

Guida operativa per UNIX e Linux

Arcserve® Replication and High Availability

r16.5

arcserve®

Informazioni di carattere legale

La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da Arcserve in qualsiasi momento.

Questa Documentazione non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di Arcserve. Questa Documentazione è di proprietà di Arcserve e non potrà essere divulgata o utilizzata se non per gli scopi previsti in (i) uno specifico contratto tra l'utente e Arcserve in merito all'uso del software Arcserve cui la Documentazione attiene o in (ii) un determinato accordo di confidenzialità tra l'utente e Arcserve.

Fermo restando quanto enunciato sopra, se l'utente dispone di una licenza per l'utilizzo del software a cui fa riferimento la Documentazione avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di Arcserve.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a Arcserve per iscritto che tutte le copie anche parziali del prodotto sono state restituite a Arcserve o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, ARCSERVE FORNISCE LA DOCUMENTAZIONE "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO ARCSERVE SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLIFICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DI AVVIAMENTO O DI DATI, ANCHE NEL CASO IN CUI ARCSERVE VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è Arcserve.

Fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

© 2017 Arcserve, incluse affiliate e controllate. Tutti i diritti riservati. Tutti i marchi o i diritti di copyright di terze parti sono di proprietà dei rispettivi titolari.

Riferimenti dei prodotti Arcserve

Questo documento fa riferimento ai seguenti prodotti Arcserve:

- Arcserve® Replication
- Arcserve® High Availability (HA)

Come contattare Arcserve

Il team di Supporto tecnico di Arcserve offre un insieme di risorse per la risoluzione dei problemi tecnici e fornisce l'accesso a importanti informazioni sul prodotto.

<https://www.arcserve.com/support>

Con il supporto Arcserve:

- È possibile consultare direttamente la stessa libreria di informazioni condivisa internamente dagli esperti del Supporto tecnico di Arcserve. Questo sito fornisce l'accesso ai documenti della Knowledge Base (KB). Da qui, è possibile cercare e trovare facilmente gli articoli della Knowledge Base relativi al prodotto e contenenti le soluzioni testate sul campo a molti problemi principali e comuni.
- È possibile utilizzare il collegamento alla Chat in tempo reale per avviare una conversazione in tempo reale con il team di Supporto tecnico di Arcserve. Con la Chat in tempo reale, è possibile ottenere risposte immediate alle proprie domande e preoccupazioni, mantenendo al contempo l'accesso al prodotto.
- È possibile partecipare alla Arcserve Global User Community per porre domande e rispondere, condividere suggerimenti e consigli, discutere su procedure consigliate e partecipare a discussioni con i propri colleghi.
- È possibile aprire un ticket di supporto. Quando si apre un ticket di supporto in linea, si verrà contattati da uno degli esperti nell'area del prodotto per il quale si richiede il supporto.

È possibile accedere ad altre risorse utili relative al prodotto Arcserve.

Commenti e suggerimenti sulla documentazione dei prodotti

Arcserve Per eventuali commenti o domande sulla documentazione di prodotto, si prega di [contattarci](#).

Contenuti

Capitolo 1: Introduzione	7
Documentazione correlata	8
Tipi di server supportati	9
Requisiti del server	10
Capitolo 2: Installazione e disinstallazione di Arcserve RHA	11
Prerequisiti	12
Installazione del modulo	13
Installazione del modulo in zone Solaris non globali	14
Gestione del modulo	15
Installazione della Gestione	16
Preparazione dell'ambiente per HA con lo script GSSnsupdate	18
Aggiornamento Arcserve RHA	22
Disinstallazione di Arcserve RHA	23
Disinstallazione dell'Arcserve RHA	24
Capitolo 3: Metodi di reindirizzamento	25
Capitolo 4: Gestione di scenari	27
Creazione di uno scenario di replica	28
Creazione di uno scenario High Availability	32
Avvio di uno scenario	35
Interruzione di uno scenario	37
Considerazioni relative agli scenari UNIX/Linux	38
Capitolo 5: File installati	41
File installati su Red Hat e Novell SUSE Linux Enterprise	42
File installati su IBM AIX	43
File installati su Solaris	44
Capitolo 6: Risoluzione dei problemi	45
Scaricamento dei driver xofs	46
L'IP spostato non viene attivato dopo l'avanzamento	48
Il listener di Oracle non accetta la connessione client dopo il failover	49

Capitolo 1: Introduzione

Questo documento è destinato ad amministratori di sistema UNIX e Linux esperti, interessati all'implementazione e alla distribuzione della soluzione Arcserve RHA nel proprio ambiente di utilizzo. Il documento fornisce tutti i dettagli necessari per l'installazione e la disinstallazione del prodotto, per la creazione di scenari Replication (DR) e High Availability (HA), per la gestione di scenari e il recupero di dati.

La presente sezione descrive i seguenti argomenti:

Documentazione correlata	8
Tipi di server supportati	9
Requisiti del server	10

Documentazione correlata

Utilizzare questa guida unitamente alla *Guida all'installazione di Arcserve RHA*, alla *Guida per l'amministratore di Arcserve RHA* e alla *Guida per PowerShell di Arcserve RHA*.

Tipi di server supportati

Per i tipi di server supportati, fare riferimento alle Note di rilascio.

Requisiti del server

Per l'implementazione di Arcserve RHA, consultare l'elenco dei requisiti appropriato, in base al tipo di server selezionato. Questi componenti sono concessi in licenza separatamente. Se non si dispone della licenza per accedere al supporto di un tipo specifico di server, rivolgersi al supporto tecnico.

Scenario HA:

- Il master e la replica devono eseguire lo stesso sistema operativo con uguale livello di Service Pack e correzioni rapide. Ad esempio, non è possibile creare uno scenario HA da AIX a Solaris.

Scenario HA per Oracle:

- Due server con supporto server UNIX/Linux, sui quali siano stati installati i medesimi Service Pack e le medesime correzioni rapide.
Nota: per un elenco completo delle applicazioni e dei sistemi operativi supportati, consultare la Note di rilascio di Arcserve RHA.
- Installare la stessa versione di Oracle su entrambi i server, inclusi i service pack e le correzioni rapide
- Il SID di Oracle sul master deve corrispondere alla replica
- L'ID dell'utente Oracle (ad esempio, utente "oracle") e dei gruppi Oracle (ad esempio, oinstall o dba) devono essere identici sul server master e di replica. Ad esempio, se l'ID di "oracle" sul master è 300, l'ID sulla replica deve essere 300.+
- Assicurarsi che il percorso alla directory ORACLE_HOME e ai file di database sia identico sul master e sulla replica.

Per ridurre il traffico di rete, i nomi spazio tabella temporanei di Oracle e il percorso sono esclusi dalla replica. Verificare che il database di Oracle sul server di replica sia configurato con gli stessi nomi spazio tabella temporanei e con lo stesso percorso utilizzati sul server master.

Nota: Arcserve HA per Oracle non supporta Oracle RAC.

Capitolo 2: Installazione e disinstallazione di Arcserve RHA

In questo capitolo vengono descritte le modalità di installazione e di disinstallazione dei componenti Modulo Arcserve RHA e Gestione Arcserve RHA.

La presente sezione descrive i seguenti argomenti:

Prerequisiti	12
Installazione del modulo	13
Gestione del modulo	15
Installazione della Gestione	16
Preparazione dell'ambiente per HA con lo script GSSnsupdate	18
Aggiornamento Arcserve RHA	22
Disinstallazione di Arcserve RHA	23

Prerequisiti

Prima dell'installazione, verificare il seguente prerequisito:

Su piattaforme Linux, alcuni pacchetti richiesti dal modulo RHA potrebbero non essere installati per impostazione predefinita. È necessario installare tali pacchetti prima di installare il modulo RHA. Il comando seguente elenca i pacchetti richiesti dal modulo RHA.

```
rpm -qpR <rha-rpm-file>
```

Ad esempio, `rpm -qpR arcserverha_rhel7_x86_64.rpm`

Installazione del modulo

Il bundle di installazione di Arcserve RHA è composto da pacchetti per tutte le piattaforme supportate e da uno script di installazione comune.

Per installare il modulo:

1. È innanzitutto necessario diventare "super utente" (root).
2. Sostituire la directory di lavoro con la directory che contiene i file di installazione.
3. Eseguire lo script *install.sh*.
4. Seguire le istruzioni fino al termine della procedura di installazione.

Viene richiesto di specificare se si accettano i termini del contratto di licenza e se si desidera creare un gruppo caarha e abilitare il supporto Oracle.

Note:

- ◆ Se si sceglie di abilitare il supporto Oracle, è necessario indicare il titolare, il percorso principale e il percorso di base di Oracle. Sarà necessario specificare prima l'utente titolare di Oracle, quindi il prodotto recupererà il percorso principale e il percorso di base attraverso l'ambiente dell'utente. Se il percorso principale e il percorso di base non potranno essere trovati, sarà necessario aggiungerli manualmente. Su Solaris, se il server Oracle installato non dispone della libreria client Oracle a 32 bit, sarà necessario fornire anche il percorso di Oracle Instant Client.
- ◆ Se il pacchetto Arcserve RHA è stato installato, verrà richiesto di reinstallarlo.
- ◆ Per consentire agli utenti non root di gestire gli scenari, è necessario creare il gruppo "caarha" sul proprio computer ed assicurarsi che questo gruppo lavori con il gruppo supplementare.
- ◆ Su Linux, lo script *install.sh* supporta l'installazione invisibile all'utente (*install.sh -y*).

Per le informazioni relative all'uso, utilizzare *install -?*.

Installazione del modulo in zone Solaris non globali

Per zone Solaris non globali, è necessario eseguire lo script *configure.sh* in ogni zona non globale.

Nota: per zone non globali su Solaris 11, assicurarsi che il modulo RHA sia installato su zone globali prima di installarlo su zone non globali.

Per installare il modulo in zone Solaris non globali, procedere come segue:

1. Eseguire lo script *install.sh* nelle zone globali come processo di livello superiore.
2. Eseguire lo script *configure.sh* in ciascuna zona non globale dopo l'installazione.

Gestione del modulo

Al termine dell'installazione, il Modulo Arcserve RHA viene gestito automaticamente dal sistema operativo. Il modulo viene avviato durante la sequenza di avvio del sistema e interrotto durante il processo di arresto. Queste procedure verranno eseguite automaticamente tramite script **.rc**.

Tuttavia, se è necessario interrompere manualmente il modulo e quindi riavviarlo, seguire le istruzioni riportate di seguito:

Linux

Per avviare un modulo, procedere come segue:

```
/etc/init.d/ARCserveRHA start
```

Per interrompere un modulo, procedere come segue:

```
/etc/init.d/ARCserveRHA stop
```

Solaris

Per avviare un modulo, procedere come segue:

```
/etc/init.d/ARCserveRHA start
```

Per interrompere un modulo, procedere come segue:

```
/etc/init.d/ARCserveRHA stop
```

AIX

Per avviare un modulo, procedere come segue:

```
/opt/ARCserveRHA/bin/ARCserveRHA.rc start
```

Per interrompere un modulo, procedere come segue:

```
/opt/ARCserveRHA/bin/ARCserveRHA.rc stop
```

Installazione della Gestione

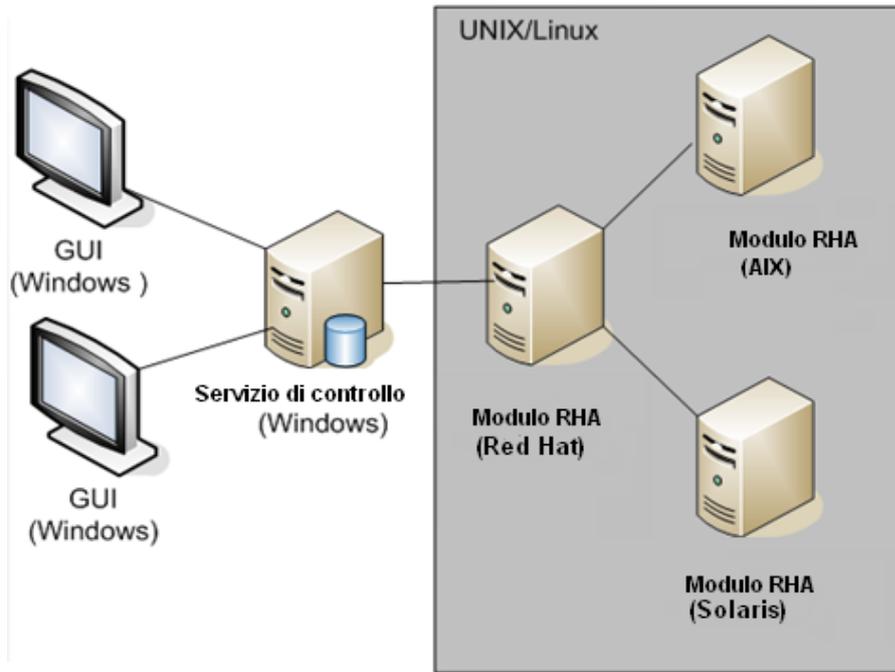
Il componente Gestione di Arcserve RHA può essere installato unicamente su piattaforme Windows. L'installazione dei componenti di Arcserve RHA su una piattaforma Windows è molto semplice. Il pacchetto di installazione contiene un file denominato *Setup.exe* che consente di eseguire una procedura guidata MSI standard.

- Al termine dell'installazione non è necessario riavviare il sistema o chiudere l'applicazione.
- Per *instmsi.exe* è richiesta la versione 2.0.2600.2 o successive. Se non si dispone di questo requisito minimo, l'installazione di Arcserve RHA aggiorna automaticamente Windows Installer al posto dell'utente. Tuttavia, l'aggiornamento del programma di installazione richiede il riavvio del sistema.

I messaggi visualizzati facilitano la procedura di installazione. L'utente deve solo decidere su quali server installare le applicazioni (la Gestione Arcserve RHA e Arcserve RHA PowerShell vengono installati contemporaneamente):

- Installare la Gestione Arcserve RHA e il Servizio di controllo su ciascun computer Windows Server con accesso di rete ai computer che si desidera gestire, come illustrato nel seguente diagramma.
- La directory di installazione predefinita (INSTALLDIR) è:
\\Programmi\CA\ARCserve RHA. Tutti gli eseguibili, le DDL e i file di configurazione si trovano nella directory di installazione INSTALLDIR.
- Gli utenti Windows che eseguono la Gestione Arcserve RHA devono disporre di autorizzazioni di lettura e scrittura per la directory di installazione.

Installare il Modulo Arcserve RHA su tutti i server coinvolti negli scenari UNIX/Linux. Per ulteriori informazioni sull'installazione della Gestione di Arcserve RHA, consultare la *Guida all'installazione di Arcserve RHA*.



Preparazione dell'ambiente per HA con lo script GSSnsupdate

Per eseguire scenari High Availability in domini protetti della zona DNS, è necessario configurare il proprio server UNIX o Linux per abilitare l'autenticazione e modificare i record A dell'host DNS per i server master e di replica presenti negli scenari.

L'ambiente UNIX/Linux può essere configurato per Arcserve RHA utilizzando lo script PERL riportato. Contattare il Supporto tecnico per acquisire altre versioni dello script.

Le fasi riportate di seguito dovranno essere eseguite su tutti gli host UNIX/Linux presenti nell'ambiente.

Per preparare gli host UNIX e Linux per HA in domini protetti della zona DNS, procedere come segue:

1. Configuri l'host di Linux come client di Kerberos modificando il file `/etc/krb5.conf` nel modo seguente:

```
[libdefaults]
```

```
default_realm = <nome DOMINIO, ad es. XOSOFT.ORG>
```

```
[realms]
```

```
<DOMAIN name> = {
```

```
kdc = <DC Server fqdn>:88
```

```
admin_server = <DNS Server fqdn>
```

```
default_domain = <DOMAIN name i.e. XOSOFT.ORG>
```

```
}
```

```
[domain_realm]
```

```
<domain name >= <DOMAIN name> ad esempio .xosoft.org =XOSOFT.ORG
```

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
default_realm = XOLAB.COM

[realms]
XOLAB.COM = {
  kdc = server01.xolab.com:88
  admin_server = server01.xolab.com:749
  default_domain = XOLAB.COM
}

[domain_realm]
.xolab.com = XOLAB.COM

[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf
```

2. Creare un file keytab con ktpass sul controller di dominio specificato in nel parametro "kdc" nella fase precedente. Accedere a KDC con un account di amministratore di dominio.

Nota: l'utilità ktpass potrebbe non essere caricata su Windows per impostazione predefinita. In tal caso è possibile ottenerla dal pacchetto Windows Support Tools.

```
ktpass -princ host/<a name you pick@DOMAIN> -mapuser <domain
admin@DOMAIN> -pass <password> -out c:\<filename->.keytab -ptype KRB5_NT_
PRINCIPAL
```

```
C:\>ktpass -princ host/xodemo@XOLAB.COM -mapuser testuser@XOLAB.COM -pass qazwsx
-out C:\xodemo.keytab -ptype KRB5_NT_PRINCIPAL
Targeting domain controller: calabdc01.xolab.com
Successfully mapped host/xodemo to testuser.
Key created.
Output keytab to C:\xodemo.keytab:
Keytab version: 0x502
keysize 48 host/xodemo@XOLAB.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-
CBC-MD5) keylength 8 (0x8545b3195d835497)
Account testuser has been set for DES-only encryption.
C:\>
```

3. Trasferimento sicuro del file keytab <nomefile>.keytab all'host di Linux
4. Sull'host di Linux, combinare il file keytab in un file singolo denominato /etc/krb5.keytab, utilizzando il programma ktutil. Prima di procedere, potrebbe essere necessario installare il pacchetto Ktutil.

```
[root@server01-1x1 bin]# ktutil
```

```
ktutil: rkt /root/ <filename->.keytab
```

```
ktutil: wkt /etc/krb5.keytab
```

ktutil: list

ktutil: q

```
[root@server01 ~]# /usr/kerberos/sbin/ktutil
ktutil: rkt ./xodemo.keytab
ktutil: wkt /etc/krb5.keytab
ktutil: list
slot KVNO Principal
-----
 1  5                               host/test@XOLAB.COM
ktutil: q
[root@calabsrv07-1x1 ~]#
```

5. Assicurarsi che l'ora dell'host Linux sia sincronizzata con il server NTP o con il server Microsoft DNS.

6. Copiare lo script PERL *nsupdate-gss.pl* e installare l'insieme delle librerie PERL necessarie per lo script. È possibile trovare le fonti PERL all'indirizzo <http://search.cpan.org> o mediante RPM.

perl-Digest-HMAC

perl-Net-IP

perl-Net-DNS

perl-GSSAPI

perl-Krb5...

7. Commentare tutte le seguenti righe nello script *nsupdate-gss.pl* contenuto in */opt/CA/ARCserve RHA/*:

```
#####
my $sys_retcode = system("kinit -k host/xodemo");
if ($sys_retcode != 0) {
    print "Fail to create and cache Kerberos ticket through 'kinit'\n";
    exit 1;
}
#####
```

8. Inizializzare la cache di Kerberos con il seguente comando:

kinit redhat

redhat è l'account dell'amministratore di dominio creato in Active Directory.

9. Verificare la cache Kerberos con il seguente comando:

kinit o kinit -l

10. Eseguire il test riportato di seguito per assicurarsi che l'ambiente è pronto e che lo script è in grado di aggiornare i record A di DNS.

```
./nsupdate-gss.pl 192,168.88,1 shagu01-RHEL5u3-x64 xosoft.org --add_
ips=192,168.88,21 --ttl=60 --del_ips=192,168.88,31
```

11. Definire lo script nsupdate-gss.pl nel file ws_rep.cfg collocato nella directory di installazione /opt/CA/ARCserveRHA/bin per eseguire un aggiornamento sicuro su Microsoft DNS. Rimuovere il simbolo # collocato al principio della riga "GSSNupdateScript =", come mostrato di seguito.

```
#####
```

```
# Script per l'aggiornamento dinamico sicuro sul server MS DNS su host UNIX/Linux
```

```
GSSNupdateScript = "[INSTALLDIR]/scripts/nsupdate-gss.pl"
```

```
#
```

```
# L'utente può visitare il sito del supporto tecnico di arcserve o
```

```
# definire lo script mediante shell o PERL con argomenti corrispondenti a
```

```
# GSSNupdateScript NAME_SERVER HOST DOMAIN [options]
```

```
# Opzioni:
```

```
# --add_ips=IPS    IP di destinazione dei record A da aggiungere
```

```
# --ttl=TTL       TTL per i record A aggiunti
```

```
# --del_ips=IPS   IP di destinazione dei record A da eliminare
```

12. Arrestare e riavviare il modulo:

```
/etc/init.d/ARCserveRHA stop
```

```
/etc/init.d/ARCserveRHA stop
```

13. Ripetere questa procedura per l'altro host.

Aggiornamento Arcserve RHA

Prima di eseguire l'aggiornamento alla presente versione, considerare quanto segue:

- Interrompere tutti gli scenari in esecuzione.
- Non è necessario disinstallare manualmente la versione precedente. La procedura di installazione rimuove la versione precedente automaticamente.
- Copiare gli scenari precedenti sul computer in cui è in esecuzione la versione corrente dell'interfaccia utente di gestione Arcserve RHA. Al termine della copia, è possibile importare gli scenari nella versione corrente di Arcserve RHA selezionando Scenario dal menu Importa. Gli scenari potrebbero trovarsi nelle posizioni seguenti:
 - ◆ UNIX: /opt/ARCserveRHA/bin/ws_scenarios
 - ◆ Windows: Program Files (x86)/CA/Arcserve RHA/Manager/ws_scenarios

Disinstallazione di Arcserve RHA

Prima di disinstallare Arcserve RHA è necessario interrompere tutti gli scenari in esecuzione e verificare che non siano presenti directory montate da xofs.

Per verificare che non vi siano directory montate da xofs, assicurarsi che il file `/etc/xofs_mnttab` sia vuoto. In caso contrario, fare riferimento alla sezione [Scaricamento dei driver xofs](#).

Nota: è possibile ignorare il processo di verifica semplicemente riavviando il computer al termine della procedura di disinstallazione.

Disinstallazione dell'Arcserve RHA

La seguente procedura è valida per la disinstallazione di Arcserve RHA su tutte le piattaforme UNIX e Linux supportate.

Per disinstallare Arcserve RHA

1. È innanzitutto necessario essere un "super utente".
2. Assicurarsi che tutti gli scenari di replica siano stati interrotti.
3. Eseguire il seguente script di disinstallazione:

```
/opt/ARCserveRHA/bin/uninstall.sh
```

Viene richiesto di confermare la procedura di disinstallazione. Ad esempio:

```
Disinstallare Arcserve RHA? (Y/N)
```

4. Immettere *Y* e premere Invio.
5. [Facoltativo] Riavviare.

Capitolo 3: Metodi di reindirizzamento

Arcserve High Availability (Arcserve HA) monitora tutti gli eventi di importanza critica, incluso il malfunzionamento del server globale e tutti gli errori del servizio di database, avviando un avanzamento automaticamente o premendo semplicemente un pulsante.

Se il server master non è più disponibile, sarà possibile eseguire l'avanzamento delle relative attività su un sito remoto (server di replica). L'avanzamento, che è trasparente all'utente, include l'avvio immediato di un database in stand-by sincronizzato e il reindirizzamento di tutti gli utenti allo stesso in un tempo minimo. Tutto ciò può essere eseguito senza la necessità di riconfigurare i clienti o la rete.

Il reindirizzamento può essere basato sui metodi seguenti:

- IP di spostamento (se il sito in stand-by è implementato all'interno dello stesso segmento di rete)
- Reindirizza DNS: può essere usato su una rete locale o quando il sito in stand-by remoto si trova su una diversa rete IP (avanzamento tra più reti)
- Modifica del nome host del server

Nota: è anche possibile applicare script definiti dall'utente che integrino o sostituiscano i metodi di reindirizzamento incorporati. Gli script di identificazione della direzione del traffico di rete sono richiesti per supportare i metodi di reindirizzamento personalizzati. Gli script personalizzati o file di batch vengono utilizzati per identificare il server attivo. Questo script determina se lo scenario successivo o precedente verrà eseguito all'avvio dello scenario. Lo script viene eseguito sia sul server master sia sul server di replica: quello tra i due che restituisce un valore pari a zero è il server attivo. Se entrambi restituiscono zero, verrà segnalato un conflitto.

La selezione del metodo di reindirizzamento si basa sui requisiti delle applicazioni da proteggere. È possibile che alcuni metodi non siano compatibili con un determinato scenario. Per ulteriori informazioni, consultare la guida operativa specifica dell'applicazione.

Se il metodo di reindirizzamento utilizzato in scenari UNIX/Linux si basa sulla modifica del nome host, sarà necessario impostare anche il reindirizzamento DNS.

Metodo di reindirizzamento con IP di spostamento per Red Hat Enterprise Linux 6.x e CentOS 6.x

Per utilizzare il metodo di reindirizzamento Sposta IP per Red Hat Enterprise Linux 6.x e CentOS 6.x, procedere come segue:

-
1. Disattivare il servizio di NetworkManager e avviare il servizio di rete nativo sul server master e sul server di replica. Per ulteriori informazioni sulle modalità di disattivazione del server NetworkManager, consultare la guida utente del sistema operativo corrispondente.
 2. Sul server master, configurare manualmente gli indirizzi IP alias aggiungendo i file di configurazione ifcfg-ethModule:<n>.

Capitolo 4: Gestione di scenari

In questo capitolo vengono descritte le modalità di creazione, avvio e interruzione degli scenari mediante la Gestione. È anche possibile utilizzare PowerShell gestire i propri scenari. Per ulteriori informazioni sull'utilizzo di PowerShell per la creazione di scenari, consultare la *Arcserve RHAGuida per PowerShell*.

Importante! Arcserve RHA è l'opzione più adatta per la replica dei file di dati. Si sconsiglia di replicare i file eseguibili e le librerie utilizzando, in quanto ciò potrebbe influire sulle prestazioni dell'applicazione. Durante la creazione dello scenario, è possibile escludere tali file dalla replica.

A partire da questa release, sarà possibile utilizzare scenari High Availability per proteggere il proprio ambiente UNIX.

La presente sezione descrive i seguenti argomenti:

Creazione di uno scenario di replica	28
Creazione di uno scenario High Availability	32
Avvio di uno scenario	35
Interruzione di uno scenario	37
Considerazioni relative agli scenari UNIX/Linux	38

Creazione di uno scenario di replica

La protezione di computer UNIX e Linux mediante Arcserve RHA richiede scenari che identifichino i server master e di replica, nonché proprietà che controllino il comportamento degli scenari. È possibile creare scenari file server o Oracle in base alle esigenze. La funzione Rilevamento automatico viene utilizzata per proteggere una sola istanza Oracle in un singolo scenario. Se si desidera proteggere più istanze Oracle in un solo scenario, utilizzare il tipo di scenario File Server. La creazione di uno scenario è un processo basato su procedure guidate e i passaggi necessari alla creazione di scenari file server e Oracle sono abbastanza simili. Se esistono delle differenze, non sono percettibili. Per ulteriori informazioni dettagliate, consultare la Guida operativa appropriata.

Nota: le directory principali non possono essere intersecate in scenari differenti. Ciò significa che non è possibile creare un secondo scenario di replica che utilizzi la stessa directory master e la stessa directory principale utilizzate dal primo scenario di replica.

Nota: RHA non è in grado di proteggere la periferica a blocchi montata nella directory principale di RHA dopo aver eseguito lo scenario.

http://<ControlServiceHost>:8088/entry_point.aspx

1. Dalla Gestione, selezionare Scenario, Nuovo oppure fare clic sul pulsante Nuovo scenario sulla barra degli strumenti.

Viene visualizzata la Procedura guidata nuovo scenario.

2. Selezionare Crea nuovo scenario e fare clic su Avanti.

Viene visualizzata la finestra di dialogo Seleziona server e tipo di prodotto.

3. Selezionare le opzioni dello scenario necessarie, come riportate di seguito:

- a. Dall'elenco Selezionare tipo di server, selezionare il tipo di scenario che si desidera creare. Per la replica con sistemi UNIX/Linux, sono supportati solo gli scenari file server e Oracle.
- b. Dalle opzioni Seleziona tipo di prodotto, selezionare Scenario di replica e ripristino dati (DR).

4. Fare clic su Avanti.

Viene visualizzata la finestra di dialogo Host master e replica.

5. Immettere i nomi o gli indirizzi IP dei server master e di replica che si desidera proteggere, quindi fare clic su Avanti.

Viene visualizzata la finestra di dialogo Verifica modulo. Attendere l'esecuzione della verifica dello stato del modulo. Se la versione corrente non è aggiornata, viene richiesto di eseguire l'aggiornamento da parte di Arcserve RHA. È possibile installare la versione più recente o continuare. Una volta completata la verifica, fare clic su Avanti.

Nota: se il tipo di scenario è Oracle, verranno richieste le credenziali utente. Immettere le credenziali dell'account con privilegi di amministrazione nel database, per consentire a Arcserve RHA di interrogare la configurazione Oracle sul server master.

6. Immettere il nome dell'istanza Oracle, il nome utente, la password e il nome DBA di Oracle, quindi fare clic su OK.

- ◆ Negli scenari **file server**, viene visualizzata la finestra di dialogo Directory principali master. Selezionare i file e/o le directory da replicare dal server master, quindi fare clic su Avanti per passare alla schermata Directory principali di replica.
- ◆ Negli scenari **Oracle**, viene visualizzata la finestra di dialogo Spazi tabella per la replica al posto della finestra di dialogo Directory principali master. Arcserve RHA visualizza un elenco dei risultati rilevati automaticamente sul server master. Selezionare o deselezionare i database di replica in base alle proprie esigenze, quindi abilitare l'opzione di replica dei nuovi file creati dall'utente nelle directory principali elencate. Fare clic su Avanti per passare alla schermata Directory principali di replica.

Viene visualizzata la finestra di dialogo Directory principali di replica. In base al tipo di scenario creato nella finestra di dialogo Directory principali di replica, viene visualizzato un elenco di directory per il database Oracle o file server.

7. Selezionare i file, le directory o entrambi sulla replica in cui verranno archiviati i dati che si desidera replicare, quindi fare clic su Avanti.

Nota: se sul server di replica esiste la stessa struttura di directory, la procedura guidata la seleziona automaticamente come directory in cui eseguire la replica.

Viene visualizzata la finestra di dialogo Proprietà scenario.

8. Configurare le proprietà del master e della replica. In genere, i valori predefiniti sono sufficienti ad eccezione delle credenziali utente. È possibile modificare tutte le impostazioni in questo riquadro dopo aver creato lo scenario.

Note:

- ◆ per la proprietà delle credenziali utente master e di replica è necessario immettere il nome utente e la password corrispondenti con autorizzazioni di controllo completo nella directory padre disponibile nella directory principale.
- ◆ Lo spool è una cartella sul disco in cui vengono temporaneamente memorizzati i dati da replicare (di cui viene quindi eseguito lo spooling). I parametri di spool, presenti nella scheda Proprietà sul server master e di replica oppure impostati con la Procedura guidata nuovo scenario, determinano la quantità di spazio su disco disponibile per lo spool. Nella maggior parte dei casi, il valore predefinito è sufficiente. Tuttavia, se si sceglie di modificare questo valore, impostarlo almeno sul 10% della dimensione totale del set di dati. Per ulteriori informazioni, consultare la *Guida per l'amministratore di Arcserve RHA*.

Viene visualizzata la finestra di dialogo Proprietà di master e replica.

9. Impostare l'opzione di ripristino dei dati su *Attivo* nel riquadro delle Proprietà di replica se si desidera abilitare il recupero dei dati dalla replica utilizzando i punti di ripristino. Per ulteriori informazioni sull'utilizzo del ripristino dei dati, si rimanda alla sezione Ripristino dei dati.
10. Dopo aver configurato le proprietà del master e della replica, fare clic su *Avanti*.
Verrà visualizzata la finestra di dialogo di verifica scenario e la procedura guidata verificherà la configurazione dello scenario.
11. Fare clic su *Avanti* se lo scenario è stato verificato correttamente, oppure, in caso di errori, fare clic sul pulsante *Indietro* e correggere le impostazioni dello scenario.
Al termine della verifica dello scenario, verrà visualizzata la pagina Esecuzione scenario, che richiederà l'esecuzione dello scenario. L'esecuzione dello scenario consente di avviare il processo di sincronizzazione dei dati.
12. Fare clic su *Esegui ora* per eseguire lo scenario, oppure su *Fine* per chiudere la creazione scenario ed eseguirlo in un secondo momento.

Viene avviato il processo di sincronizzazione.

Per zone non globali su Solaris

Consente di creare scenari nella zona globale, da cui è possibile gestire tutti gli scenari. La maggior parte delle fasi sono uguali, ad eccezione delle seguenti:

1. Immettere l'indirizzo IP della zona globale come indirizzo IP master.
2. Utilizzare i seguenti comandi per ottenere le informazioni sulla zona sulla directory principale della zona:

```
/usr/sbin/zoneadm list -vi
```

zonecfg -z <zonename> info

3. Durante l'impostazione della directory principale, aggiungere manualmente la directory principale della zona non globale al percorso che si desidera proteggere. In questo caso, non è possibile utilizzare il rilevamento automatico per le applicazioni come Oracle.

Creazione di uno scenario High Availability

Per creare scenari HA di UNIX, procedere come per qualunque altro scenario HA, utilizzando la Configurazione guidata scenario.

Per informazioni sulla creazione di scenari HA per un database Oracle, si rimanda alla *Guida operativa di Arcserve RHA per Oracle Server*.

Per creare un nuovo scenario HA di UNIX, procedere come segue:

1. Avviare la Gestione di Arcserve RHA. Selezionare File, Crea, Nuovo scenario oppure fare clic sul pulsante Nuovo scenario.

Viene visualizzata la finestra di dialogo iniziale.

2. Fare clic su Crea nuovo scenario e immettere un nome del gruppo di scenari oppure selezionarne uno dall'elenco, quindi fare clic su Avanti.

Viene visualizzata la finestra di dialogo Seleziona server e tipo di prodotto.

3. Scegliere File server e verificare che il tipo prodotto Scenario High Availability (HA) sia selezionato. Per Attività su replica, selezionare Nessuno/a, quindi fare clic su Avanti.

Viene visualizzata la finestra di dialogo Host master e replica.

4. Immettere un nome per lo scenario, il nome host o l'indirizzo IP e il numero della porta per i server master e di replica, abilitare l'opzione Verifica Modulo Arcserve RHA sugli host, quindi fare clic su Avanti. È possibile che vengano richieste le credenziali utente. In tal caso, immettere le credenziali appropriate e fare clic su OK.

Se è stata abilitata la verifica modulo, verrà visualizzata la finestra di dialogo Verifica modulo.

5. Attendere il completamento della verifica e fare clic su Avanti per continuare.

Verrà visualizzata la finestra di dialogo Directory principali | master, con un elenco delle directory identificate sul master.

6. Fare clic su Avanti.

Viene visualizzata la schermata Directory principali di replica.

7. Impostare la directory di replica e fare clic su Avanti.

Viene visualizzata la schermata Proprietà scenario.

8. Configurare le proprietà in base alle proprie esigenze e fare clic su Avanti. Per ulteriori informazioni sulla configurazione delle proprietà dello scenario, si rimanda alla *Guida per l'amministratore di Arcserve RHA*.

Viene visualizzata la schermata Proprietà di master e replica.

9. Configurare le proprietà in base alle proprie esigenze e fare clic su Avanti. Per ulteriori informazioni sulla configurazione delle proprietà master e di replica, si rimanda alla *Guida per l'amministratore di Arcserve RHA*.

Nota: per la proprietà delle credenziali utente master e di replica è necessario immettere il nome utente e la password corrispondenti con autorizzazioni di controllo completo nella directory padre disponibile nella directory principale.

Viene visualizzata la schermata Proprietà avanzamento.

10. Configurare le proprietà di avanzamento in base alle proprie esigenze e fare clic su Avanti.

Nota: i valori predefiniti consigliati sono già definiti. Per ulteriori informazioni sulla configurazione delle proprietà di avanzamento, si rimanda alla *Guida per l'amministratore di Arcserve RHA*.

Viene visualizzata la schermata Avvio replica inversa e di avanzamento.

11. Effettuare le proprie selezioni per le opzioni seguenti, in modo da controllare in modo automatico l'avanzamento e la replica inversa, quindi fare clic su Avanti.

Avvio avanzamento

Specifica se inizializzare un avanzamento in modo automatico o manuale.

L'avanzamento automatico ha inizio quando il server master non disponibile oppure quando viene rilevato un errore di database. L'avanzamento manuale viene avviato dall'amministratore. In entrambi i casi, viene fornito un messaggio di notifica in caso di errore.

Avvio replica inversa

Specifica se inizializzare una replica inversa in modo automatico o manuale. Dopo un avanzamento, lo scenario viene interrotto e viene avviata la replica inversa.

Nota: si consiglia di **non** impostare come automatiche entrambe queste opzioni in un ambiente di produzione.

Viene visualizzata la schermata Verifica scenario.

12. Attendere il completamento del processo di Verifica scenario.

Per continuare, è necessario risolvere gli eventuali errori rilevati dalla Verifica scenario. Risolvere anche gli eventuali avvisi elencati. Dopo aver apportato le modifica, fare clic su Riprova per ripetere la verifica.

13. Fare clic su Avanti.

Viene visualizzata la finestra di dialogo Esecuzione scenario.

14. Fare clic su Esegui ora per avviare la sincronizzazione e attivare lo scenario. Fare clic su Fine per eseguire lo scenario in seguito.

Per zone non globali su Solaris

Consente di creare scenari nella zona globale, da cui è possibile gestire tutti gli scenari. La maggior parte delle fasi sono uguali, ad eccezione delle seguenti:

1. Immettere l'indirizzo IP della zona globale come indirizzo IP master.
2. Utilizzare i seguenti comandi per ottenere le informazioni sulla zona sulla directory principale della zona:

```
/usr/sbin/zoneadm list -vi  
zonecfg -z <zonename> info
```
3. Durante l'impostazione della directory principale, aggiungere manualmente la directory principale della zona non globale al percorso che si desidera proteggere. In questo caso, non è possibile utilizzare il rilevamento automatico per le applicazioni come Oracle.

Avvio di uno scenario

È possibile avviare uno scenario utilizzando la Gestione.

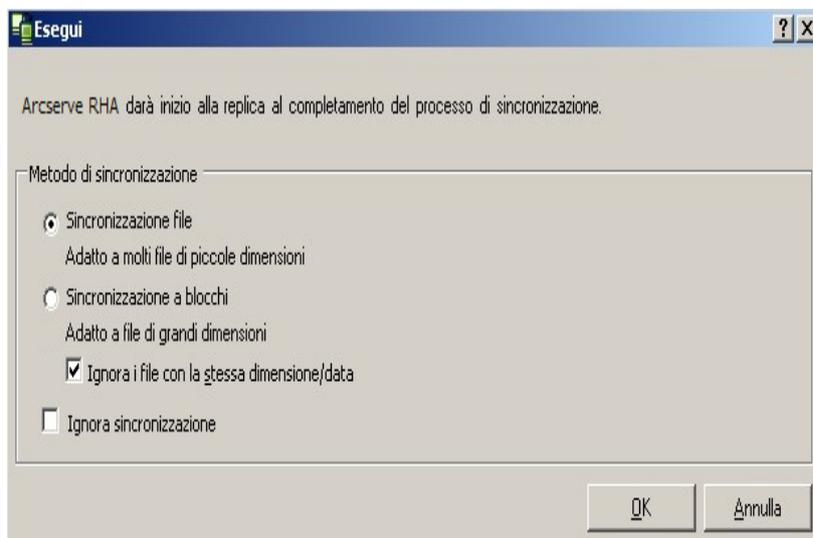
Per avviare uno scenario, procedere come segue:

1. Selezioni lo scenario che si desidera eseguire dal riquadro Scenario.
2. Fare clic su Esegui sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Risultati verifica che richiede di approvare l'esecuzione dello scenario.

3. Fare clic su Esegui. Utilizzare il pulsante Avanzate per visualizzare i dettagli dello scenario del master e della replica.

Viene visualizzata la finestra di dialogo Esegui.



Nota: quando si procede all'avvio di scenari basati su UNIX, la sincronizzazione file/a blocchi non può essere ignorata.

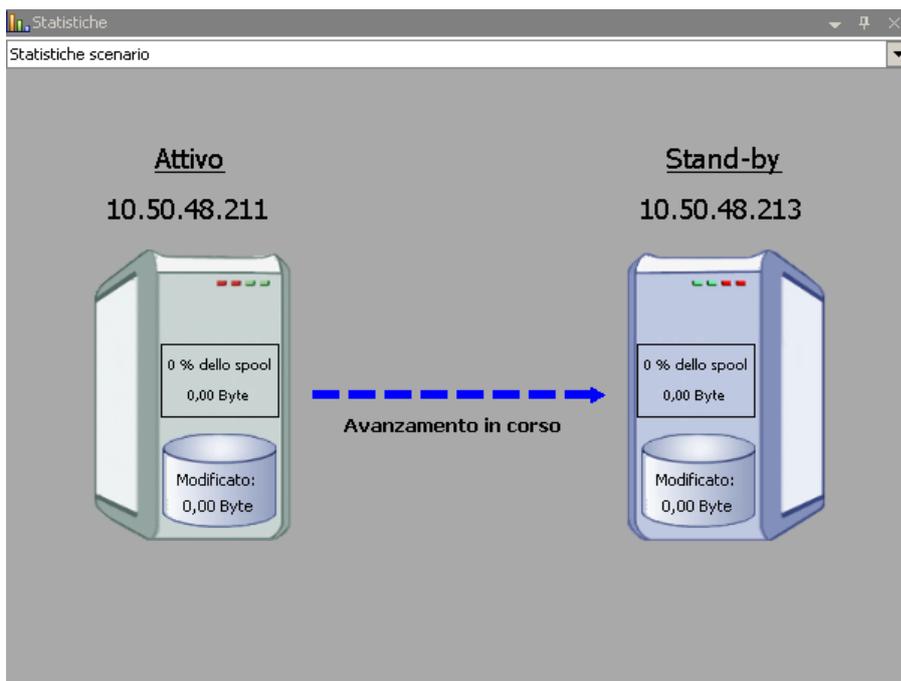
4. Scegliere Sincronizzazione file e fare clic su OK.

Nota: se si sta eseguendo uno scenario per il server Oracle, deselezionare la casella di controllo Ignora file con la stessa dimensione/data e selezionare Sincronizzazione a blocchi.

La Gestione indica, quindi, che lo scenario è in esecuzione tramite il simbolo di riproduzione di colore verde posto a sinistra dello scenario.

Scenario	Stato	Prodotto	Server	Modalità		
File Server	In esecuzione	HA/AR	FileServer	In linea		
Host	Modificato	Dati inviati	File inviati	Dati ricevuti	File ricevuti	In spool
localhost	0,00 Byte	0,00 Byte	0	-	-	0,00 B
155.35.75.128						

Quando lo scenario è in esecuzione, viene visualizzata una scheda Statistiche (nella parte inferiore del riquadro all'estremità destra):



inoltre, per impostazione predefinita, viene generato un rapporto al momento dell'esecuzione della sincronizzazione.

Interruzione di uno scenario

È possibile interrompere uno scenario utilizzando la Gestione.

Per interrompere uno scenario, procedere come segue:

1. Fare clic sul pulsante  Interrompi nella barra degli strumenti.

Viene visualizzato un messaggio di conferma in cui si richiede di approvare l'interruzione dello scenario.

2. Fare clic su Sì.

Lo scenario viene interrotto.

Nota: dopo aver interrotto lo scenario, nella Gestione non verrà più visualizzato il simbolo di riproduzione di colore verde a sinistra dello scenario e la scheda Statistiche non sarà più disponibile.

Considerazioni relative agli scenari UNIX/Linux

Per la creazione di scenari UNIX/Linux, è necessario tenere presente le informazioni seguenti.

- Una directory può essere presente solo in uno scenario.
- Per il server Network File Sharing (NFS), installare il modulo nel server NFS e assicurarsi che la directory esportata risieda nella directory principale.

Note:

- ◆ Per NFS v4, assicurarsi di impostare l'opzione `fsid` in `/etc/exports`. Inoltre, assicurarsi che ogni directory esportata abbia un valore `fsid` differente (1-255) se si dispone di più directory esportate. Esempio:

```
cat /etc/exports
/usr/nfsroot *
(rw,sync,no_root_squash,nohide,crossmnt,fsid=5)
```

- ◆ Se la directory principale di Arcserve RHA si trova all'interno della directory esportata NFS, fare riferimento all'[Articolo della Knowledge Base](#).

- SUSE 11 non include il supporto NFS.
- Replica client NFS
 - ◆ Arcserve Replication and High Availability non replica le modifiche apportate sul server NFS, incluse le modifiche apportate da altri client NFS durante l'esecuzione dello scenario.
 - ◆ NFSv4 è supportato solo su SUSE 12, RHEL 7 o Oracle Linux 7 o versioni successive.
 - ◆ Gli ACL NFSv4 vengono replicati solo in altri client NFSv4 che supportano gli ACL NFSv4. In tali casi, la versione e la configurazione del client e server NFS devono essere identiche tra master e replica.
- Con la replica da Windows a UNIX, gli ACL Windows vengono persi.
- Con la replica da UNIX a Windows, UID, GUID, collegamenti simbolici e collegamenti reali vengono persi.
- I nomi dei file su Windows non sono sensibili alla distinzione tra maiuscole e minuscole, pertanto sono possibili conflitti.
- Le directory principali non possono essere intersecate in scenari differenti. Ciò significa che non è possibile creare un secondo scenario di replica che utilizzi la

stessa directory master e la stessa directory principale utilizzate dal primo scenario di replica.

- Per la proprietà delle credenziali utente master e di replica è necessario immettere il nome utente e la password corrispondenti con autorizzazioni di controllo completo nella directory padre disponibile nella directory principale.
- Parametri HA su host UNIX/Linux:
 - ◆ Informazione di sistema: Il controller di dominio Active Directory e le proprietà cluster di MS non sono supportate, per cui i valori sono sempre impostati su *No*. Nel caso della proprietà del server DNS, viene verificato solo il processo server BIND *named*. La proprietà del server DNS è impostata su *Sì* se *named* è in esecuzione, altrimenti è impostata su *No*.
 - ◆ Configurazione di rete: nome NetBIOS non supportato.
- Collegamenti reali supportati. Collegamenti reali non supportati tra file system differenti o tra directory principali sullo stesso file system.
- L'esecuzione simultanea di più scenari provenienti da aree differenti non globali su Solaris non è supportata. Come soluzione si consiglia di creare più scenari a partire dall'area globale di Solaris, quindi gestire tutti gli scenari a partire da tale area.

Nota: verificare che tutte le directory presenti nell'area locale siano accessibili dall'area globale di Solaris.

Capitolo 5: File installati

Durante l'installazione di Arcserve RHA vengono installati file diversi per vari sistemi operativi, come descritto nelle sezioni seguenti.

La presente sezione descrive i seguenti argomenti:

File installati su Red Hat e Novell SUSE Linux Enterprise	42
File installati su IBM AIX	43
File installati su Solaris	44

File installati su Red Hat e Novell SUSE Linux Enterprise

Sulle piattaforme Linux, verranno installati i seguenti file:

File installato	Descrizione
/opt/ARCserveRHA/bin/ws_rep	Il Modulo Arcserve RHA funziona in modalità utente come un daemon. La sua responsabilità principale è quella di collaborare con il modulo kernel xofs (che funge da filtro per il file system), allo scopo di tenere traccia delle modifiche di sistema e propagarle in funzione dello scenario di replica.
/opt/ARCserveRHA/kernel/fs/xofs.*	Un file system proprietario - <i>xofs</i> . Implementato sotto forma di modulo kernel caricabile. Lo scopo principale di <i>xofs</i> è quello di tenere traccia delle modifiche apportate al file system e di inviare notifiche al modulo. <i>Xofs</i> viene caricato durante l'avvio del sistema (tramite /etc/init.d/Arcserve RHA). Nota: <i>.up</i> sta per uniprocessore, mentre <i>smp</i> sta per multiprocessore simmetrico.
/etc/init.d/ARCserveRHA	Lo script utilizzato per avviare e interrompere il modulo.
/etc/pam.d/ws_rep	Necessario affinché Arcserve RHA possa autenticare le connessioni di gestione dalla GUI.
/opt/ARCserveRHA/bin/README	File Leggimi Arcserve RHA
/opt/ARCserveRHA/bin/ws_rep.cfg	Arcserve RHA file di configurazione
/opt/ARCserveRHA/bin/uninstall.sh	Disinstalla il software.

File installati su IBM AIX

Sulle piattaforme AIX, verranno installati i seguenti file:

File installato	Descrizione
/opt/ARCserveRHA/bin/ws_rep	Il Modulo Arcserve RHA funziona in modalità utente come un daemon. La sua responsabilità principale è quella di collaborare con il modulo kernel xofs (che funge da filtro per il file system), allo scopo di tenere traccia delle modifiche di sistema e propagarle in funzione dello scenario di replica.
/opt/ARCserveRHA/bin/xofs.ext	Un file system proprietario - <i>xofs</i> . Implementato sotto forma di estensione kernel caricabile. Lo scopo principale di xofs è quello di tenere traccia delle modifiche apportate al file system e di inviare notifiche al modulo. Xofs viene caricato durante l'avvio del sistema (tramite /opt/ARCserveRHA/bin/ARCserveRHA.rc).
/opt/ARCserveRHA/bin/xoctl	Utilità di supporto (assistente di file system). Precarica xofs durante l'avvio del sistema.
/opt/ARCserveRHA/bin/xoumount	Utilità di supporto (<i>smonta xofs</i>). Analoga all'utilità <i>umount</i> della riga di comando standard. Nota: il comando <i>umounts</i> standard non funziona per xofs nella release corrente di Arcserve RHA.
/opt/ARCserveRHA/bin/ARCserveRHA.rc	Lo script utilizzato per avviare e interrompere il modulo.
/opt/ARCserveRHA/bin/uninstall.sh	Disinstalla il software.

File installati su Solaris

Sulle piattaforme Solaris, verranno installati i seguenti file:

File installato	Descrizione
/opt/CA/ARCserveRHA/bin/ws_rep	Il Modulo Arcserve RHA funziona in modalità utente come un daemon. La sua responsabilità principale è quella di collaborare con il modulo kernel xofs (che funge da filtro per il file system), allo scopo di tenere traccia delle modifiche di sistema e propagarle in funzione dello scenario di replica.
/usr/kernel/fs/xofs e /usr/kernel/fs/sparcv9/xofs	Un file system proprietario - <i>xofs</i> . Implementato sotto forma di modulo kernel caricabile. Lo scopo principale di xofs è quello di tenere traccia delle modifiche apportate al file system e di inviare notifiche al modulo. Caricato a richiesta durante l'avvio dello scenario di replica.
/opt/CA/ARCserveRHA/bin/uninstall.sh	Disinstalla il software.
/opt/CA/ARCserveRHA/bin/configure.sh (zone)	Configura ws_rep in zone non globali.

Capitolo 6: Risoluzione dei problemi

Le seguenti informazioni consentono di risolvere i problemi relativi agli scenari di Arcserve RHA per UNIX/Linux:

- Questa versione di Arcserve RHA fornisce una funzionalità "uninject" che consente a xofs di eseguire lo scaricamento automatico anche in presenza di file aperti durante un'operazione di arresto dello scenario.

La presente sezione descrive i seguenti argomenti:

Scaricamento dei driver xofs	46
L'IP spostato non viene attivato dopo l'avanzamento	48
Il listener di Oracle non accetta la connessione client dopo il failover	49

Scaricamento dei driver xofs

Se nel corso della procedura di disinstallazione alcune directory sono state lasciate inavvertitamente sotto il controllo del driver xofs (ad esempio, se lo scenario era in esecuzione e la directory è stata montata da xofs), non sarà possibile scaricare dal sistema il driver xofs utilizzando la procedura di disinstallazione.

In tal caso, si può procedere al riavvio del computer oppure scaricare manualmente il driver xofs.

Per scaricare i driver xofs, procedere come segue:

1. Verificare la presenza di punti di montaggio xofs che utilizzano il seguente comando:

```
#cat /etc/xofs_mnttab
```

2. Interrompere tutti i processi che implicano la directory. Utilizzare il comando *fuser* per la propria piattaforma per rilevare i processi con file aperti nella directory:

AIX e Solaris

```
#fuser -c <dir_from_xofs_mnttab>
```

Linux

```
#fuser -u <dir_from_xofs_mnttab>
```

3. Utilizzare il seguente comando *umount* per la directory rilevata al passaggio 1.

```
#umount <dir_from_xofs_mnttab>
```

4. Verificare che nessun processo stia utilizzando il driver xofs e scaricarlo manualmente. Seguire le istruzioni specifiche per la propria piattaforma:

AIX

Eseguire come root il comando seguente per verificare se xofs è caricato nel kernel:

```
echo lke | kdb| grep xofs
```

Eseguire come root il comando seguente per scaricare il driver xofs:

```
/opt/CA/ARCserveRHA/bin/xoctl u /opt/CA/ARCserveRHA/bin/xofs.ext
```

Solaris

Eseguire il comando seguente per verificare se il driver è caricato nella memoria:

```
modinfo|grep xofs
```

Eseguire come root il comando seguente per scaricare manualmente il driver xofs:

```
modunload -i <xofs ID>
```

Linux

Eeguire il comando seguente per verificare che il contatore di riferimento del driver xofs sia 0:

```
/sbin/lsmmod|grep xofs
```

Eeguire come root il comando seguente per scaricare manualmente il driver xofs:

```
/sbin/rmmod xofs
```

L'IP spostato non viene attivato dopo l'avanzamento

Valido per Linux

Sintomo:

In seguito al corretto completamento di un avanzamento, se si utilizza l'opzione Sposta IP, l'IP trasferito (sul nuovo server attivo) viene mostrato come non attivo. Sebbene il sistema operativo mostri gli IP come attivati e il ping locale funzioni correttamente, non è possibile accedere all'indirizzo IP da una posizione esterna al server.

Soluzione:

Per risolvere il problema, dopo l'avanzamento eseguire manualmente sul nuovo server attivo il comando ifup per l'IP trasferito. Ad esempio, ifup eth0:1.

Se lo si desidera, dopo l'avanzamento è possibile automatizzare questa operazione mediante la creazione e l'esecuzione di uno script utilizzando l'interfaccia utente RHA.

Per eseguire lo script, accedere a Proprietà High Availability, Azione per esito positivo, Script definiti dall'utente e specificare il nome dello script e il corrispondente percorso completo.

Di seguito viene fornito un esempio di script:

```
#!/bin/bash
ifup eth0:1
```

Il listener di Oracle non accetta la connessione client dopo il failover

Valido per Linux

Sintomo:

Se si utilizza solo l'opzione Sposta IP, per impostazione predefinita il listener di Oracle sul server di replica non accetta la connessione client dopo il failover.

Soluzione:

Questo problema si verifica perché il listener di Oracle rimane in ascolto sull'IP e sulla porta specificati. Quando l'IP viene trasferito alla replica, la connessione viene installata per l'IP di produzione originale e non viene accettata dal listener di Oracle. Per risolvere questo problema, configurare il listener affinché utilizzi l'IP che si desidera spostare.

