Subject: opends e sunds
Posted by Matteo Rossini on Tue, 21 Jun 2011 09:09:19 GMT
View Forum Message <> Reply to Message

Salve.
Ho un ldap SunDS installato su una macchina.
Ora devo installare un altro server con un ldap free; pensavo ad OpenDS (ma anche 389-directory server, di fedora) per la maggiore compatibilitÃ trovata con SunDS.

Poi ho bisogno di mettere i due in replica, per la precisione l'OpenDS va messo come consumer di SunDS (quindi l'OpenDS sarebbe in read-only).

Finora non sono riuscito a configurare tale replica e su google non sono riuscito a trovare niente.

Qualcuno sa se e come si puÃ² fare?

Grazie,
Matteo

Subject: Re: opends e sunds
Posted by Enrico 'Henryx' Bianc on Tue, 21 Jun 2011 22:39:06 GMT
View Forum Message <> Reply to Message

Matteo Rossini wrote:

> Qualcuno sa se e come si puÃ² fare?

Non si fa, in quanto sono due prodotti differenti. E` un po' come voler replicare un database PostgreSQL con un database MySQL senza mettere qualcosa di veramente agnostico (e specifico) in mezzo. Personalmente ti consiglio di migrare tutta la tua directory LDAP su di un altro prodotto, e con quest'ultimo eseguire la replica

Enrico
P.S. OpenDS e` considerato morto anche in virtu` del fatto che Oracle non lo considera un prodotto strategico. Se sei comunque interessato ad usare questo prodotto, usa OpenDJ, che ne e` il fork e che e` attivamente sviluppato (l'ultima release, la 2.4.3, e` stata rilasciata il 17/06/2011)

Subject: Re: opends e sunds
Posted by Matteo Rossini on Wed, 22 Jun 2011 08:52:44 GMT

Il directory server SunDS Ã¨ stato scelto per la piattaforma,
all'inizio dello scorso anno, non da me (non so se sono stati gli
sviluppatori o chi; a suo tempo poi devo dire che ero ignorante in
materia di DS, il che non Ã¨ buona cosa per mettere in piedi una
piattaforma che si basa su di esso).
Ora abbiamo bisogno di una copia dell'ldap in sola lettura.
Fortunatamente in mancanza di repliche posso permettermi un
allineamento non in realtime (export/import notturno).

L'opzione di cambiare ldap Ã¨ pura utopia anche se l'ambiente non fosse
in produzione (comporterebbe la riscrittura di metÃ o forse piÃ¹ degli
applicativi, verificare se Ã¨ ufficialmente supportato dai prodotti
proprietari che usiamo, e mesi di test funzionali e prestazionali
dell'intera piattaforma...! no! giÃ ci sono voluti mesi per migrare la
piattaforma su hardware piÃ¹ potente di quello iniziale, ma comunque
stesso tipo di hardware e stessa distribuzione (ad eccezione del
database, passato da aix a redhat).

Ora non mi resta che aspettare la prossima settimana che torna lo
sviluppatore dalle ferie e tirargli le orecchie per aver consigliato
OpenDS (noi stavamo puntanto su "389-directory server" di fedora;
stavamo cercando il DS che meglio poteva importare lo schema -
99user.ldif per intenderci). Tale sviluppatore ha detto che OpenDS si
puÃ² anche mettere in replica con SunDS (ma ce lo ha solo accennato...;
mi sembra strano perÃ², non so se lo ha provato; questo Ã¨ tra gli
sviluppatori in gamba e autorevole - mezza piattaforma Ã¨ sviluppata da
lui... e funziona discretamente - e mi sembra strano che abbia preso
una tale toppa).

VabbÃ©, intanto provo OpenDJ e vedo se importa meglio il 99user.ldif
(OpenDS mi ha dato qualche problema con un paio di attributi, 389-
directory server mi sembra di no, ma ho fatto prove superficiali), poi
vedremo il da farsi.

Grazie,
Matteo

Subject: Re: opends e sunds
Posted by Enrico 'Henryx' Bianc on Wed, 22 Jun 2011 23:16:06 GMT

Matteo Rossini wrote:

> Fortunatamente in mancanza di repliche posso permettermi un

> allineamento non in realtime (export/import notturno).

Domanda mia: SunDS non supporta le repliche? Quali sarebbero i problemi nel creare una seconda macchina con questo prodotto?

> (comporterebbe la riscrittura di metÃ o forse piÃ¹ degli
> applicativi, verificare se Ã¨ ufficialmente supportato dai prodotti
> proprietari che usiamo, e mesi di test funzionali e prestazionali
> dell'intera piattaforma...!

Errato, in quanto la dipendenza lato applicativo verso il server LDAP e` meno sentita rispetto a quella che si avrebbe utilizzando un RDBMS. Per spiegarmi meglio, devi considerare che LDAP e` un protocollo stanrdard, di conseguenza la differenza fra i vari server in circolazione non e` basata su come tale standard e` implementato, ma sulle caratteristiche di gestione dei dati salvati nella directory

> no! giÃ ci sono voluti mesi per migrare la
> piattaforma su hardware piÃ¹ potente di quello iniziale,

Personalmente farei una prova, anche informale

> (noi stavamo puntanto su "389-directory server" di fedora;
> stavamo cercando il DS che meglio poteva importare lo schema -
> 99user.ldif per intenderci).

Se quello schema funziona con 389ds, e quello schema e` essenziale per i vostri scopi, allora ti consiglio vivamente la migrazione

> Tale sviluppatore ha detto che OpenDS si
> puÃ² anche mettere in replica con SunDS (ma ce lo ha solo accennato...;

Perche` sul wiki di OpenDS e` scritto chiaramente che nelle future versioni avrebbero supportato le repliche con SunDS

> VabbÃ©, intanto provo OpenDJ e vedo se importa meglio il 99user.ldif
> (OpenDS mi ha dato qualche problema con un paio di attributi, 389-
> directory server mi sembra di no, ma ho fatto prove superficiali), poi
> vedremo il da farsi.

La strada e` quella, togliete SunDS e passate a qualcos'altro che meglio si adatta alle vostre esigenze

Enrico

Subject: Re: opends e sunds

> Domanda mia: SunDS non supporta le repliche? Quali sarebbero i problemi nel
> creare una seconda macchina con questo prodotto?
>
licenze

> > (comporterebbe la riscrittura di metÃ o forse piÃ¹ degli
> > applicativi, verificare se Ã¨ ufficialmente supportato dai prodotti
> > proprietari che usiamo, e mesi di test funzionali e prestazionali
> > dell'intera piattaforma...!
>
> Errato, in quanto la dipendenza lato applicativo verso il server LDAP e`
> meno sentita rispetto a quella che si avrebbe utilizzando un RDBMS. Per
> spiegarmi meglio, devi considerare che LDAP e` un protocollo stanrdard, di
> conseguenza la differenza fra i vari server in circolazione non e` basata su
> come tale standard e` implementato, ma sulle caratteristiche di gestione dei
> dati salvati nella directory
>
Non sono un esperto ldap, ma dall'esperienza che ho fatto in un anno e
mezzo che ci lavoro ti assicuro che a seconda dei tipi di utilizzo che
ne fanno gli applicativi talvolta puÃ² non bastare il protocollo
standard. Abbiamo faticato, a suo tempo, a trovare un ldap compatibile
con un paio di prodotti proprietari. Basti pensare che alcuni schema
di base non sono identici o non sono presenti tra sunds e opendj e per
fare l'import ho dovuto fare un overwrite ed in piÃ¹ importare i dati
con --skipSchemaValidation

> > no! giÃ ci sono voluti mesi per migrare la
> > piattaforma su hardware piÃ¹ potente di quello iniziale,
>
> Personalmente farei una prova, anche informale
>
BUM!!!
abbiamo tre ambienti, sviluppo, collaudo e produzione; ognuno di
questi ambienti Ã¨ diviso in 3 parti, gestito da 3 gruppi separati per
tipologia per dislocazione geografica, per ditta di appartenenza e per
server gestiti (anche se sono sulla stessa lan); ognuno di questi
gruppi non parla in modo diretto l'uno con l'altro ma via un tramite.
L'ambiente di sviluppo, quello in teoria candidato per l'esperimento,
non Ã¨ gestito applicativamente da me (io ho la gestione sistemistica,
il resto Ã¨ demandato agli sviluppatori).

La modifica di una sola virgola in collaudo (ogni nuovo aggiornamento,
anche minor) comporta il test della componente modificata e di quelle
coinvolte... L'ldap Ã¨ usato da tutte le componenti. E a seconda del
tipo di modifica anche gli stress test vanno rifatti. Non parliamo poi
del fatto che l'ldap incide prestazionalmente sullo storage esterno

(su cui in passato abbiamo avuto seri problemi).

GiÃ in collaudo lo _stop_ di una componente Ã¨ spesso necessario
comunicarlo se questo comporta un disservizio (il collaudo Ã¨ in uso
quasi quanto lo Ã¨ produzione).

Trasla tutto sull'ambiente di produzione e moltiplica per 10 (abbiamo
un milione di utenze).

> Se quello schema funziona con 389ds, e quello schema e` essenziale per i
> vostri scopi, allora ti consiglio vivamente la migrazione
>
Lo schema personalizzato Ã¨ chiaramente essenziale per il funzionamento
della piattaforma.
Per 389ds l'import dello schema era andato ok, ma l'import dei dati
era stato fatto con un export non completo. Non saprei come si
potrebbe comportare con l'export completo, non ho ancora provato.

> Perche` sul wiki di OpenDS e` scritto chiaramente che nelle future versioni
> avrebbero supportato le repliche con SunDS
>
1) non sono riuscito a trovarlo sul wiki, nÃ© altrove
2) opends Ã¨ morto; opendj non Ã¨ un clone di opends ma una rinomina
(confronta date, versioni e timeline presente passata e futura).
3) A dire la veritÃ anche SunDS Ã¨ morto, sostituito da OracleDS

Subject: Re: opends e sunds
Posted by Matteo Rossini on Thu, 23 Jun 2011 13:44:53 GMT
View Forum Message <> Reply to Message

389ds:

http://directory.fedoraproject.org/wiki/FAQ

* Does replication inter-operate with Netscape/iPlanet/Sun Directory
Server?

- Sun/iPlanet DS 5.0, 5.1 and Netscape Directory Server 6.x, 7.0: Yes.
The
  protocol was extended in DS7.1, but there is detection code to
identify
  downlevel replicas and fall back to the old protocol.
- Sun DS 5.2 and later: unknown - Sun DS 5.2 uses a different
replication
  protocol. It's not known if it can auto-detect and fallback. It does

have a
 "legacy" replication mode that works with Sun/iPlanet DS 5.0 and
5.1, so that
 should work.
- Netscape DS 4.x: There is a Legacy Replication Plug-in that must be
configured
 and enabled. Additionally, 389 can only act as a consumer for Legacy
 replication, so you can't have a 4.x server as a consumer for a 389
supplier.
 Finally, this mode is only intended to be used for migration
purposes, not
 long term.

Subject: Re: opends e sunds
Posted by Enrico 'Henryx' Bianc on Thu, 23 Jun 2011 22:51:12 GMT
View Forum Message <> Reply to Message

Matteo Rossini wrote:

> licenze

Posto che non sarebbe un discorso da fare, ma infischiarsene ed installarne una copia per la replica? :)

> Non sono un esperto ldap, ma dall'esperienza che ho fatto in un anno e
> mezzo che ci lavoro ti assicuro che a seconda dei tipi di utilizzo che
> ne fanno gli applicativi talvolta puÃ² non bastare il protocollo
> standard.

Cosa intendi? Tieni presente che il protocollo lato comunicazione applicativo/server e` standard, di conseguenza da quel punto di vista sei/siete a posto

> Basti pensare che alcuni schema
> di base non sono identici o non sono presenti tra sunds e opendj

Beh, gli schemi sono parte integrante di come il server gestisce i dati, non di come li comunica al client :)

>ognuno di questi
> gruppi non parla in modo diretto l'uno con l'altro ma via un tramite.

Posto che sono vostre scelte, la reputerei una brutta cosa

> L'ambiente di sviluppo, quello in teoria candidato per l'esperimento,
> non Ã¨ gestito applicativamente da me (io ho la gestione sistemistica,
> il resto Ã¨ demandato agli sviluppatori).

Non vedo dove sia il problema, alla fine si tratta di creare una macchina virtuale dove installare 389ds (che, da quello che ho capito, e` il server LDAP che ti creerebbe meno problemi di migrazione), vedere se gli schemi vengono correttamente riconosciuti e fare un import dei dati via LDIF

> La modifica di una sola virgola in collaudo (ogni nuovo aggiornamento,
> anche minor) comporta il test della componente modificata e di quelle
> coinvolte...

Ecco, questo e` il vero problema, anche se non vedo molte soluzioni per eliminarlo

> GiÃ in collaudo lo _stop_ di una componente Ã¨ spesso necessario
> comunicarlo se questo comporta un disservizio (il collaudo Ã¨ in uso
> quasi quanto lo Ã¨ produzione).

C'e` qualcosa che non mi torna, come puo` il fermo di un server di test comportare un disservizio?

> Trasla tutto sull'ambiente di produzione e moltiplica per 10 (abbiamo
> un milione di utenze).

Ecco, questo e` un altro problema (minore del primo ma tant'e`): la mole di dati non e` indifferente :)

> Per 389ds l'import dello schema era andato ok, ma l'import dei dati
> era stato fatto con un export non completo. Non saprei come si
> potrebbe comportare con l'export completo, non ho ancora provato.

Personalmente, per test interni, ho provato l'import dei dati da OpenLDAP verso 389ds o OpenDJ. In tutti e due i casi, a parte il riconoscimento iniziale degli schemi (lo schema Samba non e` direttamente disponibile per OpenDS), l'import e` andato a buon fine ed il server era direttamente funzionante. C'e` comunque da dire che non ho mai usato direttamente questi server LDAP (la sostituzione di OpenLDAP mi e` decisamente difficile per svariati motivi), ma una interrogazione tramite strumenti agnostici (e.g. LDAP Browser) non mi diede alcun problema

> 1) non sono riuscito a trovarlo sul wiki, nÃ© altrove

https://www.opends.org/wiki/page/Replication e` in fondo alla pagina

> 2) opends Ã¨ morto; opendj non Ã¨ un clone di opends ma una rinomina
> (confronta date, versioni e timeline presente passata e futura).

OpenDJ e` un fork di OpenDS, punto. I motivi per cui preferire OpenDJ rispetto all'originale sono dovuti al fatto che OpenDS e` in una fase di

stallo (ovvero Oracle non ha piu` rilasciato aggiornamenti da ottobre 2010),
ma da nessuna parte e` scritto che il progetto e` morto

> 3) A dire la veritÃ anche SunDS Ã¨ morto, sostituito da OracleDS

Motivo in piu` per spingere ad una migrazione verso un altro prodotto

Enrico

Subject: Re: opends e sunds
Posted by Matteo Rossini on Mon, 27 Jun 2011 15:37:41 GMT
View Forum Message <> Reply to Message

Sono riuscito a mettere 389-ds in replica a sunds.

L'ho messo come consumer ma c'Ã¨ un problema.

La replica master->consumer viene fatta perfettamente, ma mi viene
consentito anche l'ldapmodify sul consumer. Avendo scelto "Dedicated
Consumer" e non avendo messo i "referral" le modifiche non vendono
riportate sul master (come deve essere); questo porta ovviamente ad un
disallineamento dei due server, e questo non deve succedere.
Suppongo di dover impostare qualche aci da qualche parte, per negare
l'ldapmodify (anche all'utente Directory Manager), ma non riesco a
trovarlo.

Subject: Re: opends e sunds
Posted by Enrico 'Henryx' Bianc on Mon, 27 Jun 2011 18:05:40 GMT
View Forum Message <> Reply to Message

Matteo Rossini wrote:

> La replica master->consumer viene fatta perfettamente, ma mi viene
> consentito anche l'ldapmodify sul consumer

Detta cosi` sembra che tu abbia una configurazione multimaster. Sei sicuro
che sia impostato come consumer?

Enrico
