli di stato con l'upgrade” a pagina 24](#)
- ♦ [“Esecuzione dei controlli di stato come utility autonoma” a pagina 25](#)

Nota: per eseguire l'utility di controllo dello stato, è necessario disporre di diritti amministrativi. Il diritto minimo che è possibile impostare per eseguire l'utility è Public. Tuttavia, con il diritto Public alcuni degli oggetti NCP (NetWare Core Protocol) e delle informazioni sulle partizioni non sono disponibili.

Esecuzione dei controlli di stato con l'upgrade

I controlli dello stato vengono eseguiti per default ogni volta che si esegue l'upgrade di eDirectory.

Il test su Linux

Ogni volta che si esegue l'aggiornamento, i controlli dello stato vengono eseguiti per default prima che venga avviata l'operazione di upgrade effettiva.

Per ignorare i controlli dello stato di default, è possibile utilizzare l'opzione -j con l'utility nds-install.

Windows

I controlli dello stato del server vengono eseguiti come parte dell'installazione guidata. È possibile abilitare o disabilitare i controlli di stato quando viene richiesto.

Esecuzione dei controlli di stato come utility autonoma

È possibile eseguire i controlli dello stato come utility autonoma in qualsiasi momento lo si desidera. Nella tabella seguente vengono illustrate le utility di controllo dello stato.

Tabella 3-1 Utility di controllo dello stato

Piattaforma	Nome utility
Il test su Linux	ndscheck Sintassi: <code>ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path</code> Nota: è possibile specificare -h o --config-file, ma non entrambe le opzioni.
Windows	ndscheck

3.6.4 Tipi di controlli dello stato

Quando si esegue l'upgrade o si esegue l'utility ndscheck, vengono eseguiti i seguenti tipi di controllo dello stato:

- ♦ [Stato di base del server](#)
- ♦ [Stato delle partizioni e della replica](#)

Se si esegue l'utility ndscheck, i risultati dei controlli dello stato vengono visualizzati sulla schermata e registrati in `ndscheck.log`. Per ulteriori informazioni sui file di log, fare riferimento a [Sezione 3.6.6, "File di log"](#), a pagina 27.

Se i controlli dello stato vengono eseguiti come parte dell'upgrade, dopo tali controlli, in base alla criticità dell'errore viene richiesto di continuare il processo di upgrade oppure il processo viene interrotto. I dettagli degli errori vengono descritti in [Sezione 3.6.5, "Categorizzazione dello stato"](#), a pagina 26.

Stato di base del server

Si tratta della prima fase del controllo dello stato. L'utility di controllo dello stato controlla quanto segue:

1. Che il servizio eDirectory sia attivo. Che DIB sia aperto e in grado di leggere alcune informazioni di base dell'albero, ad esempio il nome dell'albero.
2. Che il server sia in ascolto sui rispettivi numeri di porta.

Per LDAP, l'utility ottiene i numeri di porta TCP ed SSL e verifica se il server è in ascolto su queste porte.

Allo stesso modo, ottiene i numeri di porta sicuri HTTP e HTTPS e verifica se il server è in ascolto su queste porte.

Stato delle partizioni e della replica

Dopo aver controllato lo stato di base del server, il passaggio successivo consiste nel controllare lo stato delle partizioni e della replica nel modo descritto di seguito:

1. Controlla lo stato delle repliche delle partizioni mantenute localmente.
2. Legge l'anello di replica di ogni singola partizione conservata dal server e controlla che tutti i server dell'anello di replica siano attivi e che tutte le repliche siano sullo stato ON.
3. Controlla la sincronizzazione oraria di tutti i server dell'anello di replica. In tal modo viene mostrata la differenza tra i server.

3.6.5 Categorizzazione dello stato

Sulla base degli errori rilevati durante il controllo dello stato di un server, è possibile individuare tre categorie di stato. Lo stato dei controlli dello stato viene registrato in un file di log. Per ulteriori informazioni, fare riferimento alla [Sezione 3.6.6, "File di log", a pagina 27](#).

Le tre categorie di stato sono [Normale](#), [Avviso](#) e [Critico](#).

Normale

Lo stato del server è normale quando tutti i controlli dello stato vengono completati correttamente.

L'upgrade procede senza interruzione.

Avviso

Lo stato del server rientra nella categoria di avviso se durante il controllo dello stato vengono rilevati errori minori.

Se il controllo dello stato viene eseguito come parte dell'upgrade, viene richiesto se si desidera interrompere o continuare.

Gli avvisi in genere si verificano nei seguenti scenari:

1. Il server non è in ascolto sulle porte LDAP e HTTPS, siano esse normali o sicure.
2. È impossibile contattare uno qualsiasi dei server non master dell'anello di replica.
3. I server nell'anello di replica non sono sincronizzati.

Critico

Lo stato del server è critico se durante il controllo dello stato vengono rilevati errori critici.

Se il controllo dello stato viene eseguito come parte dell'upgrade, l'operazione di upgrade viene interrotta.

Lo stato critico normalmente si verifica nei seguenti casi:

1. È impossibile leggere o aprire il DIB. Il DIB potrebbe essere bloccato o danneggiato.
2. È impossibile contattare tutti i server nell'anello di replica.
3. Le partizioni mantenute localmente sono occupate.
4. La replica non è nello stato ON.

3.6.6 File di log

Lo stato di ogni operazione di controllo dello stato del server, che sia eseguita con l'upgrade o come utility autonoma, viene mantenuto in un file di log.

Il contenuto del file di log è simile ai messaggi visualizzati sulla schermata quando si verificano i controlli.

Il file di log del controllo dello stato contiene le seguenti informazioni:

- ♦ Stato dei controlli dello stato (normale, avviso o critico).
- ♦ URL del sito di supporto NetIQ.

Nella seguente tabella vengono fornite le ubicazioni del file di log sulle varie piattaforme:

Tabella 3-2 Ubicazioni dei file di log del controllo dello stato

Piattaforma	Nome del file di log	Ubicazione del file di log
Il test su Linux	<code>ndscheck.log</code>	Dipende dall'ubicazione specificata con l'utility <code>ndscheck -F</code> . Se non è stata utilizzata l'opzione <code>-F</code> , l'ubicazione del file <code>ndscheck.log</code> è determinata da altre opzioni utilizzate alla riga di comando <code>ndscheck</code> , come indicato di seguito: <ol style="list-style-type: none">1. Se è stata utilizzata l'opzione <code>-h</code>, il file <code>ndscheck.log</code> viene salvato nella home directory dell'utente.2. Se è stata utilizzata l'opzione <code>--config-file</code>, il file <code>ndscheck.log</code> viene salvato nella directory del log dell'istanza del server. È inoltre possibile selezionare un'istanza dall'elenco delle istanze multiple.
Windows	<code>ndscheck.log</code>	<code>install_directory</code>

3.7 Integrazione di SecretStore con eDirectory

In eDirectory 8.8 viene fornita un'opzione per configurare Novell SecretStore 3.4 durante la configurazione di eDirectory. Nelle versioni precedenti di eDirectory 8.8, SecretStore deve essere installato manualmente.

SecretStore è una soluzione di gestione delle password semplice e sicura. che consente di utilizzare un'autenticazione singola a eDirectory per accedere alla maggior parte delle applicazioni Linux, Windows, Web e mainframe.

Dopo aver eseguito l'autenticazione a eDirectory, le applicazioni abilitate a SecretStore memorizzano e recuperano le credenziali di login appropriate. Quando si utilizza SecretStore, si elimina la necessità di ricordare o sincronizzare tutte le password necessarie per accedere alle applicazioni, ai siti Web e ai mainframe protetti da password.

Per configurare SecretStore 3.4 insieme a eDirectory, è possibile effettuare le seguenti operazioni:

- ◆ **Linux:**

Utilizzare il parametro `ndsconfig add -m ss`. All'interno del parametro, `ss` indica SecretStore ed è un parametro facoltativo. Se non viene indicato il nome del modulo, vengono installati tutti i moduli. Se non si desidera configurare SecretStore, è possibile passare il valore `no_ss` a questa opzione specificando `-m no_ss`.

- ◆ **Windows:**

Quando si installa eDirectory, è presente un'opzione per specificare se configurare il modulo SecretStore. Per default, questa opzione è selezionata.

Per ulteriori informazioni sull'utilizzo di SecretStore, fare riferimento a [Novell SecretStore 3.4 Administration Guide \(https://www.netiq.com/documentation/secretstore34/\)](https://www.netiq.com/documentation/secretstore34/) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

3.8 Installazione di eDirectory Instrumentation

La strumentazione precedente di eDirectory era parte di Novell Audit. A partire dalla versione eDirectory 8.8 SP3, eDirectory Instrumentation deve essere installato separatamente.

Per informazioni dettagliate sull'installazione, la configurazione e la disinstallazione di eDirectory Instrumentation, fare riferimento alla sezione eDirectory Instrumentation di [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guida all'installazione di NetIQ eDirectory 8.8 SP8).

3.9 Ulteriori informazioni

Per ulteriori informazioni su una qualsiasi delle funzioni discusse in questo capitolo fare riferimento ai documenti indicati di seguito:

- ◆ [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guida all'installazione di NetIQ eDirectory 8.8 SP8)
- ◆ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8)
- ◆ In Linux: `nds-install`, `ndsconfig` e documentazione `man ndscheck`

4 Backup e ripristino di NCI

Novell International Cryptography Infrastructure (NICI) memorizza le chiavi e i dati utente nel file system e nel sistema, nonché nelle directory e nei file specifici dell'utente. Tali directory e file sono protetti tramite l'impostazione delle autorizzazioni appropriate grazie al meccanismo fornito dal sistema operativo. Tale operazione viene eseguita dal programma di installazione NCI.

Se si disinstalla NCI dal sistema, il sistema o le directory e i file utente non vengono rimossi. Pertanto, l'unica ragione per ripristinare lo stato precedente di questi file è quella di recuperare da un guasto grave del sistema o da un errore umano. È importante comprendere che sovrascrivendo una serie di directory e file utente NCI esistenti si può danneggiare un'applicazione esistente.

La chiave di database richiesta per aprire DIB è incorporata con le chiavi NCI. Di conseguenza, se si esegue un backup di eDirectory indipendente da un backup NCI tale chiave non è utilizzabile.

Modifiche al meccanismo di backup e ripristino NCI precedente

Nelle versioni precedenti, il backup e il ripristino di NCI dovevano essere eseguiti manualmente. In questa versione, è stata aggiunta una nuova soluzione di backup e ripristino NCI. Alla soluzione di backup di eDirectory è stato aggiunto uno switch (-e) (backup eMBox e DSBK) che consente le seguenti operazioni:

1. Backup delle chiavi NCI quando viene eseguito un backup di eDirectory
2. Ripristino delle chiavi NCI quando viene eseguito un ripristino di eDirectory

Fare riferimento a [“Backing Up and Restoring NCI”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

5 Utility ndspassstore

ndspassstore è una nuova utility utilizzata per memorizzare la password cifrata per l'utente sadmin o l'utente eDirectory. L'utility è disponibile sulle piattaforme Linux e Windows. L'utility memorizza il nome utente e la password come coppie chiave-valore cifrate.

In questa versione, questa utility viene impiegata per impostare la password sadmin.

L'utility è disponibile per default in C:\Novell\NDS in Windows e in /opt/novell/eDirectory/bin in Linux.

Riepilogo dei comandi

È possibile adoperare l'utility ndspassstore immettendo il seguente comando alla console del server:

```
ndspassstore -a <adminContext> -w <password>
```

Opzione	Utilizzo
-a adminContext	Questa opzione viene utilizzata per accettare adminContext, vale a dire il nome FDN (Fully Distinguished Name) di un utente che dispone di diritti amministrativi.
-w parola_d'ordine	Questa opzione viene utilizzata per accettare la password (password utente) per l'autenticazione.

6 Istanze multiple

Di norma, è possibile configurare una sola istanza di NetIQ eDirectory su un singolo host. Grazie al supporto della funzione per le istanze multiple in eDirectory 8.8, sono possibili le seguenti configurazioni:

- ♦ Istanze multiple di eDirectory su un singolo host
- ♦ Alberi multipli su un singolo host
- ♦ Repliche multiple dello stesso albero o della stessa partizione su un singolo host

eDirectory 8.8 fornisce, inoltre, un'utility ([ndsmanage](#)) per tenere traccia delle istanze in modo semplice.

Nella tabella seguente sono elencate le piattaforme che supportano più istanze:

Funzione	Linux	Windows
Supporto di istanze multiple	✓	✗

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 6.2, "Scenari di esempio per l'installazione di istanze multiple"](#), a pagina 33
- ♦ [Sezione 6.3, "Utilizzo di istanze multiple"](#), a pagina 34
- ♦ [Sezione 6.4, "Gestione di istanze multiple"](#), a pagina 35
- ♦ [Sezione 6.5, "Scenario di esempio per più istanze"](#), a pagina 39
- ♦ [Sezione 6.6, "Ulteriori informazioni"](#), a pagina 40

6.1 Esigenza di istanze multiple

La presenza di istanze multiple nasce dalle seguenti esigenze:

- ♦ Sfruttare l'hardware avanzato configurando più istanze di eDirectory.
- ♦ Utilizzare una configurazione pilota su un singolo host prima di investire nell'hardware richiesto.

6.2 Scenari di esempio per l'installazione di istanze multiple

Le istanze multiple che appartengono allo stesso albero oppure a più alberi possono essere utilizzate in modo efficace nei seguenti scenari.

eDirectory in un'azienda di grandi dimensioni

- ◆ Nelle aziende di grandi dimensioni, è possibile fornire bilanciamento del carico e alta disponibilità dei servizi eDirectory.

Se, ad esempio, si dispone di tre server di replica sui quali sono in esecuzione i servizi LDAP sulle porte 1524, 2524 e 3524, rispettivamente, è possibile configurare una nuova istanza di eDirectory e fornire un servizio LDAP ad alta disponibilità su una nuova porta 636.

- ◆ È possibile sfruttare l'hardware avanzato tra i diversi reparti di un'organizzazione configurando più istanze su un singolo host.

eDirectory in una configurazione di valutazione

- ◆ **Università:** Molti entusiasti (studenti) possono valutare eDirectory dallo stesso host utilizzando le istanze multiple.
- ◆ **Formazione per l'amministrazione di eDirectory:**
 - ◆ I partecipanti possono provare la gestione utilizzando le istanze multiple.
 - ◆ Gli istruttori possono utilizzare un singolo host per l'insegnamento a una classe di allievi. Ciascun allievo può disporre di un albero proprio.

6.3 Utilizzo di istanze multiple

eDirectory 8.8 rende molto semplice la configurazione di istanze multiple. Per utilizzare in modo efficiente istanze multiple, è necessario pianificare la configurazione e quindi configurare le istanze multiple.

- ◆ [Sezione 6.3.1, "Pianificazione della configurazione", a pagina 34](#)
- ◆ [Sezione 6.3.2, "Configurazione di istanze multiple", a pagina 34](#)

6.3.1 Pianificazione della configurazione

Per utilizzare questa funzione in modo efficiente, è consigliabile pianificare le istanze di eDirectory e assicurarsi che ognuna disponga di ID istanza predefiniti quali il nome host, il numero di porta, il nome del server o il file di configurazione.

Quando si configurano istanze multiple, è necessario assicurarsi di aver pianificato quanto segue:

- ◆ Ubicazione del file di configurazione
- ◆ Ubicazione dei dati variabili (come i file di log)
- ◆ Ubicazione del DIB
- ◆ Interfaccia NCP™, porta di identificazione univoca per ciascuna istanza e porte degli altri servizi (come LDAP, LDAPS, HTTP e porta protetta HTTP)
- ◆ Nome server univoco per ciascuna istanza

6.3.2 Configurazione di istanze multiple

È possibile configurare istanze multiple di eDirectory mediante l'utilità ndsconfig. Nella tabella seguente sono elencate le opzioni ndsconfig che è necessario includere quando si configurano istanze multiple.

Nota: tutte le istanze condividono la stessa chiave server (NICI).

Opzione	Descrizione
--config-file	Indica il percorso assoluto e il nome file per memorizzare il file di configurazione <code>nds.conf</code> . Ad esempio, per memorizzare il file di configurazione nella directory <code>/etc/opt/novell/eDirectory/</code> , utilizzare <code>--config-file /etc/opt/novell/eDirectory/nds.conf</code> .
-b	Indica il numero di porta sul quale deve essere in ascolto la nuova istanza. Nota: <code>-b</code> e <code>-B</code> sono utilizzate in modo esclusivo.
-B	Indica il numero di porta insieme all'indirizzo IP o all'interfaccia. Ad esempio: <code>-B eth0@524</code> oppure <code>-B 100.1.1.2@524</code> Nota: <code>-b</code> e <code>-B</code> sono utilizzate in modo esclusivo.
-D	Crea le directory <code>data</code> , <code>dib</code> e <code>log</code> nel percorso specificato per la nuova istanza.
S	Indica il nome del server.

Utilizzando le opzioni indicate in precedenza, è possibile configurare una nuova istanza di eDirectory.

È inoltre possibile configurare una nuova istanza mediante l'utility `ndsmanage`. Per ulteriori informazioni, fare riferimento alla [“Creazione di un'istanza tramite ndsmanage”](#) a pagina 36.

6.4 Gestione di istanze multiple

In questa sezione vengono fornite le seguenti informazioni:

- ♦ [Sezione 6.4.1, “Utility ndsmanage”, a pagina 35](#)
- ♦ [Sezione 6.4.2, “Identificazione di un'istanza specifica”, a pagina 38](#)
- ♦ [Sezione 6.4.3, “Chiamata di un'utility per un'istanza specifica”, a pagina 39](#)

6.4.1 Utility ndsmanage

L'utility `ndsmanage` consente di effettuare le seguenti operazioni:

- ♦ [Elencare le istanze configurate](#)
- ♦ [Creare una nuova istanza](#)
- ♦ [Effettuare le operazioni seguenti per un'istanza selezionata:](#)
 - ♦ [Elencare le repliche sul server](#)
 - ♦ [Avviare l'istanza](#)
 - ♦ [Interrompere l'istanza](#)

- ◆ Eseguire DSTrace (ndstrace) per l'istanza
- ◆ Annullare la configurazione di un'istanza
- ◆ [Avviare e interrompere tutte le istanze](#)

Elenco delle istanze

Nella seguente tabella viene descritto come elencare le istanze di eDirectory.

Tabella 6-1 Uso di ndsmanage per l'elenco delle istanze

Sintassi	Descrizione
ndsmanage	Elenca tutte le istanze configurate dall'utente.
ndsmanage -a --all	Elenca le istanze di tutti gli utenti che utilizzano una particolare installazione di eDirectory.
ndsmanage <i>nome utente</i>	Elenca le istanze configurate da uno specifico utente

Per ogni istanza vengono visualizzati i seguenti campi:

- ◆ Percorso del file di configurazione
- ◆ FDN e porta del server
- ◆ Stato (se l'istanza è attiva o inattiva)

Nota: questa utility elenca tutte le istanze configurate per un singolo file binario.

Per ulteriori informazioni consultare [Figura 6-1 a pagina 36](#).

Creazione di un'istanza tramite ndsmanage

Per creare una nuova istanza tramite ndsmanage, effettuare le seguenti operazioni:

- 1 Immettere il seguente comando:

```
ndsmanage
```

Se sono configurate due istanze, viene visualizzata la seguente schermata:

Figura 6-1 Schermata di output dell'utility ndsmanage

```
root@MYSOL-8 / $ ndsmanage

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit: █
```

2 Immettere c per creare una nuova istanza.

È possibile creare un nuovo albero oppure aggiungere un server a un albero esistente. Seguire le istruzioni sulla schermata per creare una nuova istanza.

Esecuzione di operazioni per un'istanza specifica

È possibile effettuare le seguenti operazioni per ogni istanza:

- ♦ “Avvio di un'istanza specifica” a pagina 37
- ♦ “Interruzione di un'istanza specifica” a pagina 37
- ♦ “Annullamento della configurazione di un'istanza” a pagina 38

Oltre che per le istanze elencate in precedenza, è anche possibile eseguire DTrace per un'istanza selezionata.

Avvio di un'istanza specifica

Per avviare un'istanza configurata dall'utente, effettuare le seguenti operazioni:

1 Immettere quanto segue:

```
ndsmanage
```

2 Selezionare l'istanza che si desidera avviare.

Il menu si espande fino a includere le opzioni che è possibile eseguire su una specifica istanza.

Figura 6-2 Schermata di output dell'utility `ndsmanage` con le opzioni dell'istanza

```
root@mysol-8 / $ ndsmanage root

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit: 1
[1] List the replicas on the server
[s] Start the instance
[k] Stop the instance
[t] Run ndstrace
[d] Deconfigure
[q] Quit
What do you want to do with this instance? [ Choose from above]: █
```

3 Immettere s per avviare l'istanza.

In alternativa, è anche possibile immettere quanto segue al prompt dei comandi:

```
ndsmanage start --config-file configuration_file_of_the_instance_configured_by_you
```

Interruzione di un'istanza specifica

Per interrompere un'istanza configurata dall'utente, effettuare le seguenti operazioni:

1 Immettere quanto segue:

```
ndsmanage
```

- 2 Selezionare l'istanza che si desidera interrompere.

Il menu si espande fino a includere le opzioni che è possibile eseguire su una specifica istanza. Per ulteriori informazioni, fare riferimento alla [Schermata di output dell'utility ndsmanage con le opzioni dell'istanza \(pagina 37\)](#).

- 3 Immettere k per interrompere l'istanza.

In alternativa, è anche possibile immettere quanto segue al prompt dei comandi:

```
ndsmanage stop --config-file configuration_file_of_the_instance_configured_by_you
```

Annullamento della configurazione di un'istanza

Per annullare la configurazione di un'istanza, effettuare le seguenti operazioni:

- 1 Immettere quanto segue:

```
ndsmanage
```

- 2 Selezionare l'istanza di cui si desidera annullare la configurazione.

Il menu si espande fino a includere le opzioni che è possibile eseguire su una specifica istanza. Per ulteriori informazioni, fare riferimento alla [Schermata di output dell'utility ndsmanage con le opzioni dell'istanza \(pagina 37\)](#).

- 3 Immettere d per annullare la configurazione dell'istanza.

Avvio e interruzione di tutte le istanze

È possibile avviare e interrompere tutte le istanze configurate dall'utente.

Avvio di tutte le istanze

Per avviare tutte le istanze configurate dall'utente, immettere quanto segue al prompt dei comandi:

```
ndsmanage startall
```

Per avviare un'istanza specifica, fare riferimento a [“Avvio di un'istanza specifica” a pagina 37](#).

Interruzione di tutte le istanze

Per interrompere tutte le istanze configurate dall'utente, immettere quanto segue al prompt dei comandi:

```
ndsmanage stopall
```

Per interrompere un'istanza specifica, fare riferimento a [“Interruzione di un'istanza specifica” a pagina 37](#).

6.4.2 Identificazione di un'istanza specifica

Quando si configurano più istanze, a ciascuna istanza vengono assegnati un nome host, un numero di porta e un percorso file di configurazione univoco. Il nome host e il numero di porta sono ID dell'istanza.

La maggior parte delle utility dispone dell'opzione `-h hostname:port o --config-file configuration_file_location` che consente di specificare un'istanza specifica. Vedere la documentazione man delle utility per ulteriori informazioni.

6.4.3 Chiamata di un'utility per un'istanza specifica

Se desideri eseguire un'utility per un'istanza specifica, è necessario includere l'ID istanza nel comando dell'utility. Gli ID istanza sono il percorso del file di configurazione e il nome host e il numero di porta. A tal fine è possibile utilizzare `--config-file configuration_file_location -h hostname:port`.

Se non si includono gli ID istanza nel comando, all'interno dell'utility vengono visualizzate le diverse istanze di cui si è proprietari e viene richiesto di selezionare l'istanza per cui eseguire l'utility.

Ad esempio, per eseguire DTrace per un'istanza specifica che utilizza l'opzione `--config-file`, si dovrà immettere:

```
ndstrace --config-file configuration_filename_with_location
```

6.5 Scenario di esempio per più istanze

Maria è un utente nonroot che desidera configurare due alberi su un unico computer host per un singolo file binario.

6.5.1 Pianificazione della configurazione

Maria specifica i seguenti ID istanza.

- ◆ **Istanza 1:**

Numero di porta sul quale l'istanza deve essere in ascolto	1524
Percorso del file di configurazione	/home/maryinst1/nds.conf
Directory DIB	/home/mary/inst1/var

- ◆ **Istanza 2:**

Numero di porta sul quale l'istanza deve essere in ascolto	2524
Percorso del file di configurazione	/home/mary/inst2/nds.conf
Directory DIB	/home/mary/inst2/var

6.5.2 Configurazione delle istanze

Per configurare le istanze in base agli ID istanza predefiniti citati, Maria dovrà immettere i seguenti comandi.

- ◆ **Istanza 1:**

```
ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D /home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

- ◆ **Istanza 2:**

```
ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D /home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
```

6.5.3 Richiamo di un'utility per un'istanza

Se Maria decide di eseguire l'utility per l'istanza 1 DTrace che è in ascolto sulla porta 1524, con il relativo file di configurazione nell'ubicazione `/home/mary/inst1/nds.conf` e il relativo file DIB ubicato in `/home/mary/inst1/var`, può eseguire l'utility nel modo indicato di seguito:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

oppure

```
ndstrace -h 164.99.146.109:1524
```

Se Maria non specifica gli ID istanza, nell'utility vengono visualizzate tutte le istanze di proprietà di Maria e le viene richiesto di selezionarne una.

6.5.4 Elenco delle istanze

Se Maria desidera conoscere i dettagli delle istanze nell'host, può eseguire l'utility `ndsmanage`.

- ◆ Per visualizzare tutte le istanze di proprietà di Maria:

```
ndsmanage
```

- ◆ Per visualizzare tutte le istanze di proprietà di Giovanni (il nome utente è john):

```
ndsmanage john
```

- ◆ Per visualizzare tutte le istanze di tutti gli utenti che stanno utilizzando un'istanza particolare di eDirectory:

```
ndsmanage -a
```

6.6 Ulteriori informazioni

Per ulteriori informazioni sul supporto di istanza multiple, fare riferimento ai seguenti documenti:

- ◆ [NetIQ eDirectory 8.8 SP8 Installation Guide](#) (Guida all'installazione di NetIQ eDirectory 8.8 SP8)
- ◆ Per Linux: documentazione man di `ndsconfig` e `ndsmanage`

7 Autenticazione a eDirectory tramite SASL-GSSAPI

Il meccanismo SASL-GSSAPI per NetIQ eDirectory 8.8 consente di eseguire l'autenticazione a eDirectory tramite LDAP tramite una richiesta Kerberos e senza la necessità di immettere la password utente di eDirectory. La richiesta Kerberos deve essere ottenuta effettuando l'autenticazione a un server Kerberos.

Tale funzione è utile principalmente per gli utenti di applicazioni LDAP in un ambiente che dispone già di un'infrastruttura Kerberos installata. Pertanto, tali utenti devono essere in grado di effettuare l'autenticazione al server LDAP senza fornire un'altra password utente LDAP.

Per semplificare l'operazione, eDirectory introduce il meccanismo SASL-GSSAPI.

L'implementazione corrente di SASL-GSSAPI è compatibile con [RFC 2222](http://www.ietf.org/rfc/rfc2222.txt?number=2222) (<http://www.ietf.org/rfc/rfc2222.txt?number=2222>) e supporta solo Kerberos v5 come meccanismo di autenticazione.

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 7.1, "Concetti", a pagina 41](#)
- ♦ [Sezione 7.2, "Come funziona GSSAPI con eDirectory?", a pagina 42](#)
- ♦ [Sezione 7.3, "Configurazione di GSSAPI", a pagina 43](#)
- ♦ [Sezione 7.4, "In che modo LDAP utilizza GSSAPI?", a pagina 44](#)
- ♦ [Sezione 7.5, "Termini utilizzati comunemente", a pagina 44](#)

7.1 Concetti

- ♦ [Sezione 7.1.1, "Cos'è Kerberos?", a pagina 41](#)
- ♦ [Sezione 7.1.2, "Cos'è SASL?", a pagina 42](#)
- ♦ [Sezione 7.1.3, "Cos'è GSSAPI?", a pagina 42](#)

7.1.1 Cos'è Kerberos?

Kerberos è un protocollo standard che fornisce gli strumenti per autenticare le entità in una rete. È basato su un modello attendibile di terze parti. Il protocollo implica segreti condivisi e utilizza la cifratura a chiave simmetrica.

Per ulteriori informazioni, fare riferimento a [RFC 1510](http://www.ietf.org/rfc/rfc1510.txt?number=1510) (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>).

7.1.2 Cos'è SASL?

SASL (Simple Authentication and Security Layer) fornisce alle applicazioni un livello di astrazione di autenticazione. Si tratta di un framework al quale è possibile collegare i moduli di autenticazione.

Per ulteriori informazioni, fare riferimento a [RFC 2222 \(http://www.ietf.org/rfc/rfc2222.txt?number=2222\)](http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.1.3 Cos'è GSSAPI?

GSSAPI (Generic Security Services Application Program Interface) fornisce l'autenticazione e altri servizi tramite una serie di API standard. L'interfaccia supporta vari meccanismi di autenticazione. Kerberos v5 è il più comune.

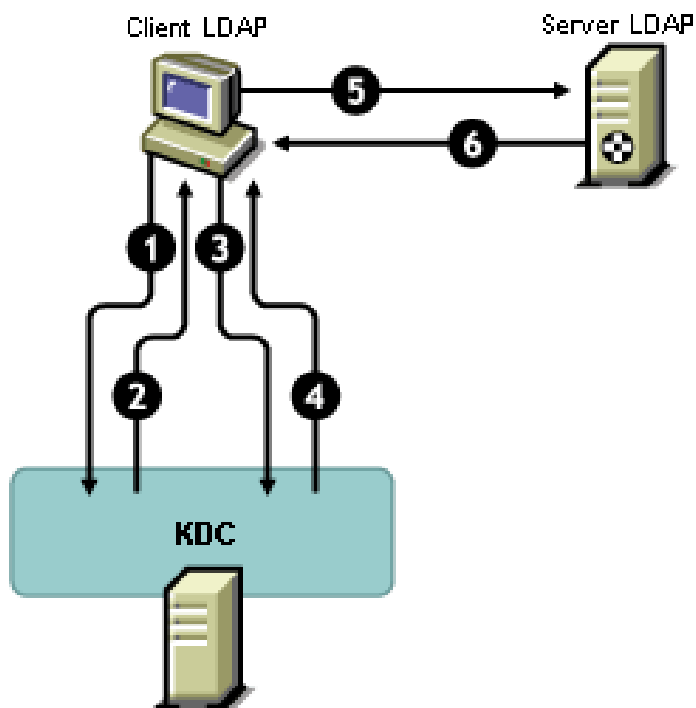
Per informazioni sulle API GSS, fare riferimento a [RFC 1964 \(http://www.ietf.org/rfc/rfc1964.txt?number=1964\)](http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Questa implementazione di SASL-GSSAPI viene dalla sezione 7.2 di [RFC 2222 \(http://www.ietf.org/rfc/rfc2222.txt?number=2222\)](http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.2 Come funziona GSSAPI con eDirectory?

Nello schema seguente viene illustrato in che modo GSSAPI funziona con un server LDAP.

Figura 7-1 Come funziona GSSAPI?



Di seguito è illustrato il significato dei numeri della figura precedente:

- 1 Un utente eDirectory invia una richiesta tramite un client LDAP al server Kerberos KDC (Key Distribution Center) per una richiesta iniziale nota come TGT (ticket granting ticket).

Un KDC Kerberos può avere come origine MIT o Microsoft*.

- 2 KDC risponde al client LDAP con una richiesta TGT.
- 3 Il client LDAP invia la richiesta TGT nuovamente al servizio KDC ed effettua una richiesta di servizio LDAP.
- 4 KDC risponde al client LDAP con la richiesta di servizio LDAP.
- 5 Il client LDAP esegue una richiesta `ldap_sasl_bind` al server LDAP e invia la richiesta di servizio LDAP.
- 6 Il server LDAP convalida la richiesta di servizio LDAP con l'aiuto del meccanismo GSSAPI e, in base al risultato, reinvia un messaggio `ldap_sasl_bind` di riuscita o di mancata riuscita al client LDAP.

7.3 Configurazione di GSSAPI

- 1 Il plug-in iManager per SASL-GSSAPI non funziona se iManager non è configurato per l'uso della connessione SSL/TLS a eDirectory. È necessaria una connessione sicura per proteggere la chiave master del dominio e le chiavi principali.

Per default, iManager in genere viene configurata per la connessione SSL/TLS a eDirectory. Se si desidera configurare il metodo di login Kerberos per GSSAPI su un albero diverso da quello che funziona da host per la configurazione iManager, è necessario configurare iManager per la connessione SSL/TLS a eDirectory.

Per informazioni sulla configurazione di iManager con la connessione SSL/TLS a eDirectory, fare riferimento alla *NetIQ iManager 2.7 Administration Guide* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guida all'amministrazione di NetIQ iManager 2.7).

Il plug-in iManager per SASL-GSSAPI (`kerberosPlugin.npm`) è disponibile come parte dei file `eDir_88_iMan26_Plugins.npm` e `eDir_88_iMan27_Plugins.npm`. Scaricare le NPM dal [sito Web di download di Novell](http://download.novell.com) (<http://download.novell.com>).

- 2 Per utilizzare un ticket Kerberos per eseguire l'autenticazione a un server eDirectory, effettuare le seguenti operazioni:
 - 2a Estendere lo schema Kerberos.
 - 2b Creare un container Realm.
 - 2c Estrarre una chiave di servizio principale o una chiave condivisa da KDC.
 - 2d Creare l'oggetto LDAP Service Principal.
 - 2e Associare un nome principale Kerberos all'oggetto Utente.

Per informazioni sui passaggi precedenti, fare riferimento alla "Configuring GSSAPI with eDirectory" in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

7.4 In che modo LDAP utilizza GSSAPI?

Dopo aver configurato GSSAPI, questo viene aggiunto, insieme ad altri metodi SASL, all'attributo `supportedSASLMechanisms` in `rootDSE.rootDSE` (DSA [Directory System Agent] Specific Entry) è una voce ubicata nella radice dell'albero DIT (Directory Information Tree). Per ulteriori informazioni, fare riferimento a [“Understanding How LDAP Works with eDirectory”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

Il server LDAP interroga SASL per i meccanismi installati quando riceve la configurazione e supporta in modo automatico tutto ciò che è installato. Il server LDAP inoltre segnala i meccanismi SASL correnti supportati in `rootDSE` mediante l'attributo `supportedSASLMechanisms`.

Pertanto, quando si configura GSSAPI, questo diventa il meccanismo di default. Tuttavia, per eseguire un'operazione LDAP in modo specifico su un meccanismo SASL GSSAPI, è possibile menzionare GSSAPI alla riga di comando.

Ad esempio, per eseguire una ricerca in OpenLDAP tramite il meccanismo GSSAPI, si immetterà quanto segue:

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 Termini utilizzati comunemente

Nella tabella seguente viene definita la terminologia utilizzata comunemente con Kerberos e GSSAPI.

Tabella 7-1 Terminologia Kerberos/GSSAPI

Termine	definizione
KDC (Key Distribution Center)	Server Kerberos che autentica gli utenti ed emette richieste.
Entità principal	Entità (utente o istanza di servizio) registrata con KDC.
Dominio	Dominio o raggruppamento di entità principal serviti da una serie di KDC.
ST (Ticket di servizio)	Record contenente informazioni client, informazioni di servizio e una chiave di sessione che è cifrata con la chiave condivisa del principal dello specifico servizio
TGT (Ticket Granting Ticket)	Tipo di richiesta con il quale il cliente può ottenere altre richieste Kerberos.

8 Applicazione di password universali che rilevano la distinzione tra maiuscole e minuscole

In NetIQ eDirectory 8.8, è possibile abilitare Universal Password e fare in modo che la password rilevi la distinzione tra maiuscole e minuscole quando si accede al server eDirectory 8.8 tramite i seguenti client e utility:

- ♦ Novell Client 4.9 e versioni successive
- ♦ Utility di amministrazione di cui è stato eseguito l'upgrade a eDirectory 8.8
- ♦ NetIQ iManager 2.7 e versioni successive, tranne se in esecuzione su Windows

È possibile utilizzare qualsiasi versione di LDAP SDK per disporre di password in grado di rilevare la differenza tra maiuscole e minuscole.

Nella tabella seguente sono elencate le piattaforme su cui è supportata la funzionalità password in grado di rilevare la differenza tra maiuscole e minuscole:

Funzione	Linux	Windows
Applicazione di Universal Password con distinzione tra maiuscole e minuscole	✓	✓

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 8.1, "Esigenza di password in grado di rilevare la distinzione tra maiuscole e minuscole", a pagina 46](#)
- ♦ [Sezione 8.2, "Come far sì che la password rilevi la distinzione tra maiuscole e minuscole", a pagina 46](#)
- ♦ [Sezione 8.3, "Aggiornamento dei client Novell e delle utility esistenti", a pagina 47](#)
- ♦ [Sezione 8.4, "Esclusione dei client Novell esistenti dall'accesso al server eDirectory 8.8", a pagina 49](#)
- ♦ [Sezione 8.5, "Ulteriori informazioni", a pagina 54](#)

8.1 Esigenza di password in grado di rilevare la distinzione tra maiuscole e minuscole

La possibilità di distinguere tra maiuscole e minuscole, aumenta la sicurezza del login alla directory. Se, ad esempio, si utilizza una password aBc in grado di rilevare la differenza tra maiuscole e minuscole, tutti i tentativi di login con combinazioni del tipo abc o Abc oppure ABC avranno esito negativo.

In eDirectory 8.8 e versioni successive, è possibile fare in modo che le password rilevino la distinzione tra maiuscole e minuscole per tutti i client per i quali è stato eseguito l'upgrade a eDirectory 8.8.

Applicando l'uso di password in grado di rilevare la distinzione tra maiuscole e minuscole, è possibile impedire che i client Novell precedenti accedano al server eDirectory 8.8. Per ulteriori informazioni consultare [Sezione 8.4, "Esclusione dei client Novell esistenti dall'accesso al server eDirectory 8.8"](#), a pagina 49.

8.2 Come far sì che la password rilevi la distinzione tra maiuscole e minuscole

In eDirectory 8.8 e versioni successive, è possibile fare in modo che le password rilevino la distinzione tra maiuscole e minuscole per tutti i client abilitando Universal Password. Il servizio Universal Password è disabilitato per default.

8.2.1 Prerequisiti

Per default, le utility LDAP e altre utility sul lato server utilizzano in primo luogo il login NDS e se si verificano problemi, utilizzano il login Password semplice. Per consentire il funzionamento della funzione, il login deve essere eseguito tramite il servizio NMAS (Novell Modular Authentication Service). Pertanto, è necessario impostare la variabile di ambiente `NDS_TRY_NMASLOGIN_FIRST` su `true` per rendere disponibile la funzione.

Per rendere disponibile la funzione di rilevamento delle distinzioni tra maiuscole e minuscole, completare la procedura seguente:

1 Impostare la variabile di ambiente

- ◆ Linux:

Aggiungere quanto segue alla fine di `/opt/novell/eDirectory/sbin/pre_ndsd_start` .

```
NDS_TRY_NMASLOGIN_FIRST=true
export NDS_TRY_NMASLOGIN_FIRST
```

- ◆ Windows:

Fare clic con il pulsante destro del mouse su Computer e selezionare Proprietà. Nella scheda Avanzate, fare clic su Variabili d'ambiente. In Variabili d'ambiente, aggiungere la variabile e impostare il valore su `true`.

2 Riavviare il server eDirectory.

Nota: se si utilizza NMAS per l'autenticazione, il tempo richiesto per il login aumenta.

8.2.2 Come fare in modo che la password rilevi la distinzione tra maiuscole e minuscole

- 1 Eseguire il login a eDirectory tramite la password esistente.

In caso di nuova installazione, la password esistente è quella impostata quando si configura eDirectory 8.8.

Ad esempio, la password in uso è "novell".

Nota: Questa password non rileva la distinzione tra maiuscole e minuscole.

- 2 Abilita Universal Password.

Per ulteriori informazioni, fare riferimento alla sezione ["Distribuzione di Universal Password" in Novell Password Management 3.3 Administration Guide \(http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html\)](http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guida all'amministrazione di Novell Password Management 3.3).

- 3 Eseguire il logout da eDirectory.

- 4 Eseguire il login a eDirectory utilizzando la password esistente con la maiuscola o la minuscola, a scelta.

La password fornita non rileverà la distinzione tra maiuscole e minuscole.

Ad esempio, è stato immesso "NoVELL".

La password ora è "NoVELL". Pertanto, "novell" o una qualsiasi altra combinazioni di maiuscole e minuscole diversa da "NoVELL" non sarà valida.

Se si esegue la migrazione alle password che rilevano la distinzione tra maiuscole e minuscole, fare riferimento a [Sezione 8.3.1, "Migrazione alle password in grado di rilevare la distinzione tra maiuscole e minuscole"](#), a pagina 48.

Tutte le nuove password impostate rileveranno la distinzione tra maiuscole e minuscole, a seconda del livello (oggetto oppure partizione) a cui è stato abilitato Universal Password.

8.2.3 Gestione delle password che rilevano la distinzione tra maiuscole e minuscole

È possibile gestire la sensibilità delle password abilitando o disabilitando Universal Password tramite iManager. Per ulteriori informazioni, fare riferimento alla sezione ["Deploying Universal Password" in NetIQ Password Management 3.3 Administration Guide \(http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html\)](http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guida all'amministrazione di NetIQ Password Management 3.3).

8.3 Aggiornamento dei client Novell e delle utility esistenti

Di seguito sono elencate le versioni più recenti dei client Novell e delle utility NetIQ:

- ♦ Novell Client4.9
- ♦ Utility di amministrazione con eDirectory 8.8
- ♦ NetIQ iManager 2.7 e versioni successive

I client e le utility precedenti alle versioni indicate in precedenza sono client Novell esistenti.

È possibile disporre di password che rilevano la distinzione tra maiuscole e minuscole per i client Novell esistenti dopo averli aggiornati alla versione più recente. eDirectory 8.8 semplifica e rende flessibile la migrazione dalle password esistenti a quelle in grado di rilevare la distinzione tra maiuscole e minuscole. Per ulteriori informazioni consultare [Sezione 8.3.1, “Migrazione alle password in grado di rilevare la distinzione tra maiuscole e minuscole”](#), a pagina 48.

Se non si esegue l'upgrade dei client esistenti alle versioni più recenti, è possibile che l'utilizzo di eDirectory 8.8 da parte di questi client venga bloccato a livello di server. Per ulteriori informazioni, fare riferimento a [Sezione 8.4, “Esclusione dei client Novell esistenti dall'accesso al server eDirectory 8.8”](#), a pagina 49.

8.3.1 Migrazione alle password in grado di rilevare la distinzione tra maiuscole e minuscole

Universal Password è disabilitato per default e, pertanto, le password esistenti non saranno interessate fino a quando non si abilita Universal Password in iManager. Per istruzioni passo passo, fare riferimento a [Sezione 8.2, “Come far sì che la password rilevi la distinzione tra maiuscole e minuscole”](#), a pagina 46.

Nell'esempio seguente, viene illustrata la migrazione alle password che rilevano la distinzione tra maiuscole e minuscole:

Sessione di login 1: Universal Password è disabilitato per default.

- ◆ Si esegue il login mediante la password esistente. Si supponga, ad esempio che la password sia netiq.
- ◆ Questa password non rileva la distinzione tra maiuscole e minuscole. Pertanto netiq e NetIQ sono entrambe password valide.
- ◆ Dopo il login, si abilita Universal Password. Fare riferimento alla sezione [“Deploying Universal Password” in NetIQ Password Management 3.3 Administration Guide \(\[http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html\]\(http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html\)\)](#) (Guida all'amministrazione di NetIQ Password Management 3.3).

Sessione di login 2: Universal Password era abilitata nella sessione precedente.

- ◆ Si esegue il login mediante la password esistente. Si supponga, ad esempio, di digitare la password noVell.
- ◆ Quando si abilita Universal Password, questa password rileva la distinzione tra maiuscole e minuscole. Pertanto, stavolta è opportuno ricordare come è stata digitata la password.

Sessione di login 3 e login successivi.

- ◆ Se si esegue il login con la password netIQ, la password è valida.
- ◆ Se si esegue il login con la password NetIQ (o qualsiasi altra versione eccetto noVell), la password non è valida.

8.4 Esclusione dei client Novell esistenti dall'accesso al server eDirectory 8.8

In eDirectory 8.7.1 e 8.7.3, era possibile impedire ai client Novell di [impostare o modificare](#) la password NDS. Con eDirectory 8.8, è inoltre possibile impedire a tali client di eseguire il login a eDirectory 8.8 e verificare le password.

Per consentire o impedire ai client Novell esistenti di utilizzare eDirectory 8.8, è necessario configurare il login NDS tramite iManager o LDAP.

In questa sezione vengono fornite le seguenti informazioni:

- ♦ [Sezione 8.4.1, “Esigenza di impedire ai client Novell esistenti l'accesso al server eDirectory 8.8”, a pagina 49](#)
- ♦ [Sezione 8.4.2, “Gestione delle configurazione di login NDS”, a pagina 49](#)
- ♦ [Sezione 8.4.3, “Operazioni sulla partizione”, a pagina 53](#)
- ♦ [Sezione 8.4.4, “Applicazione di password in grado di rilevare la distinzione tra maiuscole e minuscole in un albero misto”, a pagina 53](#)

8.4.1 Esigenza di impedire ai client Novell esistenti l'accesso al server eDirectory 8.8

Le password dei client Novell esistenti non rilevano la distinzione tra maiuscole e minuscole. Pertanto, in eDirectory 8.8 e versioni successive, quando si desidera applicare l'uso di password che rilevano la distinzione tra maiuscole e minuscole, potrebbe essere necessario bloccare l'accesso alla directory da parte dei client esistenti.

Nelle versioni precedenti a Novell Client 4.9, Universal Password non era supportato. La causa è che le modifiche al login alla password interessavano direttamente la password NDS invece di NMA. Ora, se si utilizza Universal Password, la modifica delle password tramite i client esistenti può creare un problema denominato “variazione della password”. Ciò significa che la password NDS e Universal Password non sono sincronizzate. Per evitare questo problema, un'opzione consiste nel bloccare le modifiche alla password dei client precedenti alla versione 4.9.

Per informazioni su come bloccare l'accesso al server eDirectory 8.8 da parte dei client esistenti, vedere [Gestione delle configurazione di login NDS](#).

8.4.2 Gestione delle configurazione di login NDS

Configurando il login NDS, è possibile abilitare o disabilitare l'accesso al server eDirectory 8.8 per i client Novell. Le configurazione di login NDS possono essere gestite tramite iManager 2.6 e LDAP.

In eDirectory 8.8 e versioni successive, è possibile configurare l'impostazione e la modifica delle password tramite LDAP e iManager.

In questa sezione sono incluse le seguenti informazioni:

- ♦ [“Configurazioni NDS a livelli diversi” a pagina 50](#)
- ♦ [“Gestione delle configurazioni NDS tramite iManager” a pagina 51](#)
- ♦ [“Gestione di configurazioni NDS tramite LDAP” a pagina 52](#)
- ♦ [Sezione 8.4.4, “Applicazione di password in grado di rilevare la distinzione tra maiuscole e minuscole in un albero misto”, a pagina 53](#)

Configurazioni NDS a livelli diversi

È possibile configurare il NDS a uno dei seguenti livelli o in tutti:

- ◆ Livello di partizione
- ◆ Livello di oggetto

Se non si specifica la configurazione a uno qualsiasi dei livelli, la configurazione del login NDS viene abilitata a tutti i livelli.

La configurazione a livello di oggetto ignora sempre la configurazione a livello di partizione. Tutto questo viene descritto nella tabella seguente:

Tabella 8-1 Configurazione NDS

Configurazione a livello di oggetto	Configurazione a livello di partizione	Configurazione
Non specificato	Abilitato	Abilitato
Abilitato	Non specificato	Abilitato
Non specificato	Disabilitato	Disabilitato
Disabilitato	Non specificato	Disabilitato
Abilitato	Abilitato	Abilitato
Abilitato	Disabilitato	Abilitato
Disabilitato	Abilitato	Disabilitato
Disabilitato	Disabilitato	Disabilitato

A tutti i livelli (oggetto e partizione) è possibile configurare il login NDS per le seguenti operazioni:

- ◆ Login alla directory mediante una password NDS o verifica della password NDS
- ◆ Impostazione di una nuova password e modifica della password esistente

Login alla directory o verifica della password NDS

Login/verifica della password ND significa:

- ◆ Login alla directory mediante una password NDS.
- ◆ Verifica della password esistente nella directory.

Le operazioni di login o verifica della password NDS sono abilitate per default. Quando si disabilita il tasto login/verifica, non sarà più possibile eseguire il login alla versione di eDirectory più recente né verificare le password. È possibile abilitare/disabilitare il login o la verifica della password NDS a livello di partizione o a livello di oggetto. Se il login/la verifica non è abilitata, non sarà possibile [impostare o modificare le password](#).

È possibile configurare il login/la verifica della password NDS tramite iManager e LDAP. Per ulteriori informazioni, vedere [“Gestione delle configurazioni NDS tramite iManager”](#) a pagina 51 e [“Gestione di configurazioni NDS tramite LDAP”](#) a pagina 52.

Impostazione di una nuova password o modifica della password NDS

Impostare o modificare una password NDS significa

- ♦ Impostazione di una nuova password per un oggetto.
- ♦ Modifica della password esistente per un oggetto.

Imposta/modifica password NDS è abilitato per default. Quando si disabilita il tasto di impostazione/modifica, non sarà possibile impostare una nuova password o modificare la password esistente in eDirectory. È possibile abilitare o disabilitare l'impostazione o la modifica della password NDS a livello di partizione e a livello di oggetto. Se il login/la verifica sono disabilitati, non sarà possibile impostare o modificare le password.

In precedenza era possibile impostare o modificare le password NDS solo tramite LDAP. Ora, tale operazione può essere eseguita anche tramite iManager. Per ulteriori informazioni, vedere [“Gestione delle configurazioni NDS tramite iManager” a pagina 51](#) e [“Gestione di configurazioni NDS tramite LDAP” a pagina 52](#).

Gestione delle configurazioni NDS tramite iManager


In questa sezione vengono fornite le seguenti informazioni:

- ♦ [“Abilitazione/disabilitazione della configurazione NDS per una partizione” a pagina 51](#)
- ♦ [“Abilitazione/disabilitazione della configurazione NDS per un oggetto” a pagina 51](#)

È possibile attivare il [tasto di login/verifica](#) o il [tasto di impostazione/modifica](#) nella configurazione di login NDS.

Abilitazione/disabilitazione della configurazione NDS per una partizione


Per abilitare il login NDS per i client delle versioni precedenti a eDirectory 8.8:

- 1 In iManager, fare clic sul pulsante *Roles and Tasks* (Ruoli e task) .
- 2 Selezionare *NMAS > Applicazione di Universal Password*.
- 3 Nel plug-in Applicazione di Universal Password, selezionare *NDS Configuration for a Partition* (Configurazione NDS per una partizione).
- 4 Seguire le istruzioni della configurazione NDS guidata per una partizione per configurare la gestione del login e della password a livello di partizione.

Per l'intera procedura è disponibile la Guida.

Abilitazione/disabilitazione della configurazione NDS per un oggetto

Per abilitare il login NDS per i client delle versioni precedenti a eDirectory 8.8:

- 1 In iManager, fare clic sul pulsante *Roles and Tasks* (Ruoli e task) .
- 2 Selezionare *NMAS > Applicazione di Universal Password*.
- 3 Nella procedura guidata, selezionare *NDS Configuration for an Object* (Configurazione NDS per un oggetto).
- 4 Seguire le istruzioni nella procedura guidata di configurazione NDS per un oggetto per configurare la gestione del login e delle password a livello di oggetto.

Per l'intera procedura è disponibile la Guida.

Gestione di configurazioni NDS tramite LDAP

Importante: È vivamente consigliato di utilizzare iManager per la gestione delle configurazioni NDS, non LDAP.

È possibile gestire le configurazioni NDS tramite LDAP utilizzando un attributo eDirectory su un container radice della partizione o su un oggetto. Gli attributi sono parte dello schema in eDirectory 8.7.1 o versione successiva e non sono supportati su eDirectory 8.7 o versioni precedenti.

Il metodo utilizzato dai client esistenti per configurare le configurazioni di login NDS è denominato gestione del login NDAP, mentre il metodo utilizzato per le configurazioni password NDS è denominato gestione delle password NDAP.

In questa sezione vengono fornite informazioni su:

- ♦ [“Abilitazione/Disabilitazione della configurazione NDS per una partizione”](#) a pagina 52
- ♦ [“Abilitazione/disabilitazione delle configurazioni NDS per un oggetto”](#) a pagina 52

Abilitazione/Disabilitazione della configurazione NDS per una partizione

Login e verifica gestione delle password

Utilizzare l'attributo `ndapPartitionLoginMgmt` per abilitare o disabilitare il login NDS e verificare la gestione delle password per una partizione.

Valore dell'attributo <code>ndapPartitionLoginMgmt</code>	Descrizione
Non presente o non specificato	Gestione login NDAP abilitata.
0	Gestione login NDAP disabilitata.
1	Gestione login NDAP abilitata.

Imposta e modifica password NDS

Utilizzare l'attributo `ndapPartitionPasswordMgmt` per abilitare o disabilitare l'impostazione e la modifica di una password NDS per una partizione.

Valore dell'attributo <code>ndapPartitionPasswordMgmt</code>	Descrizione
Non presente o non specificato	Gestione password NDAP abilitata.
0	Gestione password NDAP disabilitata.
1	Gestione password NDAP abilitata.

Abilitazione/disabilitazione delle configurazioni NDS per un oggetto

Login e verifica password NDS

Utilizzare l'attributo `ndapLoginMgmt` per abilitare o disabilitare la gestione del login NDS e la verifica per un oggetto.

Valore dell'attributo ndapLoginMgmt	Descrizione
Non presente o non specificato	La gestione del login NDAP dipende dalla configurazione a livello di partizione.
0	La gestione del login NDAP è disabilitata se è disabilitata a livello di partizione.
1	La gestione del login NDAP è abilitata a prescindere dall'impostazione di configurazione a livello di partizione.

Imposta e modifica password NDS

Utilizzare l'attributo ndapPasswordMgmt per abilitare o disabilitare l'impostazione e la modifica di una password NDS per un oggetto.

Valore dell'attributo ndapPasswordMgmt	Descrizione
Non presente o non specificato	La gestione della password NDAP dipende dalla configurazione a livello di partizione.
0	La gestione della password è disabilitata a livello di partizione.
1	La gestione della password NDAP è abilitata indipendentemente dall'impostazione della configurazione a livello di partizione.

Nota: Per ulteriori informazioni sulla creazione e la gestione delle policy di sincronizzazione della priorità, fare riferimento a [“Using LDAP Tools on Linux”](#) e [“NetIQ Import Conversion Export Utility”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

8.4.3 Operazioni sulla partizione

Quando si suddivide una partizione, le configurazioni NDS non vengono ereditate dalla partizione secondaria. Quando si uniscono le partizioni, le configurazioni NDS della partizione principale vengono conservate dalla partizione risultante.

8.4.4 Applicazione di password in grado di rilevare la distinzione tra maiuscole e minuscole in un albero misto

Se è presente un albero con un server eDirectory 8.8 o successivo oppure un server eDirectory 8.7 o precedente e i due server condividono una partizione, disabilitando la configurazione del login NDS per quella partizione si otterranno risultati non affidabili. Il server 8.8 applicherà l'impostazione, impedendo l'accesso alla directory da parte dei client esistenti. Tuttavia, il server 8.7 non applicherà l'impostazione, per cui sarà possibile accedere alla directory tramite il server 8.7.

8.5 Ulteriori informazioni

Fare riferimento alle risorse indicate di seguito per informazioni aggiuntive sulle password in grado di rilevare la differenza tra maiuscole e minuscole:

- ◆ Guida in linea di iManager
- ◆ Sezione “Deploying Universal Password” di *NetIQ Password Management 3.3 Administration* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guida all'amministrazione di NetIQ Password Management 3.3)

9 Supporto di Criteri password di Microsoft Windows Server 2008

Nelle versioni precedenti di eDirectory, gli utenti potevano utilizzare sia la policy per la complessità di default di Microsoft, sia la sintassi Novell esistente. Tuttavia, NetIQ eDirectory 8.8 SP8 supporta l'uso di policy password conformi ai requisiti di complessità delle policy password di Microsoft Windows Server 2008, che differiscono dai requisiti della policy di complessità Microsoft precedente. È possibile utilizzare iManager per creare una policy utilizzando l'opzione di sintassi Criteri password di Microsoft Server 2008 e configurare tale policy come necessaria per l'ambiente in uso.

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 9.1, "Creazione di criteri password Windows Server 2008", a pagina 55](#)
- ♦ [Sezione 9.2, "Gestione dei Criteri password di Windows Server 2008", a pagina 55](#)
- ♦ [Sezione 9.3, "Ulteriori informazioni", a pagina 56](#)

9.1 Creazione di criteri password Windows Server 2008

È possibile utilizzare iManager per creare policy password che utilizzano i criteri di complessità di Microsoft Windows Server 2008 e assegnare gli utenti nell'ambiente eDirectory in uso alla nuova policy. Per istruzioni dettagliate sulla creazione di policy password, vedere [NetIQ Password Management 3.3.2 Administration Guide \(http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html\)](http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guida all'amministrazione di NetIQ Password Management 3.3.2).

Nota

- ♦ Prima di creare una nuova policy password mediante la sintassi di Criteri password di Microsoft Server 2008, accertarsi di avere installato la versione più recente del plug-in Novell iManager Password Management. Per ulteriori informazioni sull'installazione dei moduli plug-in iManager, vedere [NetIQ iManager 2.7 Administration Guide \(https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html\)](https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guida all'amministrazione di NetIQ iManager 2.7).
 - ♦ È necessario assicurarsi che per la policy che si desidera creare o configurare siano impostate Universal Password e Advanced Password Rules.
-

9.2 Gestione dei Criteri password di Windows Server 2008

È possibile gestire con iManager le policy che utilizzano i requisiti di complessità delle policy password Windows Server 2008. Per ulteriori informazioni, fare riferimento alla sezione ["Managing Passwords by Using Password Policies" in Novell Password Management 3.3.2 Administration Guide \(http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxj0.html\)](http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxj0.html) (Guida all'amministrazione di Novell Password Management 3.3.2).

9.3 Ulteriori informazioni

Per ulteriori informazioni sulle policy password in eDirectory, fare riferimento alle seguenti risorse:

- ♦ Guida in linea di iManager
- ♦ *Novell Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guida all'amministrazione di Novell Password Management 3.3.2)
- ♦ *Novell Modular Authentication Services 3.3.4 Administration Guide* (<http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html>) (Guida all'amministrazione di Novell Modular Authentication Services 3.3.4)

10 Sincronizzazione con priorità

Sincronizzazione con priorità è una nuova funzione NetIQ eDirectory 8.8 inclusa nel processo di sincronizzazione di eDirectory. La funzione consente di sincronizzare i dati critici modificati, ad esempio le password, in modo immediato.

È possibile sincronizzare i dati critici tramite Sincronizzazione con priorità quando non è possibile attendere la sincronizzazione normale. Il processo Sincronizzazione priorità è più rapido rispetto al processo di sincronizzazione normale. Sincronizzazione con priorità è supportata solo tra due o più server eDirectory 8.8 o versioni successive che ospitano la stessa partizione.

Nella tabella seguente sono elencate le piattaforme che supportano la funzione Sincronizzazione con priorità:

Elenco funzioni	Linux	Windows
Sincronizzazione con priorità	✓	✓

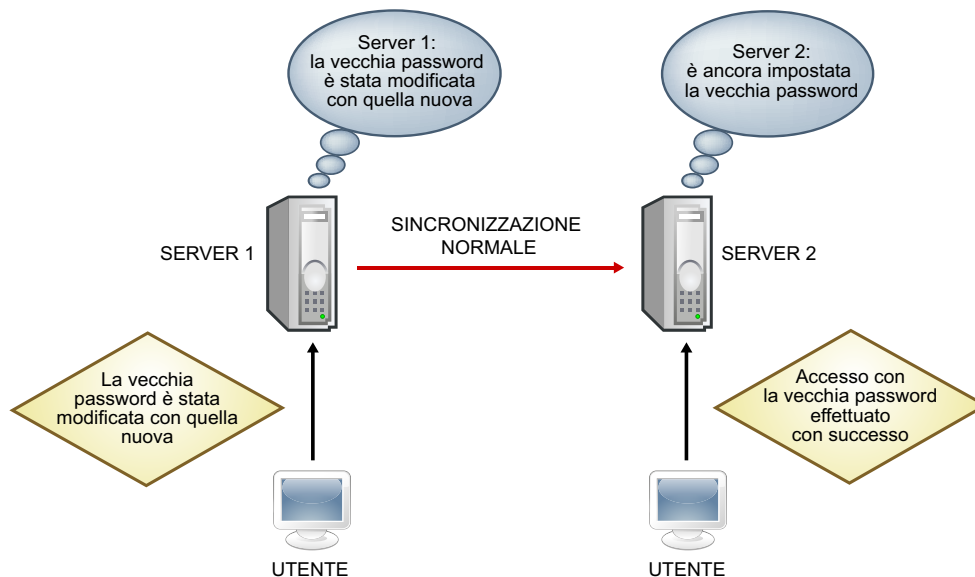
In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 10.1, “Esigenza di Sincronizzazione con priorità”, a pagina 57](#)
- ♦ [Sezione 10.2, “Utilizzo di Sincronizzazione con priorità”, a pagina 58](#)
- ♦ [Sezione 10.3, “Ulteriori informazioni”, a pagina 58](#)

10.1 Esigenza di Sincronizzazione con priorità

La sincronizzazione normale può richiedere del tempo, durante il quale i dati modificati non sono disponibili sugli altri server. Si supponga, ad esempio, che nella configurazione in uso siano presenti varie applicazioni in comunicazione con la directory. La password del Server1 viene modificata. Nella sincronizzazione normale, la modifica avviene poco prima che la stessa modifica venga sincronizzata con Server2. Pertanto, un utente sarà comunque in grado di effettuare l'autenticazione alla directory tramite un'applicazione che comunica con Server2, utilizzando la vecchia password.

Figura 10-1 Esigenza di Sincronizzazione con priorità



Nelle distribuzioni più grandi, quando i dati critici di un oggetto vengono modificati, le modifiche devono essere sincronizzate immediatamente. Il processo Sincronizzazione con priorità consente di risolvere il problema.

10.2 Utilizzo di Sincronizzazione con priorità

Per sincronizzare le modifiche di data tramite Sincronizzazione con priorità, è necessario effettuare le seguenti operazioni:

1. Abilitare Sincronizzazione con priorità, configurare il numero di thread e utilizzare la funzione per la dimensione della coda tramite iMonitor.
2. Definire le policy di Sincronizzazione con priorità identificando gli attributi critici in iManager.
3. Applicare le policy Sincronizzazione priorità alle partizioni tramite iManager.

10.3 Ulteriori informazioni

Per ulteriori informazioni su Sincronizzazione priorità, vedere:

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8)
- ♦ Guida in linea di iManager e iMonitor

11 Cifratura dei dati

In NetIQ eDirectory 8.8 e versioni successive, è possibile cifrare i dati specifici quando questi vengono memorizzati sul disco e quando vengono trasmessi tra due o più server eDirectory 8.8. Tutto questo fornisce una sicurezza maggiore per i dati riservati.

Nella tabella seguente sono elencate le piattaforme che supportano la funzione di cifratura dei dati:

Funzione	Linux	Windows
Attributi cifrati	✓	✓
Replica cifrata	✓	✓

In questo capitolo vengono fornite le seguenti informazioni:

- ♦ [Sezione 11.1, “Cifratura degli attributi”, a pagina 59](#)
- ♦ [Sezione 11.2, “Cifratura della replica”, a pagina 60](#)
- ♦ [Sezione 11.3, “Ulteriori informazioni”, a pagina 61](#)

11.1 Cifratura degli attributi

eDirectory 8.8 consente di cifrare i dati sensibili memorizzati sul disco. Gli attributi di cifratura sono una funzione specifica del server.

È possibile accedere agli attributi cifrati solo tramite canali protetti a meno che non si scelga di fornire l'accesso anche sui canali con testo non cifrato. Per ulteriori informazioni consultare [Sezione 11.1.3, “Accesso agli attributi cifrati”, a pagina 60](#).

In questa sezione vengono fornite le seguenti informazioni:

- ♦ [Sezione 11.1.1, “Esigenza di attributi cifrati”, a pagina 59](#)
- ♦ [Sezione 11.1.2, “Come cifrare gli attributi”, a pagina 60](#)
- ♦ [Sezione 11.1.3, “Accesso agli attributi cifrati”, a pagina 60](#)

La funzione degli attributi cifrati è supportata solo su eDirectory 8.8 e sui server successivi.

11.1.1 Esigenza di attributi cifrati

Prima di eDirectory 8.8, i dati venivano memorizzati con testo non cifrato sul disco. Era necessario proteggere i dati e fornire l'accesso a questi solo tramite canali protetti.

Questa funzione può essere utilizzata in scenari in cui è necessario proteggere i dati riservati, quali i membri in possesso di carta di credito dei clienti bancari.

11.1.2 Come cifrare gli attributi

È possibile cifrare gli attributi creando e definendo delle policy per gli attributi e quindi applicando tali policy ai server. È possibile creare, definire, applicare e gestire le policy attributi cifrati tramite iManager e LDAP.

- 1 Creare e definire una policy attributo cifrato:
 - 1a Determinare gli attributi per la cifratura.
 - 1b Determinare lo schema di cifratura per gli attributi.
- 2 Applicare la policy per gli attributi cifrati a un server.

11.1.3 Accesso agli attributi cifrati

È possibile accedere agli attributi cifrati solo tramite canali sicuri come la porta SSL LDAP o la porta sicura HTTP. È possibile scegliere di fornire l'accesso agli attributi cifrati tramite canali con testo non cifrato mediante il plug-in iManager. Per ulteriori informazioni, fare riferimento a [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

11.2 Cifratura della replica

L'espressione "replica cifrata" fa riferimento alla cifratura dei dati che vengono trasmessi tra due o più server eDirectory 8.8.

La replica cifrata è inclusa nella sincronizzazione normale in eDirectory.

In questa sezione vengono fornite le seguenti informazioni:

- ♦ [Sezione 11.2.1, "Esigenza della replica cifrata", a pagina 60](#)
- ♦ [Sezione 11.2.2, "Abilitazione della replica cifrata", a pagina 60](#)

11.2.1 Esigenza della replica cifrata

Prima di eDirectory 8.8, i dati venivano trasmessi tramite cavo nel corso della replica in testo non cifrato. Era necessario proteggere i dati riservati tramite la cifratura, specialmente se le repliche erano separate dal punto di vista geografico e connesse tramite Internet.

Tale funzione può essere utilizzata nei seguenti scenari:

- ♦ Se i server di directory sono in ubicazioni geografiche diverse tramite WAN e Internet ed esiste l'esigenza di cifrare i dati sensibili su cavo.
- ♦ Se si desidera proteggere solo alcune partizioni dell'albero, è possibile indicare selettivamente quali partizioni sulle quali sono conservati i dati sensibili devono essere cifrati per la replica.
- ♦ Se si richiede la replica cifrata tra due repliche specifiche di una partizione che contiene dati sensibili.
- ♦ Se si ha la sensazione che la rete utilizzata nella propria configurazione sia ostile, è possibile che si desideri proteggere i dati sensibili durante la replica.

11.2.2 Abilitazione della replica cifrata

È possibile abilitare la replica cifrata utilizzando iManager. È possibile abilitare la replica cifrata a livello di partizione e a livello di replica.

Importante: Prima di abilitare la replica cifrata, accertarsi che il server di origine e quello di destinazione dispongano di certificati di default. Se sono state apportate modifiche ai certificati, come la rinomina, la replica cifrata non riesce.

11.3 Ulteriori informazioni

Per ulteriori informazioni sulla cifratura dei dati in eDirectory vedere le seguenti risorse:

- ♦ [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8)
- ♦ Guida in linea di iManager e iMonitor

12 Prestazioni dell'inoltro di massa

NetIQ eDirectory 8.8 fornisce miglioramenti per aumentare le prestazioni dell'inoltro di massa.

Per informazioni sull'aumento delle prestazioni dell'inoltro di massa, fare riferimento alle seguenti sezioni di *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8):

- ♦ ["eDirectory Cache Settings"](#)
- ♦ ["LBURP Transaction Size Setting"](#)
- ♦ ["Increasing the Number of Asynchronous Requests in ICE"](#)
- ♦ ["Increased Number of LDAP Writer Threads"](#)
- ♦ ["Disabling Schema Validation in ICE"](#)
- ♦ ["Disabling ACL Templates"](#)
- ♦ ["Backlinker"](#)
- ♦ ["Enabling/Disabling Inline Cache"](#)
- ♦ ["Increasing the LBURP Time Out Period"](#)
- ♦ ["Offline Bulkload Utility"](#)

13 Plug-in ICE di iManager ICE

Prima di NetIQ eDirectory 8.8, alcune delle opzioni della riga di comando dell'utility ICE (Import Conversion Export) di Novell non avevano opzioni corrispondenti nel plug-in iManager.

Nella tabella seguente sono elencate le piattaforme che supportano questa funzione:

Funzione	Linux	Windows
Miglioramenti di ICE iManager	✓	✓

Nella procedura guidata ICE in iManager 2.7 con eDirectory 8.8 vengono fornite le seguenti funzioni:

- ♦ [Aggiunta dello schema mancante](#)
- ♦ [Confronto dello schema](#)
- ♦ [Generazione di un file di ordini](#)

13.1 Aggiunta dello schema mancante

In eDirectory 8.8, iManager fornisce le opzioni per aggiungere lo schema mancante allo schema di un server. Questo processo implica il confronto di un'origine e di una destinazione. Se è presente un altro schema nello schema di origine, questo viene aggiunto allo schema di destinazione. L'origine può essere un file o un server LDAP, mentre la destinazione sarà un server LDAP.

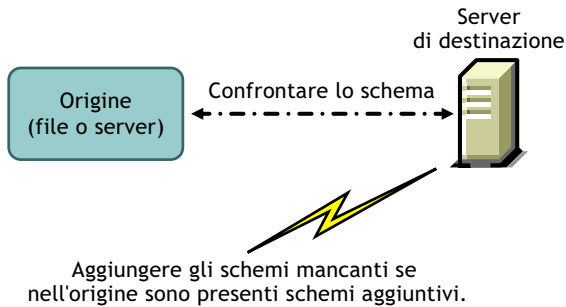
La procedura guidata ICE in iManager, consente di aggiungere lo schema mancante mediante le seguenti opzioni:

- ♦ [Aggiungi schema da un file](#)
- ♦ [Add Schema from a Server \(Aggiungi schema a un server\)](#)

13.1.1 Aggiungi schema da un file

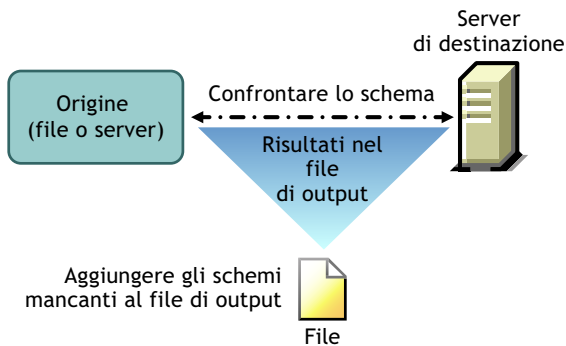
ICE è in grado di confrontare lo schema nell'origine e nella destinazione. L'origine è un file o un server LDAP, mentre la destinazione è un server LDAP. Il file dello schema di origine può essere in formato LDIF o SCH.

Figura 13-1 Compare and Add the Schema from a File (Confronta e aggiungi lo schema da un file)



Se si desidera soltanto confrontare lo schema, ma non aggiungere l'altro schema al server di destinazione, selezionare l'opzione *Confronta lo schema senza aggiungerlo*. In questo caso, l'altro schema non viene aggiunto al server di destinazione ma le differenze tra gli schemi sono disponibili per l'utente come collegamento alla fine dell'operazione.

Figura 13-2 Compare Schema and Add the Results to an Output File (Confronta lo schema e aggiungi i risultati)



Per ulteriori informazioni, fare riferimento a [“NetIQ eDirectory Management Utilities”](#) in [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

13.1.2 Add Schema from a Server (Aggiungi schema a un server)

L'origine e la destinazione sono server LDAP.

Se si desidera soltanto confrontare lo schema, ma non aggiungere l'altro schema al server di destinazione, selezionare l'opzione *Confronta lo schema senza aggiungerlo*. In tal caso, l'altro schema non viene aggiunto al server di destinazione, ma le differenze tra lo schema sono disponibili come collegamento al termine dell'operazione.

Per ulteriori informazioni, fare riferimento a [“NetIQ eDirectory Management Utilities”](#) in [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

13.2 Confronto dello schema

iManager consente di confrontare lo schema tra un'origine e una destinazione. L'origine può essere un file o un server, mentre la destinazione deve essere un file LDIF.

Tramite iManager viene eseguito un confronto dello schema tra un'origine e una destinazione e i risultati vengono memorizzati in un file di output.

La procedura guidata ICE di iManager consente di confrontare lo schema utilizzando le seguenti opzioni:

- ♦ [Confronta file dello schema](#)
- ♦ [Confronta schema tra server e file](#)

13.2.1 Confronta file dello schema

L'opzione *Confronta file dello schema* confronta lo schema tra un file di origine e un file di destinazione e inserisce i risultati in un file di output. Per aggiungere lo schema mancante al file di destinazione, applicare i record del file di output al file di destinazione.

Per ulteriori informazioni, fare riferimento a “[NetIQ eDirectory Management Utilities](#)” in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

13.2.2 Confronta schema tra server e file

L'opzione *Confronta schema tra server e file* confronta lo schema tra un server di origine e un file di destinazione e inserisce i risultati in un file di output. Per aggiungere lo schema mancante al file di destinazione, applicare i record del file di output al file di destinazione.

Per ulteriori informazioni, fare riferimento a “[NetIQ eDirectory Management Utilities](#)” in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

13.3 Genera file dell'ordine

Questa opzione consente di creare un file dell'ordine da utilizzare con il gestore delimitatore per importare i dati da un file di dati delimitato. La procedura guidata consente di creare questo file dell'ordine che contiene un elenco di attributi per una specifica classe di oggetti.

Per ulteriori informazioni, fare riferimento a “[NetIQ eDirectory Management Utilities](#)” in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

13.4 Ulteriori informazioni

Per ulteriori informazioni su questa funzione, fare riferimento alle seguenti risorse:

- ♦ *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8)
- ♦ Guida in linea di iMonitor

14 Backup basato su LDAP

La funzione di backup basato su LDAP è introdotta con NetIQ eDirectory 8.8. Si tratta di una funzione utilizzata per il backup degli attributi e dei relativi valori un oggetto per volta.

Nella tabella seguente sono elencate le piattaforme che supportano questa funzione:

Funzione	Linux	Windows
Backup basato su LDAP	✓	✓

La funzione consente di eseguire un backup incrementale nel quale il backup dell'oggetto viene eseguito solo se sono presenti modifiche all'oggetto.

Il backup basato su LDAP fornisce una serie di interfacce per il backup e il ripristino degli oggetti eDirectory esposti mediante LDAP Libraries for C tramite le operazioni estese LDAP.

Per ulteriori informazioni su LDAP Libraries for C SDK, fare riferimento alla [documentazione di LDAP Libraries for C](http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html) (<http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html>) (in lingua inglese).

Per un esempio su come eseguire il backup e il ripristino degli oggetti di eDirectory tramite LDAP, fare riferimento al [codice di esempio backup.c](http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html) (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Esigenza del backup basato su LDAP

Il backup basato su LDAP tenta di risolvere i problemi relativi al backup e ripristino corrente.

Di seguito sono indicati i problemi risolti da questa funzione:

- ♦ Fornire un'interfaccia coerente che consenta a qualsiasi applicazione di backup di terze parti o agli sviluppatori di eseguire un backup di eDirectory su tutte le piattaforme supportate.
- ♦ Fornire una soluzione per il backup incrementale degli oggetti.

14.2 Ulteriori informazioni

Per ulteriori informazioni su questa funzione, fare riferimento alle seguenti risorse:

- ♦ [LDAP Libraries for C](http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) (<http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html>)
- ♦ Codice di esempio: [backup.c](http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html) (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 Elenco LDAP Richiedi diritti effettivi

L'elenco LDAP Richiedi diritti effettivi è stato introdotto con NetIQ eDirectory 8.8 SP6.

Nella tabella seguente sono elencate le piattaforme che supportano questa funzione:

Funzione	Linux	Windows
Elenco LDAP Richiedi diritti effettivi	✓	✓

Questa funzione può essere usata per ottenere i privilegi effettivi per un determinato DN oggetto su un determinato DN di destinazione per una data serie di attributi. Viene così fornita un'interfaccia per ottenere l'elenco dei privilegi tramite LDAP libraries for C mediante le operazioni estese LDAP.

Per ulteriori informazioni su LDAP Libraries for C SDK, fare riferimento alla [documentazione di LDAP Libraries for C](http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html). (<http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html>).

15.1 Esigenza dell'interfaccia dell'elenco Richiedi diritti effettivi LDAP

L'interfaccia elenco Richiedi diritti effettivi LDAP tenta di risolvere i problemi relativi all'API Richiedi diritti effettivi.

Di seguito sono indicati i problemi risolti da questa funzione:

- ♦ Eseguire una sola richiesta a Directory per ricevere i diritti effettivi per più attributi.
- ♦ Ridurre il tempo di roundtrip impiegato da Directory per ricevere i diritti effettivi per più attributi.
- ♦ Identificare eventuali guasti negli input nella richiesta o in Directory.

15.2 Ulteriori informazioni

Per ulteriori informazioni su questa funzione, fare riferimento alle seguenti risorse:

- ♦ [LDAP Libraries for C](http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) (<http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html>).
- ♦ Codice di esempio: [getpriv.c](http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html) (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Gestione della registrazione degli errori in eDirectory 8.8

Molti clienti hanno segnalato che la registrazione degli errori di NetIQ eDirectory non è utile nell'identificazione e nella risoluzione dei problemi comuni. La registrazione degli errori viene avviata automaticamente durante l'installazione di eDirectory.

Questo capitolo è composto dalle seguenti sezioni:

- ♦ Sezione 16.1, "Livelli di sicurezza dei messaggi", a pagina 73
- ♦ Sezione 16.2, "Configurazione della registrazione degli errori", a pagina 74
- ♦ Sezione 16.3, "Messaggi DSTrace", a pagina 77
- ♦ Sezione 16.4, "Filtraggio dei messaggi di iMonitor", a pagina 80
- ♦ Sezione 16.5, "Filtraggio dei messaggi SAL", a pagina 80

16.1 Livelli di sicurezza dei messaggi

Tutti i messaggi sono collegati a un livello di gravità che consente di stabilire la criticità del messaggio. I livelli, in ordine decrescente di gravità sono:

- ♦ Sezione 16.1.1, "Fatale", a pagina 73
- ♦ Sezione 16.1.2, "Avviso", a pagina 73
- ♦ Sezione 16.1.3, "Errore", a pagina 74
- ♦ Sezione 16.1.4, "Informazioni", a pagina 74
- ♦ Sezione 16.1.5, "Debug", a pagina 74

16.1.1 Fatale

Un messaggio fatale indica un problema grave, ad esempio la perdita di dati o di funzionalità.

Esempi:

- ♦ Se il server eDirectory non riesce a caricare i moduli di sistema quali NCP Engine e DSLoader durante il caricamento dei moduli, viene segnalato e registrato un errore fatale.
- ♦ Se il server eDirectory non riesce a eseguire il collegamento alla porta sicura 636, viene segnalato e registrato un errore fatale.

16.1.2 Avviso

Messaggio non necessariamente grave, ma che potrebbe essere possibile causa di un problema futuro.

Esempi:

- ♦ Errori di connessione tra due server qualsiasi dell'albero, in seguito al quale il server viene aggiunto a una cache di indirizzi errata. È possibile ripristinare il server da questo particolare stato reimpostando la cache degli indirizzi errata.
- ♦ Se l'applicazione client LDAP effettua un collegamento e chiude la connessione senza annullare il collegamento, il server LDAP dovrà registrare un avviso con un messaggio di avviso appropriato.
- ♦ Se il server eDirectory ha consumato tutti i descrittori file e ha raggiunto il limite di soglia, non potrà più elaborare le richieste in ingresso né rispondere, causando un errore dell'applicazione.

16.1.3 Errore

Messaggio che potrebbe essere dovuto a un'operazione non valida, ma che non causa alcun problema.

Esempi:

- ♦ Quando un client tenta di aggiungere un oggetto per il quale non sono definiti attributi nello schema, il server eDirectory segnala un errore ERR_NO_SUCH_ATTRIBUTE.
- ♦ Quando un utente tenta di eseguire il login con una password non valida, il server eDirectory segnala l'errore ERR_FAILED_AUTHENTICATION.

16.1.4 Informazioni

Messaggio che descrive il corretto completamento di un'operazione o di un evento nel server eDirectory.

Esempi:

- ♦ Quando un modulo viene caricato o scaricato correttamente, può essere appropriato registrare un messaggio informativo dell'operazione.
- ♦ Quando si modifica la configurazione della cache del database, è necessario registrare un messaggio informativo relativo al corretto salvataggio della configurazione.

16.1.5 Debug

Messaggio contenente informazioni che consentiranno agli sviluppatori di eseguire il debug di un programma.

Esempi:

Quando si esegue una ricerca di gruppo dinamico, visualizzare tutti i membri di gruppo dinamici con informazioni di ID voce, ID partizione e DN dei membri. Queste informazioni consentiranno di sapere che tutti i membri vengono restituiti a livello di eDirectory.

16.2 Configurazione della registrazione degli errori

- ♦ [Sezione 16.2.1, "Il test su Linux", a pagina 75](#)
- ♦ [Sezione 16.2.2, "Windows", a pagina 75](#)

16.2.1 Il test su Linux

Per configurare le impostazioni di registrazione degli errori per i messaggi lato server, è possibile utilizzare i parametri `n4u.server.log-levels` e `n4u.server.log-file` nel file di configurazione `/etc/opt/novell/eDirectory/conf/nds.conf`.

Impostazione del livello di gravità

I livelli di gravità disponibili sono `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` e `LogDbg` (in ordine di gravità decrescente). Per ulteriori informazioni sui livelli di gravità, fare riferimento a [Sezione 16.1, "Livelli di sicurezza dei messaggi"](#), a pagina 73.

Per default, il livello di gravità è impostato su `LogFatal`. Pertanto, saranno registrati solo i messaggi con livello di gravità fatale.

Per impostare il livello di gravità, utilizzare il parametro `n4u.server.log-levels` nel file `nds.conf` nel modo indicato di seguito:

```
n4u.server.log-levels=severity_level
```

Ad esempio:

- ♦ Per impostare il livello di gravità su `LogInfo` e superiore, digitare quanto segue:

```
n4u.server.log-levels=LogInfo
```

Con questa configurazione, i messaggi con livello di gravità `LogInfo` e superiore (vale a dire, `LogFatal`, `LogWarn` e `LogErr`) saranno registrati nel file di log.

- ♦ Per impostare il livello di gravità su `LogWarn` e superiore, digitare quanto segue:

```
n4u.server.log-levels=LogWarn
```

Con questa configurazione, i messaggi con livello di gravità `LogWarn` e superiore (`LogFatal`) saranno registrati nel file di log.

Specifica del nome del file di log

Per specificare l'ubicazione del file di log nel quale saranno registrati i messaggi, utilizzare il parametro `n4u.server.log-file` nel file `nds.conf`. Per default, i messaggi vengono registrati nel file `nds.log`.

Ad esempio, per registrare i messaggi in `/tmp/edir.log`, digitare quanto segue:

```
n4u.server.log-file=/tmp/edir.log
```

Per registrare i messaggi nel log di sistema, utilizzare il parametro `n4u.server.log-file` nel modo indicato di seguito:

```
n4u.server.log-file=syslog
```

16.2.2 Windows

- ♦ ["Impostazione del livello di gravità"](#) a pagina 76
- ♦ ["Specifica del nome e del percorso del file di log"](#) a pagina 76
- ♦ ["Specifica delle dimensioni del file di log"](#) a pagina 76

Impostazione del livello di gravità

I livelli di gravità disponibili sono LogFatal, LogWarn, LogErr, LogInfo e LogDbg (in ordine di gravità decrescente). Per ulteriori informazioni sui livelli di gravità, fare riferimento a [Sezione 16.1, “Livelli di sicurezza dei messaggi”, a pagina 73](#).

Per impostare il livello di gravità, effettuare le seguenti operazioni:

- 1 Fare clic su *Start > Impostazioni > Pannello di controllo > NetIQ eDirectory Services* (Servizi NetIQ eDirectory)
- 2 Nella scheda *Servizi*, selezionare *dhlog.dlm*.
- 3 Immettere il livello di registrazione nella casella *Startup Parameters* (Parametri di avvio).

Ad esempio, per impostare il livello di registrazione su LogErr e superiore, immettere quanto segue:

```
LogLevel=LogErr
```

- 4 Fare clic *Configura*
- 5 Nella scheda *ACS Config* (Config ACS), fare clic sul segno più di *DHostLogger*.
Il parametro `LogLevel` verrà aggiornato con il valore configurato.

Specifica del nome e del percorso del file di log

- 1 Fare clic su *Start > Impostazioni > Pannello di controllo > NetIQ eDirectory Services* (Servizi NetIQ eDirectory)
- 2 Nella scheda *Servizi*, selezionare *dhlog.dlm*.
- 3 Immettere il percorso del file di log in *Startup Parameters* (Parametri di avvio), nel modo indicato di seguito:

```
LogFile=file_path
```

Ad esempio, per impostare il percorso del file su `/tmp/Err.log`, immettere quanto segue nei parametri di avvio:

```
LogFile=/tmp/Err.log
```

- 4 Fare clic *Configura*
- 5 Nella scheda *ACS Config* (Config ACS), fare clic sul segno più di *DHostLogger*.
Il parametro `LogFile` viene aggiornato con il valore configurato.

Specifica delle dimensioni del file di log

- 1 Fare clic su *Start > Impostazioni > Pannello di controllo > NetIQ eDirectory Services* (Servizi NetIQ eDirectory)
- 2 Nella scheda *Servizi*, selezionare *dhlog.dlm*.
- 3 Immettere il percorso del file di log in *Startup Parameters* (Parametri di avvio), nel modo indicato di seguito:

```
LogSize=size
```

La dimensione file predefinita è 1 MB.

- 4 Fare clic *Configura*

5 Nella scheda *ACS Config* (Config ACS), fare clic sul segno più di *DHostLogger*.

Il parametro `LogSize` viene aggiornato con il valore configurato.

16.3 Messaggi DSTrace

È possibile filtrare i messaggi di traccia in base all'ID del thread, all'ID di connessione e alla gravità del messaggio.

Una volta specificato un filtro per il messaggio, sullo schermo vengono visualizzati solo i messaggi che rientrano nel filtro. Tutti gli altri messaggi per i tag abilitati verranno registrati in `ndstrace.log` se il file è impostato su ON.

È possibile applicare un solo filtro per volta. Il filtro deve essere specificato per ciascuna sessione di DSTrace.

Per default, il livello di gravità è impostato su INFO, a indicare che saranno visualizzati tutti i messaggi con un livello di gravità superiore a INFO. È possibile vedere il livello di gravità abilitando il tag `svty`.

È inoltre possibile utilizzare *iMonitor* per filtrare i messaggi di traccia. Per ulteriori informazioni, fare riferimento alla [Sezione 16.4, "Filtraggio dei messaggi di iMonitor"](#), a pagina 80.

16.3.1 Il test su Linux

Completare la seguente procedura per filtrare i messaggi di traccia:

1 Abilitare il filtraggio con il seguente comando:

```
ndstrace tag filter_value
```

Per disabilitare il filtraggio, immettere il seguente comando:

```
ndstrace tag
```

Esempi per abilitare il filtraggio:

- ♦ Per abilitare il filtraggio per il thread ID 35, immettere quanto segue:

```
ndstrace thrd 35
```

- ♦ Per abilitare il filtraggio per il livello di gravità fatale, immettere quanto segue:

```
ndstrace svty fatal
```

I livelli di gravità possono essere FATALE, AVVISO, ERRORE, INFO e DEBUG.

- ♦ Per abilitare il filtraggio per la connessione ID 21, immettere quanto segue:

```
ndstrace conn 21
```

Esempi per la disabilitazione del filtraggio:

- ♦ Per disabilitare il filtraggio in base all'ID del thread, immettere quanto segue:

```
ndstrace thrd
```

- ♦ Per disabilitare il filtraggio in base all'ID di connessione, immettere quanto segue:

```
ndstrace conn
```

- ◆ Per disabilitare il filtraggio in base alla gravità, immettere quanto segue:

```
ndstrace svty
```

Figura 16-1 Esempio di schermata di tracce con filtri

```
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 241, size 121, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 120, size 32, err 0.
NCPEng : INFO : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 120, size 54, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 121, size 248, err 0.
NCPEng : INFO : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent : DEBUG : Calling DSAResolveName conn:22 for client .[Public].
Reslv : DEBUG : ConvertDNToID: dn=\T=WIN-0510\novell\CN=OSG-NTS-2-NDS, cts=4281a5dc:01:001
NCPcli : DEBUG : DCCreateContext context 3464002c moduleHandle 60000000 C:\Novell\NDS\ds.dlm, idHandle 00000000
Reslv : DEBUG : Connect to tcp:164.99.148.219:524 succeeded
DRL : INFO : Primary object is ID_INVALID
NCPcli : DEBUG : DCFreeContext context 3464002c idHandle 00000000, connHandle 00001b00, C:\Novell\NDS\ds.dlm
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 121, size 74, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 242, size 32, err 0.
NCPEng : INFO : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 242, size 46, flags 0, ncperr 0.
NCPEng : INFO : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 243, size 196, err 0.
NCPEng : INFO : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent : DEBUG : Calling DSASStartUpdateReplica conn:14 for client .OSG-NTS-2-NDS.novell.WIN-0510.
Reslv : DEBUG : ConvertDNToID: dn=\T=WIN-0510, cts=4281a5dc:01:001
SyncI : INFO : ** SYNCHRONIZATION DISABLED! .WIN-0510., .OSG-NTS-2-NDS.novell.WIN-0510.
Agent : DEBUG : DSASStartUpdateReplica failed, synchronization disabled (-701).
NCPEng : INFO : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 243, size 32, flags 0, ncperr 0.
```

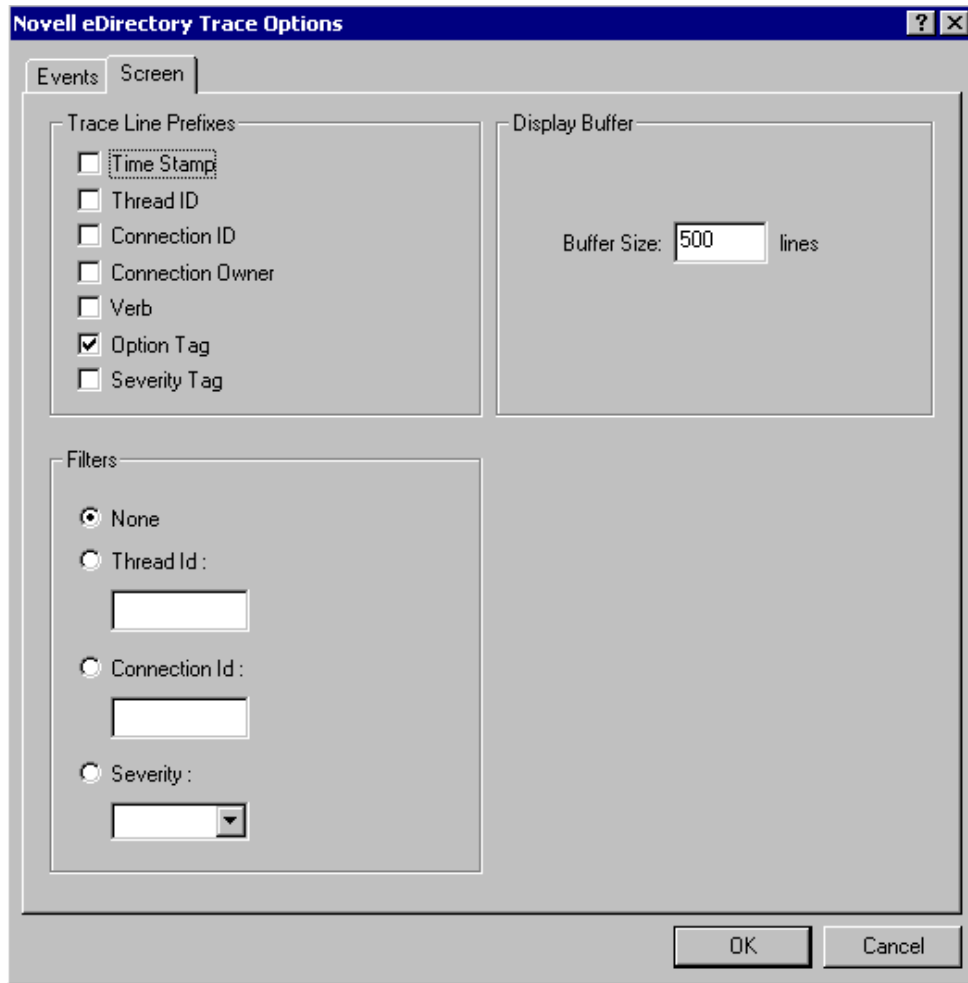
16.3.2 Windows

Completare la seguente procedura per filtrare i messaggi di traccia:

- 1 Selezionare *Start > Pannello di controllo > NetIQ eDirectory Services* (Servizi NetIQ eDirectory)
- 2 Nella scheda *Servizi*, selezionare *dstrace.dlm*.
- 3 Fare clic su *Modifica > Opzioni* nella finestra Traccia.

Viene visualizzata la finestra di dialogo NetIQ eDirectory Trace Options (Opzioni di traccia di NetIQ eDirectory).

Figura 16-2 Schermata Trace Options (Opzioni di traccia) in Windows



4 Fare clic sulla scheda *Schermo*.

5 Selezionare l'opzione di filtro dal gruppo *Filters* (Filtri) e immettere il valore del filtro.

È possibile filtrare il messaggio in base ai seguenti valori:

- ◆ ID thread
- ◆ ID connessione
- ◆ Severity

Prima di selezionare un qualsiasi filtro, accertarsi che sia abilitato in *Prefissi per la linea di traccia*.

È inoltre possibile disabilitare il filtraggio selezionando *Nessuno* oppure deselectando l'opzione di filtro.

Nota: se è stato selezionato *ID thread* o *ID connessione* come opzione di filtro e si immette un valore che non esiste, il messaggio non verrà visualizzato sullo schermo. Tuttavia, tutti gli altri messaggi continueranno a essere registrati nel file `ndstrace.log`.

16.4 Filtraggio dei messaggi di iMonitor

È possibile filtrare i messaggi di traccia di iMonitor in base all'ID connessione, all'ID thread o al numero di errore.

Per filtrare in base all'ID connessione e all'ID thread, accertarsi di averli abilitati nella scheda Configurazione della traccia.

Per ulteriori informazioni, fare riferimento alla guida in linea di iMonitor.

16.5 Filtraggio dei messaggi SAL

SAL è stato migliorato per registrare un numero maggiore di informazioni sugli errori, su richiesta. È possibile tenere traccia delle chiamate della funzione con argomenti nelle build di debug.

16.5.1 Configurazione dei livelli di gravità

È possibile utilizzare il parametro `SAL_LogLevels` per configurare i livelli di gravità per i messaggi SAL. `SAL_LogLevels` è un elenco separato da virgola, dei livelli di log desiderati.

I livelli di log sono illustrati nella tabella seguente:

Tabella 16-1 Parametri di filtraggio dei messaggi SAL

Parametro	Descrizione
LogCrit	Messaggi critici. Questo livello è abilitato per default. Dopo la registrazione di un messaggio critico, il sistema si arresta.
LogErr	Tutti i messaggi di errore. Il sistema continua a funzionare, ma i risultati sono imprevedibili.
LogWarn	Messaggi di avviso. Si tratta di un semplice avviso che informa di un errore imminente.
LogInfo	Messaggi informativi.
LogDbg	Messaggi di debug utilizzati per il debug in fase di sviluppo. Questi messaggi sono compilati da una build di versione per ridurre la dimensione dei dati binari.
LogCall	Tracce per le chiamate di funzione. Si tratta di un sottoinsieme dei messaggi di debug.
LogAll	Abilita tutti i messaggi tranne LogCall.

A “-” all’inizio di un livello di log specifico disabilita tale livello.

Esempi

Per filtrare in base a tutti i livelli di log, tranne LogInfo e LogDbg, completare i seguenti passaggi:

Il test su Linux

- 1 Interrompere ndsd.
- 2 Digitare il seguente comando:

```
export SAL_LogLevels=LogAll, -LogInfo, -LogDbg
```

- 3 Avviare ndsd.

Windows

- 1 Arrestare DHost.
- 2 Digitare il seguente comando al prompt dei comandi:

```
set SAL_LogLevels=LogAll, -LogInfo, -LogDbg  
c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
```

- 3 Riavviare DHost.

16.5.2 Impostazione del percorso del file di log

È possibile utilizzare la variabile ambientale `SAL_LogFile` per specificare l'ubicazione del file di log. Può trattarsi di un nome file valido, con un percorso valido o una delle ubicazioni indicate di seguito.

- ♦ Console: tutti i messaggi vengono registrati nella console.
- ♦ Syslog: in Linux, i messaggi vengono registrati nel log di sistema. In Windows, i messaggi vengono registrati in un file con il nome `syslog`. Si tratta del comportamento predefinito per la registrazione.

Tutti gli errori critici vengono sempre registrati nel log di sistema a meno che questo non sia disabilitato specificamente.

17 Utility bulkload offline: Idif2dib

Idif2dib è una nuova utility introdotta con NetIQ eDirectory 8.8 per il bulkload dei dati dai file LDIF al database di eDirectory. Si tratta di un'utility offline che consente bulkload più rapidi rispetto agli altri strumenti online.

Nella tabella seguente sono elencate le piattaforme per le quali è supportato Idif2dib.

Funzione	Linux	Windows
Idif2dib	✓	✓

17.1 Esigenza di Idif2dib

L'utility Idif2dib nei casi in cui occorre popolare un database utente di grandi dimensioni con le voci di un file LDIF. Strumenti online quali ICE e ldapmodify sono più lenti rispetto a Idif2dib per quanto riguarda questa operazione, a causa dei sovraccarichi associati al bulkload online, ad esempio il controllo dello schema, la conversione del protocollo e le verifiche di controllo dell'accesso. Idif2dib consente un tempo di operatività rapido nel caso in cui sia necessario popolare un database utente di grandi dimensioni e quando il tempo di fermo iniziale non è un problema.

17.2 Ulteriori informazioni

Per ulteriori informazioni su questa utility, fare riferimento a [“Offline Bulkload Utility”](#) in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

18 Backup di eDirectory Backup con SMS

SMS (Storage Management Services) di Novell è un framework API utilizzato dalle applicazioni di backup per fornire una soluzione di backup completa. Il framework SMS è implementato da due componenti principali:

- ◆ Storage Management Data Requester (SMDR)
- ◆ TSA (Target Service Agent)

Il TSA per eDirectory (`tsands`) serve destinazioni eDirectory e fornisce un'implementazione dell'API SMS di Novell per gli alberi della directory. Le applicazioni possono essere scritte sull'API SMS per fornire una soluzione di backup completa.

Il TSA per NDS è supportato in Linux.

19 Revisione LDAP

La revisione è una delle funzionalità principali di interesse per l'amministratore nella valutazione di una directory. Il meccanismo di eventi di eDirectory semplifica la revisione di eDirectory. Poiché le applicazioni utilizzano sempre più il protocollo LDAP per accedere alle directory, il requisito di revisione delle operazioni LDAP sta diventando prevalente.

Questo capitolo è composto dalle seguenti sezioni:

- ♦ [Sezione 19.1, "Esigenza della revisione LDAP"](#), a pagina 87
- ♦ [Sezione 19.2, "Utilizzo della revisione LDAP"](#), a pagina 87
- ♦ [Sezione 19.3, "Ulteriori informazioni"](#), a pagina 88

19.1 Esigenza della revisione LDAP

Questo meccanismo di eventi era evidentemente assente nel server LDAP eDirectory esistente, che non era in grado di fornire informazioni sufficienti su LDAP. Sebbene il sistema di eventi NDS producesse eventi per tutte le operazioni di eDirectory, la maggior parte di queste informazioni era insufficiente o irrilevante per un'applicazione per la revisione del server LDAP. Le informazioni relative al protocollo, ai dettagli del collegamento, all'indirizzo di rete, ai metodi di autenticazione, ai tipi di autenticazione, ai dettagli della ricerca e delle transazioni LDAP e così via, di importanza fondamentale per la revisione di un server LDAP non erano disponibili con gli eventi. Gli sviluppatori di applicazioni trovavano difficile scrivere applicazioni di revisione LDAP in base a questi eventi

Poiché LDAP è un'interfaccia importante di eDirectory, per fornire un meccanismo per la revisione del server LDAP eDirectory da parte delle applicazioni, in NetIQ eDirectory 8.8 versione SP3 viene introdotto un nuovo sottosistema di eventi LDAP. Tale sottosistema genera eventi specifici LDAP con tutte le informazioni di rilievo per la revisione di un server LDAP da parte di un'applicazione. Tali eventi sono noti come revisione LDAP.

19.2 Utilizzo della revisione LDAP

La revisione LDAP consente alle applicazioni di monitorare/revisionare operazioni LDAP quali l'aggiunta, la modifica, la ricerca e via di seguito e recupera informazioni utili dal server LDAP, quali le informazioni sulla connessione, l'IP del client a cui era connesso il server al momento dell'operazione LDAP, l'ID messaggio, il codice risultato dell'operazione e via di seguito.

La revisione LDAP può essere eseguita tramite [NDK LDAP Libraries for C \(http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html\)](http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html), che fornisce l'interfaccia lato client per questa funzione mediante le nuove strutture e i nuovi eventi LDAP.

19.3 Ulteriori informazioni

Per ulteriori informazioni sugli eventi di revisione LDAP, fare riferimento alle risorse indicate di seguito:

- ♦ “Configuring LDAP Services for NetIQ eDirectory” in *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).
- ♦ NDK: LDAP Tools (<http://developer.novell.com/documentation/cldap/ltolenu/data/hevgtl7k.html>) nella documentazione relativa a LDAP Libraries for C.

Per informazioni sugli strumenti LDAP, vedere *LDAP Libraries for C* (<http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html>).

20 Revisione con XDASv2

La specifica XDASv2 fornisce una classificazione standard degli eventi di revisione, e definisce un set di eventi generici a livello di sistema globale distribuito. XDASv2 fornisce un formato per i record di revisione semplice e trasferibile, mediante il quale è possibile semplificare i processi di unione e analisi delle informazioni di revisione provenienti da diversi componenti a livello di sistema distribuito. Gli eventi XDASv2 vengono incapsulati all'interno di un sistema notazionale che consente di estendere il gruppo di identificatori evento standard oppure esistente.

Con eDirectory 8.8 SP8, se l'agente XDASv2 non è in grado di comunicare con il server syslog, può essere configurato in modo da inserire nella cache gli eventi di revisione registrati, garantendo che i dati non vengano persi. L'agente quindi tenta di reinviare gli eventi di revisione memorizzati, continuando fino a quando la comunicazione non viene ripristinata. La memorizzazione nella cache degli eventi XDAS è disabilitata per default.

Per ulteriori informazioni, fare riferimento a [NetIQ XDASv2 Administration Guide](#) (Guida all'amministrazione di NetIQ XDASv2).

21 Varie

In questo capitolo vengono illustrate diverse nuove funzioni di NetIQ eDirectory 8.8.

- ♦ Sezione 21.1, “Segnalazione di dump della cache di iMonitor”, a pagina 91
- ♦ Sezione 21.2, “Supporto di Microsoft Large Integer Syntax in iManager”, a pagina 91
- ♦ Sezione 21.3, “Memorizzazione nella cache degli oggetti di sicurezza”, a pagina 92
- ♦ Sezione 21.4, “Miglioramento delle prestazioni della ricerca nei sottoalberi”, a pagina 92
- ♦ Sezione 21.5, “Modifiche a Localhost”, a pagina 93
- ♦ Sezione 21.6, “Gestione di 256 file in Solaris”, a pagina 93
- ♦ Sezione 21.7, “Gestione della memoria in Solaris”, a pagina 93
- ♦ Sezione 21.8, “Gruppi nidificati”, a pagina 93

21.1 Segnalazione di dump della cache di iMonitor

Nella pagina Cache modifiche di iMonitor viene visualizzato un solo oggetto per volta, per cui diventa difficile sfogliare l'intera cache delle modifiche. In eDirectory 8.8 SP8 è stato aggiunto un nuovo Change Cache Dump Report (Report dump cache delle modifiche) ai report di default inclusi in iMonitor. Questo report consente di visualizzare l'intera cache delle modifiche in una sola volta. Il report può aiutare l'amministratore a comprendere meglio le modifiche che si verificano su un particolare server.

Quando si esegue un Change Cache Dump Report (Report dump cache delle modifiche) iMonitor genera anche un dump XML completo di tutti gli oggetti della cache, insieme agli attributi e ai valori che devono essere sincronizzati tra i server.

Per ulteriori informazioni sui report di iMonitor, fare riferimento a [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

21.2 Supporto di Microsoft Large Integer Syntax in iManager

eDirectory 8.8 SP8 fornisce una nuova sintassi per supportare Microsoft Large Integer Syntax. La nuova sintassi può essere utilizzata per memorizzare valori con numeri interi estesi o date precedenti al 1970 o successive al 2038. È possibile utilizzare LDAP o iManager per creare o gestire attributi con questa sintassi.

Nota: in eDirectory si continuano a utilizzare la sintassi esistente e i valori a 32 per le registrazioni orario interne.

21.3 Memorizzazione nella cache degli oggetti di sicurezza

Il container di sicurezza viene creato dalla partizione radice quando il primo server viene installato nell'albero e contiene informazioni quali i dati globali, le policy di sicurezza e le chiavi.

Dopo l'introduzione della password universale, ogni volta che un utente esegue il login a eDirectory tramite NMAS, NMAS aveva accesso alle informazioni nel container di sicurezza per autenticare il login. Quando la partizione con il container di sicurezza non era presente localmente, NMAS aveva accesso al server, che conteneva questa partizione. Tutto questo aveva un impatto negativo sulle prestazioni dell'autenticazione NMAS. La situazione era peggiore negli scenari in cui l'accesso al server contenente la partizione con il container di sicurezza doveva essere eseguito su collegamenti WAN.

Per risolvere il problema, con eDirectory 8.8, i dati del container di sicurezza vengono memorizzati nella cache sul server locale. Pertanto, NMAS non dovrà accedere al container di sicurezza ubicato su un computer diverso ogni volta che un utente esegue il login, può accedere facilmente al container localmente. In tal modo le prestazioni migliorano. L'aggiunta della partizione con il container di sicurezza nel server locale migliora le prestazioni, ma potrebbe non essere fattibile negli scenari in cui sono presenti troppi server.

Se i dati effettivi nel container di sicurezza cambiano sul server sul quale è presente la partizione del container di sicurezza, la cache locale viene aggiornata mediante un processo in background denominato backlink. Di default, il backlink viene eseguito ogni tredici ore e sposta i dati modificati dal server remoto. Se i dati devono essere sincronizzati immediatamente, è possibile pianificare il backlink sul server locale tramite iMonitor, ndstrace in Linux oppure ndscons in Windows. Per ulteriori informazioni, fare riferimento alla guida in linea di iMonitor o alla manpage ndstrace.

La funzione di memorizzazione nella cache degli oggetti di protezione è abilitata per default. Se non si desidera memorizzare nella cache i dati tramite backlink, rimuovere `CachedAttrsOnExtRef` dall'oggetto server NCP.

21.4 Miglioramento delle prestazioni della ricerca nei sottoalberi

Le prestazioni di ricerca nei sottoalberi di eDirectory per un albero di grandi dimensioni con una struttura molto nidificata restano invariate a prescindere dal DN di base della ricerca. Tale problema è stato risolto utilizzando l'attributo `AncestorID`. L'attributo `AncestorID` è un elenco di ID voce di tutti gli antenati associati a ciascuna voce. Questo attributo `AncestorID` viene utilizzato internamente durante la ricerca nel sottoalbero e pertanto restringe l'ambito della ricerca.

L'attributo viene popolato quando si aggiunge una voce e si esegue l'upgrade per tutte le voci del DIB e viene ripopolato per tutte le voci del sottoalbero dopo che questo è stato spostato. Tuttavia, per la ricerca nel sottoalbero non si utilizzerà l'attributo `AncestorID` durante il popolamento dell'attributo dopo l'upgrade e lo spostamento del sottoalbero. Pertanto, le prestazioni del sottoalbero restano simili alle prestazioni della ricerca nel sottoalbero precedente a eDirectory 8.8.

Per verificare se i valori `AncestorIDs` vengono aggiornati dopo l'upgrade:

Una volta che i valori `AncestorIDs` vengono popolati, la versione dell'upgrade degli oggetti NDS passa a 6 o alla versione successiva. È possibile visualizzare tutto questo utilizzando iMonitor nella sezione *DIB History* di Informazioni sugli agenti.

Per verificare se i valori `AncestorIDs` vengono aggiornati dopo l'operazione di spostamento del sottoalbero:

Mentre i valori di `AncestorIDs` vengono popolati, l'attributo `UpdateInProgress` nell'oggetto `Pseudo server` contiene l'elenco di ID voce della radice della partizione del sottoalbero. Una volta che i valori di `AncestorIDs` vengono popolati, l'attributo non sarà presente in `Pseudo server`.

`DSRepair` aggiorna l'attributo `AncestorID` nel caso in cui non sia valido.

21.5 Modifiche a Localhost

I server eDirectory 8.8 non sono in ascolto su un indirizzo di loopback. Le utility che impiegano localhost devono essere modificate in modo da utilizzare il nome host o la risoluzione degli indirizzi IP.

Se uno strumento o un'utility di terze parti risolve tramite localhost, è necessario fare in modo che venga invece utilizzato il nome host o l'indirizzo IP, non l'indirizzo localhost.

21.6 Gestione di 256 file in Solaris

In precedenza, per l'implementazione dei flussi di Solaris 2.x era possibile utilizzare solo un massimo di 256 descrittori file. Tale limite era insufficiente per il corretto funzionamento di eDirectory. eDirectory 8.8 fornisce una libreria stub per superare questo limite.

21.7 Gestione della memoria in Solaris

Nelle versioni precedenti di eDirectory su Solaris come gestore di memoria veniva utilizzato Geodesic*, un prodotto di terze parti. Con questa versione, in eDirectory 8.8 non è incluso alcun allocatore di memoria di terze parti, ma viene utilizzato il gestore di memoria nativo.

Tale soluzione non ha alcun impatto negativo sulle prestazioni di eDirectory. Nella maggior parte dei casi le prestazioni sono migliorate o sono rimaste identiche agli allocatori di terze parti.

21.8 Gruppi nidificati

eDirectory 8.8 SP2 supporta il raggruppamento di gruppi, fornendo in tal modo una forma di raggruppamento più strutturata. Questa funzione è denominata Nested Groups (Gruppi nidificati). Al momento, la nidificazione è consentita per i gruppi statici.

La nidificazione può includere fino a 200 livelli.

Per ulteriori informazioni sui gruppi nidificati, fare riferimento a [NetIQ eDirectory 8.8 SP8 Administration Guide](#) (Guida all'amministrazione di NetIQ eDirectory 8.8 SP8).

