Giugno 2015

DocuShare
Guida di Active Directory/LDAP

Data di pubblicazione: giugno 2015.

Questo documento supporta DocuShare versione 7.0.

Indice generale

1 Struttura LDAP

Descrizione generale del protocollo LDAP

In questa guida vengono fornite informazioni che consentono di apprendere i concetti di base su LDAP o Windows Active Directory; tuttavia, non vengono incluse istruzioni per la loro implementazione. Si presuppone che il server Active Directory sia già in funzione e che sia gestito da un amministratore di Active Directory o LDAP. Negli esempi citati in questa guida vengono utilizzati Microsoft Windows 2012 Server con Microsoft Internet Explorer (IE).

Il protocollo LDAP (Lightweight Directory Access Protocol) è un'alternativa leggera al protocollo X.500 Directory Access Protocol (DAP). LDAP utilizza lo stack di protocollo TCP/IP invece dello stack di protocollo OSI richiesto da X.500. Come alternativa leggera, LDAP semplifica alcune operazioni, tuttavia non offre il supporto per alcune funzioni di X.500 DAP.

LDAP viene utilizzato come protocollo tra un client directory e un server. LDAP definisce il contenuto dei messaggi scambiati tra un client LDAP e un server LDAP. Il client LDAP, in questo caso il server DocuShare, comunica con il server LDAP. Il server LDAP agisce da gateway e accede all'elenco in linea LDAP. L'elenco in linea LDAP può essere implementato come funzionalità autonoma nel server LDAP o come elenco in linea in un server X.500.

DocuShare invia le query sul contenuto dell'elenco in linea al server LDAP. Il server LDAP accede all'elenco in linea, LDAP o X.500, e restituisce i risultati a DocuShare. Il protocollo LDAP consente ai clienti di eseguire operazioni di lettura e di aggiornamento dei dati dell'elenco in linea.

Nota: DocuShare non aggiorna i dati dell'elenco in linea LDAP e si limita a leggere i risultati delle query inviate al server LDAP.

Struttura LDAP

Le voci all'interno di un elenco in linea LDAP sono organizzate in una struttura gerarchica specifica.

Elenchi in linea

Un elenco in linea è un tipo di database speciale. Gli elenchi in linea sono ottimizzati per supportare un volume elevato di richieste di **lettura** insieme all'accesso in **scrittura**, che in genere è limitato agli amministratori di sistema. Un elenco in linea LDAP è simile alle pagine bianche di una rubrica telefonica, nel senso che viene letto più spesso di quanto non venga aggiornato.

Come in una rubrica telefonica in cui sono elencate persone, società e organizzazioni, in un elenco in linea LDAP sono elencati oggetti quali utenti, server e stampanti. Analogamente a una rubrica che contiene informazioni su ciascun elemento, ad esempio nome, numero e indirizzo, le voci dell'elenco in linea LDAP contengono informazioni relative a ciascun oggetto. Le informazioni sugli oggetti sono definite **attributi**.

Attributi

Ciascuna voce relativa a un oggetto contenuta in un elenco in linea LDAP comprende uno o più attributi. Ogni attributo è composto da un **tipo** e da un **valore**. Una voce di rubrica telefonica ha attributi quali il nome di una persona e il corrispondente numero telefonico. Gli attributi LDAP vengono visualizzati nel formato **commonName=Jane Smith telephoneNumber=555-555-5555**. Nella seguente tabella vengono elencati alcuni attributi LDAP comuni, insieme agli alias associati all'attributo.

Attributo LDAP	Alias attributo	Descrizione dell'attributo	Esempio
commonName	cn	Nome comune di una voce	Jane Doe
Surname	sn	Cognome della persona	Doe
userID	uid	ID utente o nome di login	jdoe
telephoneNumber	-	Numero telefonico	555-123-4567
organizationalUnitName	ou	Nome dell'unità organizzativa	my department
organization	o	Nome dell'organizzazione	my company
domainComponent	dc	Componente DNS	xyz.com

Nome distinto relativo

Il nome distinto relativo, o **RDN** (Relative Distinguished Name), è rappresentato sotto forma di **coppia di attributi** (tipo e valore), ad esempio:

cn=Jane Doe

uid=smith

ou=marketing

dc=Xerox

Nome distinto

Le voci nell'elenco in linea sono organizzate per Nome distinto o DN (Distinguished Name). Il nome distinto è simile al percorso assoluto di un file nel file system di Windows. Il DN di un oggetto è composto dal nome e dalla posizione della voce all'interno dell'elenco in linea.

Un DN è composto da coppie di attributi RDN separate da virgole, ad esempio:

cn=John Smith,ou=marketing,dc=Xerox,dc=com

cn=John Smith,ou=assistenza,dc=Xerox,dc=com

Il percorso per un DN va dall'ordine più basso a quello più alto. L'ordine è inverso rispetto a quello utilizzato nel file system di Windows. Analogamente al file system di Windows, che consente a più file di avere lo stesso nome se ciascuno di essi si trova in una directory diversa, più utenti possono avere lo stesso RDN a condizione che il DN sia univoco. Come illustra l'esempio di DN di cui sopra, un utente John Smith potrebbe essere elencato nel reparto marketing e un altro John Smith potrebbe essere elencato nel reparto assistenza.

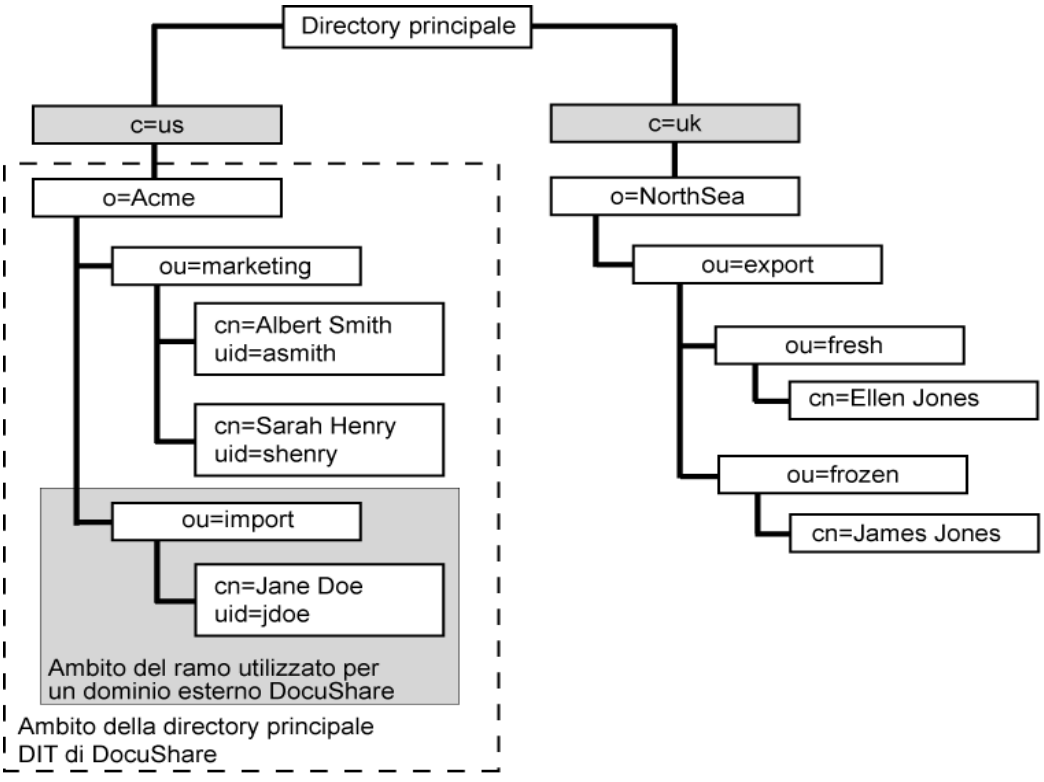
Directory principale DIT (Directory Information Tree)

Nell'elenco in linea le voci sono disposte in una struttura gerarchica denominata directory principale o **DIT** (Directory Information Tree). Una directory principale DIT è basata sul nome distinto delle voci, con i nomi distinti organizzati in rami che in genere rappresentano una struttura geografica o organizzativa. Microsoft Active Directory è spesso organizzata per domini geografici o per DNS.

Organizzazione DIT basata su domini geografici

L'esempio riportato di seguito mostra come l'amministratore di un'azienda che importa prodotti ittici potrebbe organizzare geograficamente la propria gerarchia dell'elenco in linea LDAP.
Per ospitare un server DocuShare per la società Acme negli Stati Uniti, l'amministratore dovrebbe definire la **directory principale DIT** come **o=Acme, c=us**.

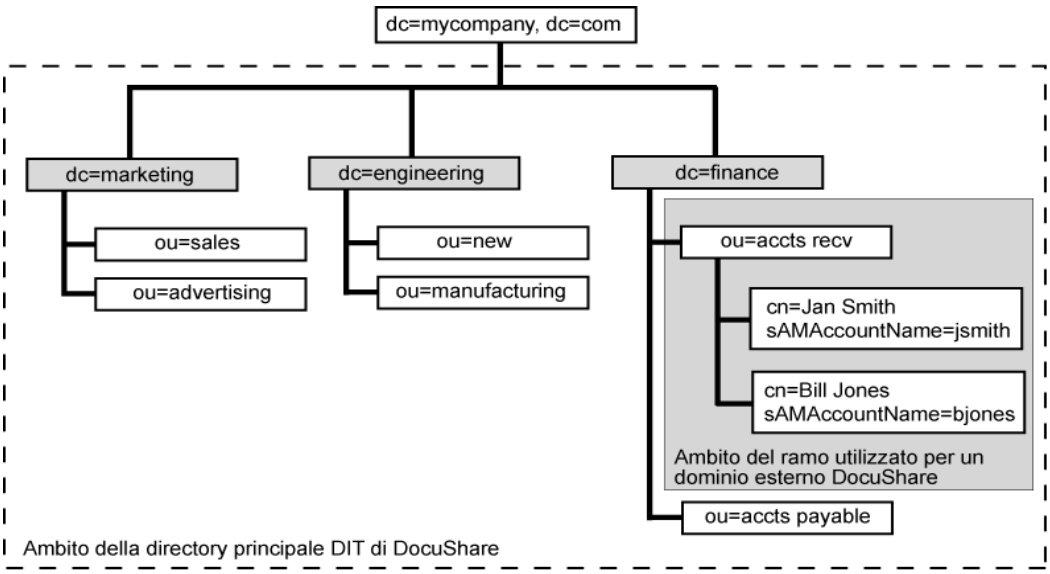
Per definire un **dominio esterno** per il reparto importazioni di Acme, l'amministratore deve definire il Localizzatore autenticazione relativa e il Localizzatore servizi directory relativi come **ou=import**.



Organizzazione DIT basata su DNS

L'esempio riportato di seguito mostra come l'amministratore di un'azienda potrebbe organizzare la propria gerarchia dell'elenco in linea LDAP in base al DNS. La società utilizza dei server di dominio Windows per le divisioni marketing, assistenza e finanza. Definendo la directory principale DIT come **dc=mycompany, dc=com**, l'amministratore può creare un dominio DocuShare esterno per ciascun reparto all'interno di una divisione.

Per definire un **dominio esterno** per il reparto contabilità clienti nella divisione Finanza, l'amministratore deve definire il Localizzatore autenticazione relativa e il Localizzatore servizi directory relativi come **ou=accts recv**, **dc=finance**.



2 Configurazione di LDAP/DocuShare

Configurazione di DocuShare

Per configurare il sito DocuShare per l'utilizzo di LDAP/Active Directory, accedere come amministratore al proprio sito DocuShare, quindi seguire le procedure dalla A alla F.
Per configurare DocuShare correttamente, utilizzare **Active Directory Administration Tool** oppure il **comando LDIFDE di Active Directory** per raccogliere le informazioni necessarie. Entrambi i processi di raccolta di informazioni sono descritti in questo capitolo.

A — Configurazione di LDAP

Utilizzare la pagina di amministrazione Configurazione LDAP di DocuShare per stabilire una connessione tra il server DocuShare e il server LDAP nonché per definire la directory principale DTI (Directory Information Tree) utilizzata per creare domini DocuShare esterni.

1. Aprire la pagina **Configurazione LDAP** dell'interfaccia di amministrazione.
2. Nel campo **Host**, inserire il nome host, l'indirizzo IP o il nome DNS del server LDAP/Active Directory (preferibilmente FQDN o, in alternativa, l'indirizzo IP). Utilizzare uno spazio per separare più indirizzi server LDAP.
3. Nel campo **Porta**, inserire il numero di porta utilizzato dal server LDAP, se è diverso dal numero di porta 389.
4. **Facoltativo**: nel campo **SSL**, inserire il numero di porta utilizzato per Secure Socket Layer.
5. Nel campo **Directory principale DIT**, inserire le informazioni ottenute mediante la ricerca con Active Directory Administration Tool per un riferimento a namingContext. Ad esempio, queste informazioni avrebbero il formato dc=adoc,dc=Xerox,dc=com.
6. Nel campo **Chiave RDN utente**, inserire l'attributo cn. Questo è l'alias per il commonName dell'attributo. L'attributo potrebbe essere diverso, a seconda del tipo di server LDAP utilizzato (iPlanet e così via).
7. Selezionare **Agente** nel campo **Agente di sistema**.

   La maggior parte dei server Active Directory richiede il login mediante un account Agente o un account di servizio.
8. Inserire il nome distinto **DN** dell'account agente.

   Ad esempio, cn=john,cn=users,dc=adoc,dc=xerox.
9. Nel campo **Password**, inserire la password per l'account agente.

10. Andare alla sezione Verifica connessione LDAP nella parte inferiore della pagina Configurazione LDAP.

    Utilizzare l'opzione Verifica connessione LDAP per controllare che sia presente una connessione valida al server LDAP e che il login sia stato eseguito correttamente.

11. Selezionare **Agente** nel campo **Connection DN** (DN connessione).

12. Nel campo **Nome**, inserire il nome distinto inserito nel campo DN al passaggio 8.

13. Nel campo **Password**, inserire la password inserita nel campo Password al passaggio 9.

14. Fare clic su **Applica** e **verifica**.

    Se la connessione al server LDAP è stata stabilita correttamente, verrà visualizzato il messaggio “Operazione riuscita”.

15. Ripetere i passaggi da 11 a 14 ma selezionando Utente nel campo Connection DN (DN connessione).

    Nota: questa verifica non controlla la validità della directory principale DIT né il Localizzatore autenticazione relativa di domini esterni. Viene controllato soltanto se DocuShare ha ricevuto una risposta positiva dal server LDAP.

B — Configurazione avanzata

Utilizzare la configurazione avanzata LDAP per impostare il modo in cui specifiche classi di oggetto devono essere definite nel server LDAP.

1. Fare clic su **Avanzate** nella parte inferiore della pagina Configurazione LDAP.
2. Viene visualizzata la pagina Configurazione avanzata LDAP.
3. Nella parte inferiore della pagina Configurazione avanzata LDAP, individuare il titolo della sezione **Classi oggetto**.
4. Nel campo **Utente**, sostituire la voce predefinita **person** con il termine **user** (tutte lettere minuscole).
5. Nel campo **Gruppo statico** sostituire la voce predefinita **groupOfUniqueNames** con il termine **group** (tutte lettere minuscole).
6. Fare clic su **Applica**.

C — Abilitazione dei provider LDAP

Utilizzare le pagine di amministrazione **Servizi di protezione** e **Servizio Directory** di DocuShare per abilitare sia i servizi di protezione che i servizi directory per LDAP. In tal modo gli utenti possono selezionare i domini esterni LDAP dall'elenco a discesa Domini quando viene visualizzata la richiesta durante il login.

1. Aprire la pagina **Servizi di protezione** dell'interfaccia di amministrazione.
2. Nella pagina Servizi di protezione, selezionare la casella di controllo **LDAP** per abilitare LDAP come provider dell'autenticazione per tutti i domini esterni, quindi fare clic su **Applica**.
3. Aprire la pagina **Servizi directory** dell'interfaccia di amministrazione.
4. Nella pagina Servizi directory, selezionare la casella di controllo **LDAP** per abilitare LDAP come provider dei servizi directory per tutti i domini esterni, quindi fare clic su **Applica**.

D — Associazione dell'utente

Utilizzare la pagina di amministrazione **Associa utente** di DocuShare per stabilire un'associazione tra le proprietà dell'account DocuShare e gli attributi dell'account LDAP.

1. Aprire la pagina **Associa utente** dell'interfaccia di amministrazione.
2. Nel campo **Nome**, inserire l'attributo utilizzato da LDAP per il nome di un utente. In genere è **givenName**.
3. Nel campo **Cognome**, inserire l'attributo utilizzato da LDAP per il cognome di un utente. In genere è **surname** oppure **sn**. Questo è un campo obbligatorio.
4. Nel campo **Nome utente**, inserire l'attributo utilizzato da LDAP per il nome di login di un utente. In genere è **sAMAccountName**. Questo è un campo obbligatorio.
5. Se l'elenco in linea LDAP contiene attributi aggiuntivi, ad esempio indirizzo e-mail, fermo posta, numero telefonico o home page, inserire questi attributi nei campi appropriati nella pagina Associa utente.
6. Fare clic su **Applica** per salvare queste informazioni.

E — Associazione del gruppo

Utilizzare la pagina di amministrazione **Associa gruppo** di DocuShare per stabilire un'associazione tra le proprietà dell'account DocuShare e gli attributi dell'account LDAP.

1. Utilizzare le informazioni ottenute usando il comando LDIFDE e inserire questi attributi nei campi appropriati della pagina Associa gruppo.

   Per ulteriori informazioni, fare riferimento alla sezione di questo capitolo intitolata *Il comando LDIFDE di Active Directory/Analisi del contenuto del file adexport.text/E. Proprietà Associa gruppo*.
2. Fare clic su **Applica** per salvare queste informazioni.

F — Creazione di un dominio

Utilizzare la pagina di amministrazione Domini di DocuShare per creare domini esterni nel sito DocuShare locale. Ciascun dominio DocuShare esterno rappresenta un ramo della struttura dell'elenco in linea LDAP e ogni ramo contiene una raccolta di account utente e account di gruppo DocuShare.

1. Aprire la pagina **Domini** dell'interfaccia di amministrazione.
2. Nel campo **Aggiungi**, inserire il nome del dominio esterno che si desidera aggiungere al sito locale.

   Questo può essere semplicemente un nome descrittivo, ad esempio Assistenza.
3. Selezionare **LDAP** nelle pagine Provider | Servizi di protezione e Provider | Servizi directory dell'interfaccia di amministrazione.
4. Nel campo **Localizzatore autenticazione relativa**, inserire una o più coppie di attributi per definire il percorso della directory che contiene gli account utente e di gruppo.

   Utilizzare i componenti attributo del nome distinto (DN) che si trovano a sinistra della directory principale DIT e a destra del nome distinto relativo (RDN) dell'utente.

Ad esempio, il DN per un account utente in un dominio è cn=users name,ou=assistenza,ou=docushare,dc=adoc,dc=xerox,dc=com. Il dominio Assistenza si trova nel ramo ou=assistenza, ou=docushare. La directory principale DIT è dc=adoc, dc=xerox, dc=com.

5. Nel campo **Localizzatore servizi directory relativi**, inserire una o più coppie di attributi.

   Utilizzare le stesse coppie di attributi inserite nel campo Localizzatore autenticazione relativa.

   DocuShare 6.6.x supporta solo LDAP per servizi di autenticazione e directory, pertanto i valori per il Localizzatore autenticazione relativa e il Localizzatore servizi directory relativi sono identici.

6. Fare clic su **Aggiungi** per aggiungere questo dominio esterno al proprio menu di login locale.

G — Aggiunta

Dopo aver completato la pagina Configurazione LDAP, Provider, Associa utente e Domini, si è pronti per aggiungere account utente e di gruppo al dominio esterno nel proprio sito DocuShare. Se si tenta di elencare utenti o gruppi nel nuovo dominio esterno, il dominio risulterebbe vuoto. Ora è necessario aprire il dominio sul server LDAP e selezionare gli account utente e di gruppo che si desidera rendere membri del dominio esterno locale.

1. Aprire la pagina **Aggiungi** dell'interfaccia di amministrazione.

   Questa non è la stessa della pagina **Aggiungi utente**.

2. Selezionare un **Tipo di account** e un **Dominio** esterno.

3. Scegliere la modalità di filtro dell'elenco degli account di dominio esterni e includere un filtro semplice, ad esempio un nome o un nome parziale o una proprietà oggetto specifica.

4. Fare clic su **Vai** per visualizzare un elenco dei tipi di account selezionati.

5. Selezionare gli account che si desidera visualizzare localmente sul sito e fare clic sulla freccia **Aggiungi** per spostarli nel campo **Selezionato**. Se non si include un account nel campo Selezionato si impedisce all'utente o al gruppo di accedere al sito.

6. Al termine dell'operazione, fare clic su **Aggiungi account**. DocuShare aggiunge gli account utente o di gruppo del dominio esterno all'elenco locale del dominio esterno.

7. Andare alla pagina **Vai a elenco/Cerca/Aggiungi utente** per visualizzare gli utenti assegnati a un nuovo dominio esterno.

H — Visualizzazione del login

1. Tornare alla home page di DocuShare.

2. Nella sezione Login della home page, il nuovo dominio esterno dovrebbe essere visualizzato nel menu **Login Domain** (Dominio login).

3. L'utente di un dominio esterno deve selezionare il dominio corretto per il login, in caso contrario in DocuShare verrà visualizzato un messaggio di errore di login e verrà chiesto di riprovare.

LDAP e SSL

Secure Socket Layer (SSL) è un protocollo sviluppato da Netscape per la trasmissione di documenti riservati tramite Internet. SSL funziona utilizzando una chiave pubblica per crittografare i dati trasferiti tramite una connessione SSL. Il protocollo SSL è supportato sia da Netscape Navigator che da Internet Explorer. Numerosi siti Web utilizzano il protocollo SSL per ricevere informazioni riservate da parte degli utenti, ad esempio numeri di carte di credito e password di account. Le sessioni SSL vengono avviate utilizzando un URL che inizia con **https** anziché con **http**.

Certificati

Quando si utilizza SSL, i server e i client utilizzano certificati per comprovare la propria identità prima di stabilire una connessione protetta. I certificati contengono inoltre una chiave privata e una pubblica che vengono utilizzate per stabilire una sessione. I server e i client utilizzano **chiavi di sessione** per crittografare e decrittografare i dati.

I certificati possono essere autofirmati oppure possono essere rilasciati da una CA (Certificate Authority, autorità di certificazione), ad esempio Entrust, Equifax, Valicert o Verisign. I certificati rilasciati da una CA sono considerati come provenienti da una **Autorità di certificazione esterna attendibile**. In pratica, l'autorità esterna garantisce l'identità di un utente. La maggioranza dei browser client è configurata per riconoscere e considerare attendibili i certificati rilasciati dalle CA.

Quando i certificati sono autofirmati, è l'utente stesso ad agire come autorità di certificazione. Un certificato autofirmato deve essere installato nell'archivio certificati del browser e non viene riconosciuto come autorità attendibile di terze parti.

I certificati vengono rilasciati come certificati client o server. DocuShare non supporta i certificati client. DocuShare utilizza una copia del certificato del server LDAP per attivare una sessione SSL con il server LDAP.

Importazione del certificato in DocuShare

A seconda della CA che ha rilasciato il certificato, è possibile che l'amministratore debba importare il certificato dal server LDAP nell'archivio certificati del browser del server DocuShare. Se il certificato è autofirmato, l'amministratore **deve** importare il certificato nell'archivio certificati del browser del server DocuShare.

Per importare il certificato da un server LDAP specifico:

1. Aprire un Web browser sul server DocuShare.
2. Connettersi al server LDAP utilizzando l'indirizzo - https://<your.ldap.server>:636.

   La porta 636 è la porta standard per SSL.
3. Se il certificato non è stato installato nell'archivio certificati del browser del server DocuShare, viene visualizzata una finestra di avviso di protezione in cui viene chiesto di installare il certificato.
4. Per installare il certificato, fare clic su **Visualizza certificato** nella parte inferiore della finestra di avviso di protezione.

   Verrà visualizzata la finestra Certificato.
5. Fare clic sulla scheda **Dettagli**, quindi sul pulsante **Copia su file**.

Esportazione del certificato e salvataggio come file CER

Dopo aver importato il certificato dal server LDAP, è necessario esportarlo nella directory DocuShare e salvarlo come file certificato.

Per esportare il certificato e salvarlo come file certificato:

1. Fare clic su **Avanti** nella parte inferiore della finestra della procedura guidata.

   Se il certificato contiene una chiave privata, viene visualizzata la finestra Esporta la chiave privata con il certificato.

2. Nella finestra Esporta la chiave privata con il certificato, selezionare **Non esportare la chiave privata**.

   DocuShare non richiede una chiave privata per attivare una sessione SSL con il server LDAP.

3. Fare clic su **Avanti**.

   Verrà visualizzata la finestra Formato file di esportazione.

4. Nella finestra Formato file di esportazione, selezionare **Codificato Base 64 X.509 (.CER)**.

5. Fare clic su **Avanti**.

   Viene visualizzata la finestra File da esportare.

6. Nel campo **Nome file**, inserire il percorso della directory dell'unità in cui si desidera esportare il certificato. Ad esempio **D:**.

7. Nel campo Nome file, dietro il percorso della directory, inserire il nome file per il certificato con estensione **.cer**. Ad esempio **D:\SSL_Cert4LDAP.cer**.

8. Fare clic su **Avanti** per completare l'esportazione del certificato.

   Viene visualizzata la finestra di completamento della procedura guidata di esportazione del certificato.

9. Fare clic su **Fine** per chiudere la procedura guidata.

   Il certificato LDAP viene salvato come file .cer nel sito DocuShare.

10. Seguire le istruzioni riportate nella pagina successiva, *Inserimento del certificato in DSTrustStore*.

Inserimento del certificato in DSTrustStore

Una volta salvato il certificato come file certificato, è necessario inserirlo nel file **DSTrustStore**.

Per inserire il file di certificato (.cer) in un file DSTrustStore:

1. Individuare il file .cer esportato utilizzando Esportazione guidata certificati.
2. Copiare il file .cer nella directory DocuShare che contiene il file DSTrustStore **jdk\jre\lib\security**.
3. Aprire una finestra del prompt dei comandi e accedere alla directory che contiene **dstruststore**.

```
C:\>cd\xerox\docushare\jdk\jre\lib\security
C:\Xerox\DocuShare\jdk\jre\lib\security\dir
  Volume in drive C is Local Disk
  Volume in Serial Number is 508B-0D2F
  Directory of C:\Xerox\DocuShare\jdk\jre\lib\security
18-11-02   15:55          <DIR>          -
18-11-02   15:55          <DIR>          --
02-10-02   12:25                   7,365 cacerts
02-10-02   12:26                     589 dstruststore
02-10-02   12:26                   2,271 java.policy
02-10-02   12:26                   4,115 java.security
10-11-02   15:43                     844 SLL_Cert4LDAP.cer
               5 Files(s)         15,184 bytes
               2 Dir(s)    1,486,024,704 bytes free
C:\Xerox\DocuShare\jdk\jre\lib\security
```

4. Al prompt dei comandi, inserire il comando **set PATH** per impostare la variabile di ambiente PATH. Utilizzare il comando set **PATH=%PATH%;**<directory DocuShare>**\jdk\jre\bin**.

```
C:\Xerox\Docushare\jdk\jre\lib\security>set
PATH=%PATH%;C:\XEROX\DocuShare\jdk\jre\bin
```

5. Dopo aver impostato la variabile PATH, al prompt dei comandi inserire **keytool**, senza argomenti.

   Viene visualizzata la guida dell'utilità Keytool. L'utilità Keytool inserisce il certificato SSL nel file DSTrustStore.

6. Al prompt dei comandi, inserire il seguente comando dell'utilità Keytool: “keytool -import -alias <nome_alias> -file <file_cert> -keystore dstruststore”

   Sostituire **<nome_alias>** con un nome univoco per il file del certificato.

   Sostituire **<file_cert>** con il nome del file di certificato (.cer) che è stato esportato e copiato nella directory contenente il file dstruststore.

7. Premere **Invio** per avviare il comando.

   Viene visualizzato un messaggio per chiedere l'inserimento di una password.

8. Inserire **password**, quindi premere **Invio**.

```
C:\Xerox\Docushare\jdk\jre\lib\security>keytool -import -alias Test
LDAPss1 -file SDL_Cert4LDAP.cer -keystore dstruststore

Enter keystore password: password
Owner: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
Issuer: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
Serial number: 5ee8abd44c2cd2b14ffbee159f03d354
Valid from: Tue Feb 19 10:57:21 PST 2012 until: Thu Jan 26 10:57:21
PST 2102
Certificate fingerprints:
          MD5: 78:C7:A3:04:32:69:EB:97:76:FE:F4:8A:11:A2:65:26
          SHA1:
02:DD:9A:BE:BE:DE:3C:AA:22:AE:14:9A:F2:F2:5B:11:61:6D:5A:5F
Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Xerox\DocuShare\jdk\jre\lib\security>
```

9. Esaminare il contenuto della schermata per assicurarsi che Keytool abbia aggiunto correttamente il certificato al keystore. Se Keytool ha completato l'operazione, il server DocuShare è pronto per utilizzare il certificato per attivare una sessione SSL con il server LDAP.
10. Dopo aver importato il certificato, riavviare il server DocuShare.

Active Directory Administration Tool

È possibile utilizzare Active Directory Administration Tool (ldp.exe) per eseguire varie operazioni su Active Directory e inviare query a un server di directory LDAP.

Per utilizzare ldp.exe per connettersi a un server LDAP abilitato per SSL, è necessario innanzitutto abilitare il certificato SSL sul server DocuShare. Per importare e caricare un certificato SSL, seguire le istruzioni su **LDAP** e **SSL** nel *Capitolo 2* di questa guida.

Il comando ldp.exe è incorporato in Windows Server 2008 e Windows Server 2012. Il comando ldp.exe è disponibile se è installato il ruolo server Servizi di dominio Active Directory (Active Directory completo).

Per avviare ldp.exe:

1. Nella pagina **Start** del server, fare clic su **Esegui**.
2. Digitare **ldp**.
3. Fare clic su **OK**.

Utilizzo di Active Directory Administration Tool

È possibile utilizzare Active Directory Administration Tool per raccogliere le informazioni sul server LDAP necessarie per configurare il sito DocuShare per utilizzare il server per domini esterni. Seguire le procedure dalla A alla F.

Nota: questa procedura è basata sull'utilizzo dello strumento per la raccolta di informazioni da una configurazione tipica di server LDAP. Sono possibili variazioni, in base al modo in cui è stato configurato il server.

A — Connessione

1. Selezionare **Connection** sulla barra di spostamento di Active Directory Administration Tool, quindi selezionare **Connect** dal menu Connection.

   Viene visualizzata la finestra di dialogo Connect.
2. Nel campo **Server**, inserire l'indirizzo IP o il nome DNS del server Active Directory LDAP.
3. Nel campo **Port**, inserire il numero di porta utilizzato, se diverso da quello predefinito visualizzato.
4. Fare clic su **OK**.

   A questo punto, l'indirizzo del server LDAP e il numero di porta sono impostati.

B — Associazione

Dopo aver impostato la connessione al server LDAP, è necessario associare il server a un account amministrativo che disponga dell'autorizzazione ad accedere ed effettuare ricerche nella directory.

1. Selezionare **Connection** sulla barra di spostamento di Active Directory Administration Tool, quindi selezionare **Bind** dal menu Connection.

   Viene visualizzata la finestra di dialogo Bind.

2. Inserire il nome dell'account utente nel campo **User**, la password nel campo **Password** e il dominio nel campo **Domain**.
3. Fare clic su **OK**.

   Dopo aver effettuato la connessione e creato un'associazione al server LDAP, viene visualizzato un **testo di risposta del server nel riquadro destro** di Active Directory Administration Tool.

C — Individuazione del nome distinto di base

Il DN di base sarà il punto di partenza per l'analisi della struttura di directory.

1. Cercare un riferimento a **namingContext** nel testo di risposta visualizzato nel riquadro destro di Active Directory Administration Tool.

   Il formato del namingContext varia in base al server LDAP utilizzato.
2. Il testo evidenziato è il nome distinto di base per la directory principale DIT.

   Ad esempio, il DN di base evidenziato potrebbe essere **dc=adoc,dc=Xerox,dc=com**. Il DN di base effettivo potrebbe variare in base alle singole strutture di directory LDAP. Annotare queste informazioni per utilizzi futuri.

D — Visualizzazione della directory principale DIT

1. Selezionare **View** sulla barra di spostamento di Active Directory Administration Tool, quindi selezionare **Tree** dal menu View.

   Viene visualizzata la finestra di dialogo View.
2. Nel campo **BaseDN**, inserire il **nome distinto di base** trovato nella ricerca namingContext descritta sopra.
3. Fare clic su **OK**.

   La directory principale DIT per il server LDAP è visualizzata nel riquadro sinistro della finestra di Active Directory Administration Tool.
4. Esaminare la struttura per stabilire dove si troverà la directory principale DIT per i domini DocuShare esterni che si desidera creare.

   La directory principale dovrebbe trovarsi a un livello sufficientemente alto nella gerarchia in modo da includere tutti i rami (quali organizationUnit e domainComponents) che avranno accesso al server DocuShare.

   Nel nostro esempio si utilizzerà dc=adoc, dc=xerox,dc=com come directory principale DIT per includere soltanto gli utenti presenti nel dominio ADOC e non tutti gli utenti in Xerox.com.

E — Individuazione dell'account agente

Nella maggior parte dei casi, una Active Directory non accetta query anonime effettuate nella directory. Eseguire query nel server richiede l'utilizzo di un account agente o di un account di servizio. Utilizzare il comando Search per individuare il DN dell'account agente.

1. Selezionare **Browse** sulla barra di spostamento di Active Directory Administration Tool, quindi selezionare Search dal menu Browse.

   Viene visualizzata la finestra di dialogo Search.

2. Inserire un DN di base nel campo **Base DN**.

   In base al valore utilizzato per il DN di base e alla posizione dell'account agente all'interno della gerarchia, potrebbe essere necessario selezionare Subtree per espandere l'ambito della ricerca.

3. Inserire un filtro nel campo **Filter**.

   Per il filtro è stato utilizzato l'attributo sAMAccoutName in quanto si sapeva il nome di login dell'account agente. Questo attributo è univoco di Active Directory ed è un residuo di Windows NT. Se si avesse saputo il commonName (cn) dell'account si avrebbe utilizzato commonName=Peter Pan, ad esempio. Un server iPlanet può utilizzare l'uid o l'attributo commonName (cn).

4. Selezionare l'**ambito** della ricerca.

   Selezionare **Subtree** se l'opzione **One Level** non è sufficiente.

5. Fare clic su **Run**.

   I risultati della ricerca vengono visualizzati come testo nel riquadro destro della finestra di Active Directory Administration Tool. Ad esempio, una ricerca potrebbe mostrare che il **distinguishedName** per l'account utente è cn=TestUser1,cn=users,dc=adoc,dc=xerox,dc=com.

F — Passaggio successivo

Dopo aver eseguito le procedure dalla A alla E, dovrebbe essere possibile utilizzare Active Directory Administration Tool per raccogliere le informazioni necessarie alla configurazione del sito DocuShare per l'utilizzo di LDAP per l'autenticazione degli account utente.

- L'indirizzo IP o il nome DNS del server LDAP
- La directory principale DIT
- L'account agente per DocuShare

Il comando LDIFDE di Active Directory

È possibile utilizzare il comando **LDIFDE** per scrivere in un file di testo il contenuto dell'intera directory LDAP o di un dominio specifico all'interno della directory LDAP. Questo file di testo contiene la maggior parte delle informazioni necessarie alla configurazione di DocuShare per l'utilizzo con LDAP.

Il file di testo generato da LDIFDE è il file principale utilizzato dal Supporto DocuShare per la risoluzione di problemi di configurazione LDAP.

LDIFDE è uno strumento della riga di comando incorporato in Windows Server 2008 e Windows Server 2012. Lo strumento è disponibile se è installato il ruolo server Servizi di dominio Active Directory (Active Directory completo) o AD LDS (Active Directory Lightweight Directory Services).

Per utilizzare LDIFDE, è necessario eseguire il comando LDIFDE da un prompt dei comandi con privilegi elevati. Per aprire un prompt dei comandi con privilegi elevati, fare clic su Start e poi fare clic con il pulsante destro del mouse sul prompt dei comandi, quindi scegliere **Esegui come amministratore**.

Nota: per ulteriori informazioni sull'utilizzo del comando LDIFDE, visitare http://technet.microsoft.com/en-us/library/cc731033.aspx

Sintassi e utilizzo del comando LDIFDE

Per utilizzare il comando LDIFDE, aprire una finestra del prompt dei comandi sul server LDAP e digitare **C:\Windows\system32>idifde -?** Premere **Invio**. LDIFDE restituisce quanto segue:

```
LDIF Directory Exchange


General Parameters

==================

-i Turn on Import Mode (The default is Export)

-f filename Input or Output filename

-s servername The server to bind to (Default to DC of computer's in
Domain)

-c FromDN ToDN Replace occurences of FromDN to ToDN

If either FromDN or ToDN ends with #attributeName, the attribute
value will be looked up in rootDSE and used to replace
#attributeName.  See example for "Macro expansion in DNs"

-v Turn on Verbose Mode

-j Log File Location

-t Port Number (default = 389)

-u Use Unicode format

-w timeout Terminate execution if the server takes longer than the
specified number of seconds to respond to an operation (default = no
timeout specified)

-h Enable SASL layer signing and encryption

-? Help
```

```
Export Specific
===============
-d RootDN The root of the LDAP search (Default to Naming Context)
-r Filter LDAP search filter (Default to "(objectClass=*)")
-p SearchScope Search Scope (Base/OneLevel/Subtree)
-l listList of attributes (comma separated) to look for in an LDAP
search
-o listList of attributes (comma separated) to omit from input
-g Disable Paged Search
-m Enable the SAM logic on export
-n Do not export binary values
-x Include deleted objects (tombstones)
-1 Retain only the important replPropertyMetadata

Import
======
-k The import will go on ignoring 'Constraint Violation' and 'Object
Already Exists' errors
-y The import will use lazy commit for better performance (enabled by
default)
-e The import will not use lazy commit
-q threads The import will use the specified number of threads
(default is 1)
-z Continue importing irrespective of errors
-x Enable tombstone reanimation support (passes deleted objects
control with ldap modify requests)

Credentials Establishment
=========================
Note that if no credentials is specified, LDIFDE will bind as the
currently
logged on user, using SSPI.

-a UserDN [Password | *]Simple authentication
-b UserName Domain [Password | *]SSPI bind method

Example: Simple import of current domain
    ldifde -i -f INPUT.LDF
```

```
Example: Simple export of current domain
    ldifde -f OUTPUT.LDF

Example: Export of specific domain with credentials
    ldifde -m -f OUTPUT.LDF
           -b USERNAME DOMAINNAME *
           -s SERVERNAME
           -d "cn=users,DC=DOMAINNAME,DC=Microsoft,DC=Com"
           -r "(objectClass=user)"

Example: Macro expansion in DNs
    ldifde -f export.ldf -c "#configurationNamingContext"
"cn=configuration,dc=x"
    ldifde -i -f import.ldf -c "cn=configuration,dc=x"
"#configurationNamingContext"

No log files were written.  In order to generate a log file, please
specify the log file path via the -j option.
```

Esempio di comando LDIFDE

Il seguente è un esempio di comando LDIFDE che scrive il contenuto di Active Directory su un server denominato Corvette in un file di testo denominato **adexport.txt**.

Esecuzione del comando LDIFDE:

Digitare il comando **C:\Windows\system32\LDIFDE.exe -f adexport.txt -s corvette** e premere **Invio**.

```
The command runs and displays its progress:
Connecting to "corvette"
Logging in as current user using SSPI
Exporting directory to file adexport.txt
Searching for entries...
Writing out
entries.....................................................

132 entries exported

The command has completed successfully
```

Il file adexport.txt generato

Di seguito è riportato il contenuto del file adexport.txt generato nell'esempio dal comando FDIFDE. Questo esempio mostra solo una parte del contenuto complessivo del file. Esaminare attentamente gli elementi evidenziati in grassetto: si tratta degli elementi necessari alla configurazione di DocuShare per l'utilizzo con questo server LDAP.

dn: DC=infodev,DC=xcm,DC=xerox,DC=com

changetype: add

masteredBy:CN=NTDS Settings, CN=CORVETTE, CN=Servers, CN=infodev-xcm-site, CN=Sites, CN=Configuration, DC=infodev, DC=xcm, DC=xerox, DC=com

auditingPolicy:: AAE=

creationTime: 127199619543431088

dc: infodev

forceLogoff: -9223372036854775808

fSMORoleOwner:CN=NTDS Settings, CN=CORVETTE, CN=Servers, CN=infodev-xcm-site, CN=Sites, CN=Configuration, DC=infodev, DC=xcm, DC=xerox, DC=com

- l
- l
- l

[Sample Directory Record for a single User]

dn: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=xcm, DC=xerox, DC=com

changetype: add

accountExpires: 9223372036854775807

badPasswordTime: 0

badPwdCount: 0

codePage: 0

cn: Duncan Donkey

countryCode: 0

displayName: Duncan Donkey

mail: ddonkey@infodev.xerox.com

givenName: Duncan

instanceType: 4

lastLogoff: 0

lastLogon: 0

logonCount: 0

distinguishedName: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=xcm, DC=xerox, DC=com

objectCategory:CN=Person, CN=Schema, CN=Configuration, DC=infodev, DC=xcm, DC=xerox, DC=com

objectClass: user

objectGUID:: xmi02W78lEmpYca7AtiupQ==

objectSid:: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0bgQAAA==

primaryGroupID: 513

pwdLastSet: 127293917905389760

name: Duncan Donkey

sAMAccountName: duncan

sAMAccountType: 805306368

sn: Donkey

userAccountControl: 512

userPrincipalName: duncan@infodev.xcm.xerox.com

uSNChanged: 7353

uSNCreated: 7349

whenChanged: 20140518220950.0Z

whenCreated: 20140518220933.0Z

-
-
-

[Sample Directory Record for a Group]

dn: CN=labusers,CN=Users,DC=infodev,DC=xcm,DC=xerox,DC=com

changetype: add

member: CN=Greg Wong,CN=Users,DC=infodev,DC=xcm,DC=xerox,DC=com

member: CN=Janet Gilmore,CN=Users,DC=infodev,DC=xcm,DC=xerox,DC=com

member: CN=Jennings\, Ferris,CN=Users,DC=infodev,DC=xcm,DC=xerox,DC=com

member: CN=Cua\, Kiam T,CN=Users,DC=infodev,DC=xcm,DC=xerox,DC=com

info: Authorized Login User to the InforDev Lab

cn: labusers

description: InfoDev Lab Users

groupType: -2147483644

instanceType: 4

distinguishedName:CN=labusers, CN=Users, DC=infodev, DC=xcm, DC=xerox, DC=com

objectCategory: CN=Group, CN=Schema, CN=Configuration, DC=infodev, DC=xcm, DC=xerox, DC=com

objectClass: group

objectGUID:: Cm9phZkOn0ig4iEWMRPWsg==

objectSid:: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0VgQAAA==

name: labusers

sAMAccountName: labusers

sAMAccountType: 536870912

uSNChanged: 3975

uSNCreated: 2540

whenChanged: 20140302161513.0Z

whenCreated: 20140130190128.0Z

Analisi del contenuto del file adexport.txt

Nell'esempio, il file adexport.txt utilizza il nome distinto (DN) per Duncan Donkey, un membro del team Digital Actors nel reparto InfoDev di XCM di Xerox Corporation.

Nell'esempio, il DN per Duncan Donkey è definito nel modo seguente: **CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=xcm, DC=xerox, DC=com**

Esaminando il nome distinto di un utente è possibile trovare le informazioni necessarie per identificare quanto segue:

a. La directory principale DIT (Directory Information Tree)
b. La chiave RDN utente
c. Localizzatore autenticazione relativa e Localizzatore servizi directory relativi
d. Gli attributi di associazione utente
e. Gli attributi di associazione gruppo

A — La directory principale DIT (Directory Information Tree)

Impostare la directory principale DIT su un livello della struttura di directory che includa tutti i rami della directory che contengono utenti con la necessità di accedere al server DocuShare. Nell'esempio, soltanto i membri dell'organizzazione XCM di Xerox avranno accesso al server DocuShare.

L'organizzazione XCM comprende diversi reparti e team all'interno di ciascun reparto. Tali reparti e team sono organizzati nella directory LDAP in base a componenti del dominio (DC, Domain Components) e unità organizzative (OU, Organizational Units). Nell'esempio verrà impostato un dominio esterno in DocuShare per autenticare gli utenti che sono membri del team Digital Actors nel reparto InfoDev di XCM all'interno di Xerox Corporation.

In questo esempio, la directory principale DIT del valore DN per Duncan Donkey viene mostrata in grassetto: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, **DC=xcm, DC=xerox, DC=com**

Definendo la directory principale DIT a questo livello della gerarchia è possibile creare domini esterni per ciascun reparto/team all'interno dell'organizzazione XCM.

B — La chiave RDN utente

La chiave RDN utente è l'alias dell'attributo utilizzato per identificare l'utente.

In questo esempio, la chiave RDN utente del valore DN per Duncan Donkey viene mostrata in grassetto: **CN=Duncan Donkey**, OU=Digital, OU=Actors, DC=infodev, DC=xcm, DC=xerox, DC=com

C — Localizzatore autenticazione relativa e Localizzatore servizi directory relativi

Il Localizzatore autenticazione relativa e il Localizzatore servizi di directory relativi sono i puntatori al ramo della directory del dominio esterno contenente un gruppo, un utente o utenti specifici.

In questo esempio, il Localizzatore autenticazione relativa e il Localizzatore servizi directory relativi vengono mostrati in grassetto: CN=Duncan Donkey, **OU=Digital, OU=Actors, DC=infodev**, DC=xcm, DC=xerox, DC=com.

D — Gli attributi di associazione utente

Il file di testo generato dal comando FDIFDE contiene gli alias degli attributi utilizzati per identificare il cognome, il nome utente e l'indirizzo e-mail di ciascun utente elencato. Utilizzare questi alias degli attributi per configurare le proprietà di associazione utente LDAP DocuShare. Nel file di testo del comando FDIFDE, gli utenti presenti nella directory LDAP sono identificati tramite la voce **objectClass: user**.

Nell'esempio, sono mostrati gli alias degli attributi LDAP per le seguenti proprietà:

Cognome = **sn**

Nome utente = **sAMAccountName**

Indirizzo e-mail = **mail**

I valori assegnati a questi alias degli attributi LDAP nell'esempio sono:

sn: Donkey

sAMAccountName: duncan

mail: ddonkey@infodev.xerox.com

E — Gli attributi di associazione gruppo

Il file di testo generato dal comando FDIFDE contiene gli alias degli attributi utilizzati per identificare il nome, la descrizione e le informazioni riassuntive di ciascun gruppo elencato. Questi alias degli attributi verranno utilizzati per configurare le proprietà di associazione gruppo LDAP DocuShare.

Nel file di testo del comando FDIFDE, i gruppi presenti nella directory LDAP sono identificati tramite la voce **objectClass: group**.

Nell'esempio si trovano gli **alias degli attributi LDAP** per le seguenti proprietà:

Nome = **cn**

Descrizione = **description**

Riassunto = **info**

I valori assegnati a questi alias degli attributi LDAP nell'esempio sono:

cn: labusers

description: InfoDev Lab Users

info: Authorized Login User to the InfoDev Lab

3 Sincronizzazione LDAP/DocuShare

Domande frequenti sulla sincronizzazione LDAP/DocuShare

Domanda: Come è possibile impostare il controllo di accesso a un sito in modo da consentire solo a determinati utenti di connettersi?

Risposta: Vedere Impostazione del controllo di accesso per gli utenti a pagina 29 e Impostazione del controllo della privacy per gli utenti a pagina 29

Domanda: Come è possibile impostare il controllo di accesso a un sito in modo da consentire solo a determinati membri di un gruppo di connettersi?

Risposta: Vedere Impostazione del controllo di appartenza ai gruppi per gli utenti a pagina 29

Domanda: Come è possibile impostare DocuShare in modo che le informazioni sugli account del sito vengano aggiornate quando vengono modificate sul server LDAP?

Risposta: Vedere Effetti sull'accesso dell'utente quando è selezionata l'opzione Abilita listener a pagina 31

Domanda: Se si abilita Listener in un sito DocuShare, cosa succede quando si riavvia DocuShare?

Risposta: Vedere Effetti sull'avvio di DocuShare quando è selezionato il servizio Listener a pagina 31

Domanda: Come è possibile impostare DocuShare in modo da aggiornare le nuove informazioni sugli account quando un utente si connette al sito?

Risposta: Vedere Opzione Abilita all'accesso selezionata a pagina 32 e Opzione Abilita all'accesso non selezionata a pagina 32

Domanda: Come è possibile aggiornare DocuShare in modo da riflettere l'aggiunta di un utente come membro di un gruppo?

Risposta: Vedere Opzione Abilita sincronizzazione di gruppo selezionata a pagina 32 e Opzione Abilita sincronizzazione di gruppo non selezionata a pagina 33

Domanda: Cosa può causare ritardi frequenti nell'aggiornamento delle modifiche apportate sul server LDAP?

Risposta: Vedere Effetti sull'avvio di DocuShare quando è selezionato il servizio Listener – Problemi di sincronizzazione a pagina 31

Informazioni sulle impostazioni del controllo di autenticazione LDAP

Utilizzare la pagina **Gestione account l Account LDAP l Configurazione l Avanzate** del menu di amministrazione DocuShare per impostare i controlli utilizzati per filtrare l'accesso degli utenti a un sito DocuShare.

Durante l'autenticazione, un utente che esegue un tentativo di accesso deve soddisfare **tutti** i filtri di controllo abilitati, altrimenti gli verrà negato l'accesso al sito.

Impostazione del controllo di accesso per gli utenti

Selezionare **Abilita controllo di accesso per gli utenti** e inserire un filtro per definire gli utenti autorizzati ad accedere al sito DocuShare. La sintassi del filtro segue il formato di query LDAP standard e consente di eseguire il filtraggio utilizzando attributi utente LDAP, ad esempio cn.

Ad esempio, se si sceglie **Abilita controllo di accesso per gli utenti** e si inserisce **cn=Tom*** nel campo **Filtro**, un utente che cerca di accedere usando i valori DN di cn=John Smith,ou=marketing,dc=Xerox,dc=com non sarà in grado di farlo perché il valore cn (nome comune) di questo utente non soddisfa il filtro, ovvero il nome (o cn) non inizia con Tom.

Impostazione del controllo della privacy per gli utenti

Selezionare **Abilita controllo privacy utenti** e inserire un filtro per definire gli utenti autorizzati ad accedere al sito DocuShare. Anche la sintassi di questo filtro segue il formato di query LDAP standard e consente di eseguire il filtraggio utilizzando attributi di utente LDAP.

Ad esempio, se si sceglie **Abilita controllo privacy utenti** e si inserisce **mail=*acme.org*** nel campo **Filtro**, un utente che cerca di accedere usando un attributo e-mail di acme.com non sarà in grado di farlo perché l'attributo e-mail di questo utente non soddisfa il filtro, ovvero l'indirizzo e-mail non contiene acme.org.

Tra l'attributo di controllo della privacy degli utenti e l'attributo di controllo di accesso per gli utenti esiste una relazione di tipo AND (e). Se entrambi gli attributi sono selezionati e vi vengono applicati dei filtri, un utente che tenta di accedere a un sito DocuShare deve soddisfare **entrambi** i filtri prima di essere autorizzato ad accedere al sito.

Impostazione del controllo di appartenza ai gruppi per gli utenti

Selezionare **Abilita controllo appartenenza utenti** e inserire un filtro per definire il/i gruppo/i a cui un utente deve appartenere come membro per essere autorizzato ad accedere al sito DocuShare. Se questo controllo viene utilizzato insieme al controllo di accesso o al controllo della privacy degli utenti (o ad entrambe le voci), un utente che tenta di accedere a un sito deve soddisfare i filtri di **tutti** i controlli abilitati.

Ad esempio, se si sceglie **Abilita controllo appartenenza utenti** e si inserisce **(l(childOf =CN=GROUP1,OU=marketing,DC=docushare,DC=Xerox,DC=com)(descendantOf= CN=GROUP2,OU=marketing,DC=docushare,DC=Xerox,DC=com))** nel campo **Filtro**, un utente che cerca di accedere senza essere un membro di Group1 (gruppo 1) e non un discendente di Group2 (gruppo 2) non sarà in grado di farlo.

Nota: se la mappatura del titolo del gruppo non è definita sulla pagina Gestione account l Account LDAP l Associa gruppo, DocuShare imposta automaticamente su "cn" l'attributo LDAP per il titolo del gruppo.

Tabella dei filtri di controllo dell'appartenenza degli utenti

Filtro	Uso, attributo ed esempio
childOf =	(childOf = DN del gruppo) L'utente che tenta di accedere deve essere un membro diretto di un gruppo specifico (childOf = CN=Group1,OU=marketing,DC=docushare,DC=Xerox,DC=com) L'utente deve essere un membro di Group1 (gruppo 1):
descendantOf =	(descendantOf = DN del gruppo) L'utente che tenta di accedere deve essere un membro discendente di una voce specifica di group descendantOf = CN=Group2,OU=marketing,DC=docushare,DC=Xerox,DC=com) L'utente deve essere un discendente di Group 2 (gruppo 2).
OR	Relazione OR di più gruppi L'utente che tenta di accedere deve essere un membro di almeno uno dei gruppi specificati (l(childOf = CN=Group1,OU=marketing,DC=docushare,DC=Xerox,DC=com)(descendantOf = CN=Group2,OU=marketing,DC=docushare,DC=Xerox,DC=com)) L'utente deve essere un membro di Group 1 (gruppo 1) o un discendente di Group 2 (gruppo 2). NOTA: gli operandi AND e OR non possono essere utilizzati nello stesso filtro.
AND	Relazione AND (E) di più gruppi L'utente che tenta di accedere deve essere un membro di tutti i gruppi definiti (&(childOf = CN=Group1,OU=marketing,DC=docushare,DC=Xerox,DC=com)(descenda ntOf = CN=Group2,OU=marketing,DC=docushare,DC=Xerox,DC=com)) L'utente deve essere un membro di Group 1 (gruppo 1) E un discendente di Group 2 (gruppo 2). NOTA: gli operandi AND e OR non possono essere utilizzati nello stesso filtro.

Informazioni sul servizio Listener

L'opzione **Abilita listener** è disponibile per ciascun dominio DocuShare.

Effetti sull'accesso dell'utente quando è selezionata l'opzione Abilita listener

Se in **Gestione account l Domini** è selezionata l'opzione **Abilita listener**, DocuShare esegue il servizio listener nel back-end del sistema. Quando sul server LDAP viene eseguito un aggiornamento per un account, DocuShare aggiorna le informazioni sul sito locale con le informazioni aggiornate trovate sul server LDAP.

Una volta selezionata, l'opzione Abilita listener annulla le impostazioni di Abilita all'accesso e Abilita sincronizzazione di gruppo, così il sistema non esegue la sincronizzazione all'accesso. Quando l'opzione Abilita listener è selezionata, gli account DocuShare vengono aggiornati in tempo reale mentre vengono eseguiti aggiornamenti sul server LDAP.

Effetti sull'avvio di DocuShare quando è selezionato il servizio Listener

Se in **Gestione account l Domini** è selezionata l'opzione **Abilita listener**, il servizio directory esegue una sincronizzazione tra DocuShare e il server LDAP all'avvio di DocuShare.

Durante la sincronizzazione, il sevizio listener interroga il server LDAP per ottenere eventuali aggiornamenti di account disponibili dall'ultima chiusura del server DocuShare. I risultati della query non includono gli account utente o di gruppo eliminati da LDAP durante il riavvio di DocuShare. I record degli account eliminati rimangono nel registro di sistema di DocuShare fino al successivo riavvio di DocuShare o alla sincronizzazione manuale di DocuShare con LDAP eseguita utilizzando **Gestione account l Account LDAP l Sincronizza**.

Problemi di sincronizzazione

Per la query di avvio si presuppone che l'orario del server LDAP sia sincronizzato con l'orario del server DocuShare. Se l'orologio del server LDAP è impostato su un'ora precedente rispetto all'orologio del server DocuShare, alcuni aggiornamenti potrebbero non essere comunicati immediatamente al server DocuShare. Se l'orologio del server LDAP è impostato su un'ora successiva rispetto all'orologio del server DocuShare, la comunicazione degli aggiornamenti al server DocuShare viene eseguita correttamente.

Informazioni sull'intervallo di sincronizzazione LDAP

L'intervallo di sincronizzazione LDAP dipende dalla configurazione di LDAP.

Se in **Gestione account l Domini**, l'opzione **Abilita listener** non è selezionata per un determinato dominio LDAP, l'intervallo di sincronizzazione LDAP dipende dalla configurazione delle impostazioni di **Abilita all'accesso** e **Abilita sincronizzazione di gruppo**.

Nota: una volta selezionata, l'opzione Abilita listener annulla le impostazioni di Abilita all'accesso e Abilita sincronizzazione di gruppo, così il sistema non esegue la sincronizzazione all'accesso mentre è abilitato Listener.

Opzione Abilita all'accesso selezionata

In corrispondenza di **Gestione account l Account LDAP l Configurazione l Avanzate** dell'area **Sincronizzazione l Utente**, la casella di controllo **Abilita all'accesso** è selezionata.

Azione: quando un utente si connette a un sito, DocuShare comunica con il server LDAP per ricevere eventuali aggiornamenti di attributi/proprietà che sono stati eseguiti per quell'account utente sul server LDAP. Finché l'utente non si connette a DocuShare, le proprietà dell'account utente non vengono aggiornate con le modifiche apportate a quell'account sul server LDAP.

Quando un utente accede a DocuShare, il sistema confronta l'ora di accesso corrente con il valore di data e ora dell'ultima sincronizzazione LDAP. Se il confronto mostra una differenza temporale inferiore ai 20 minuti, il sistema non sincronizza le informazioni dell'utente su DocuShare con le informazioni dell'utente sul server LDAP.

Esempio: l'attributo e-mail di un account utente viene modificato sul server LDAP. Quando un utente si connette a DocuShare, il sistema comunica con il server LDAP e modifica la proprietà e-mail DocuShare di quell'utente in modo che corrisponda al nuovo attributo e-mail LDAP.

Opzione Abilita all'accesso non selezionata

In corrispondenza di **Gestione account l Account LDAP l Configurazione l Avanzate** dell'area **Sincronizzazione l Utente**, la casella di controllo **Abilita all'accesso** non è selezionata.

Azione: se la casella Abilita all'accesso non è selezionata, la sincronizzazione di proprietà DocuShare/attributo LDAP non viene eseguita all'accesso. In questo caso, per sincronizzare le informazioni sull'account, accedere a **Gestione account l Account LDAP l Sincronizza** ed eseguire manualmente la sincronizzazione.

Opzione Abilita sincronizzazione di gruppo selezionata

In corrispondenza di **Gestione account l Account LDAP l Configurazione l Avanzate** dell'area **Sincronizzazione l Gruppo**, la casella di controllo **Abilita sincronizzazione di gruppo** è selezionata.

Azione: quando un utente si connette a un sito, DocuShare comunica con il server LDAP per ricevere eventuali modifiche di appartenenza al gruppo apportate a quell'account utente sul server LDAP. Finché l'utente non si connette a DocuShare, l'appartenenza al gruppo non viene aggiornata con le modifiche apportate a quell'account sul server LDAP.

Finché l'utente non si connette a DocuShare, le appartenenze ai gruppi DocuShare dell'account utente non vengono aggiornate con le modifiche apportate alle appartenze ai gruppi sul server LDAP.

Esempio: sul server LDAP, un utente viene aggiunto al gruppo 15. Quando quell'utente si connette a DocuShare, il sistema comunica con il server LDAP e aggiunge l'utente al gruppo 15 nel registro di sistema DocuShare.

Opzione Abilita sincronizzazione di gruppo non selezionata

Se la casella Abilita sincronizzazione di gruppo non è selezionata, la sincronizzazione dell'appartenza ai gruppi non viene eseguita all'accesso. In questo caso, per sincronizzare le informazioni sull'appartenza ai gruppi, accedere a **Gestione account l Account LDAP l Sincronizza** ed eseguire manualmente la sincronizzazione.