Guida sulla sicurezza di Oracle® ZFS Storage Appliance, Release OS8.6.x

N. di parte: E78557-01
Settembre 2016

N. di parte: E78557-01

Accessibilità alla documentazione

Per informazioni sull'impegno di Oracle per l'accessibilità, visitare il sito Oracle Accessibility Program all'indirizzo: http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso il portale Oracle My Oracle Support. Per tutte le necessarie informazioni, si prega di visitare il sito http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oppure http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs per clienti non udenti.

Indice

Guida sulla sicurezza di Oracle ZFS Storage Appliance

Nella presente guida vengono esplorate, analizzate ed evidenziate le considerazioni sulla sicurezza necessarie per creare un sistema di storage sicuro e una comprensione degli obiettivi di sicurezza specifici a livello di team. Prima di configurare l'appliance, è consigliabile leggere la presente guida per usufruire delle funzioni di sicurezza disponibili e creare i livelli di sicurezza necessari.

È anche possibile utilizzare questa guida come riferimento per informazioni più dettagliate relativamente alle considerazioni sulla sicurezza delle diverse funzioni e funzionalità di Oracle ZFS Storage Appliance. Per le procedure di configurazione dell'appliance, consultare *Oracle ZFS Storage Appliance Administration Guide*.

Nelle sezioni riportate di seguito vengono descritte le funzioni e i suggerimenti per la sicurezza di Oracle ZFS Storage Appliance.

- **Operazioni iniziali**: vengono descritte le funzioni di sicurezza per il login durante l'installazione iniziale dell'appliance e i suggerimenti per la sicurezza fisica del sistema.
- **Modello amministrativo**: viene descritto l'accesso remoto mediante BUI e CLI, le limitazioni dell'accesso a BUI e CLI, il modello di applicazione di patch al sistema, gli aggiornamenti rinviati, i bundle di supporto e il backup della configurazione.
- **Utenti dell'appliance**: vengono descritti i ruoli amministrativi, gli utenti che possono amministrare l'appliance e la gestione delle autorizzazioni agli utenti.
- **Liste di controllo dell'accesso**: viene descritto il meccanismo di concessione o negazione dell'accesso a file e directory.
- **Servizi di dati**: vengono descritti i servizi dati supportati dall'appliance e la sicurezza offerta dai diversi servizi di dati.
- **Servizi di directory**: vengono descritti i servizi di directory che è possibile configurare sull'appliance e le relative ramificazioni per la sicurezza.
- **Impostazioni di sistema**: vengono descritte le impostazioni di sistema, come Phone Home, Tag servizio, SMTP, SNMP, Syslog, System Identity, Disk Scrubbing e Preventing Destruction.
- **Log di sicurezza**: vengono descritti i tipi di log relativi alla sicurezza.

Operazioni iniziali

In questa sezione vengono descritte le funzioni di sicurezza per il login durante l'installazione iniziale dell'appliance e i suggerimenti per la sicurezza fisica del sistema.

Installazione iniziale

Oracle ZFS Storage Appliance viene fornito con il software dell'appliance preinstallato. Non è necessario installare il software e non vengono forniti supporti.

L'installazione iniziale viene eseguita con nome di account e password predefiniti. Dopo l'installazione, è necessario modificare la password root predefinita. Se vengono reimpostate le impostazioni predefinite di Oracle ZFS Storage Appliance, viene reimpostata anche la password root predefinita sia per l'appliance che per il processore di servizio.

Durante l'installazione iniziale di Oracle ZFS Storage Appliance, al processore di servizio del sistema sono associati un nome di account e una password predefiniti. Si tratta dell'account predefinito che consente a un amministratore di sistema di effettuare il primo accesso all'appliance, dopo il quale all'amministratore viene richiesto di effettuare le prime operazioni di installazione iniziale del sistema. Una delle operazioni necessarie consiste nell'impostare una nuova password amministrativa per l'appliance, che a sua volta determina la reimpostazione della password predefinita del processore di servizio sullo stesso valore.

Sicurezza fisica

Per controllare l'accesso al sistema, è necessario garantire la sicurezza fisica dell'ambiente informatico. Se, ad esempio, si esegue il login a un sistema lasciandolo incustodito, tale sistema può essere soggetto ad accesso non autorizzato. L'ambiente circostante il computer e l'hardware del computer devono essere sempre protetti fisicamente da accessi non autorizzati.

Oracle ZFS Storage Appliance prevede un accesso limitato tramite l'uso di un dispositivo di sicurezza (ad esempio, accesso tramite chiave, lucchetto, strumento, badge) e il personale autorizzato all'accesso deve essere informato dei motivi delle limitazioni e delle precauzioni da prendere.

Modello amministrativo

In questa sezione viene descritta la sicurezza per il modello amministrativo di Oracle ZFS Storage Appliance.

Accesso amministrativo remoto

In questa sezione viene descritta la sicurezza dell'accesso remoto a Oracle ZFS Storage Appliance.

Browser User Interface

L'interfaccia BUI (Browser User Interface) viene utilizzata per l'amministrazione generale dell'appliance. È possibile utilizzare le schermate BUI Services per visualizzare e modificare i servizi e le impostazioni di accesso remoto.

Le attività di amministrazione vengono eseguite in una sessione del browser HTTPS (HTTP Secure). Le sessioni HTTPS sono cifrate con un certificato autofirmato generato in modo univoco per ciascuna istanza di Oracle ZFS Storage Appliance durante l'installazione iniziale. Le sessioni HTTPS prevedono un timeout predefinito definibile dall'utente di 15 minuti.

Command Line Interface

L'interfaccia CLI (Command Line Interface) può essere utilizzata per eseguire la maggior parte delle stesse azioni amministrative che è possibile eseguire nell'interfaccia BUI.

Secure Shell (SSH) consente agli utenti di eseguire il login a Oracle ZFS Storage Appliance mediante una connessione SSL (Secure Sockets Layer) all'interfaccia CLI. SSH può essere utilizzato anche per eseguire script automatici da un host remoto, ad esempio per recuperare i log giornalieri o le statistiche analitiche.

Autorizzazione utente limitata

L'accesso amministrativo è limitato all'utente root, agli amministratori locali definiti con i privilegi rilevanti e agli utenti autorizzati tramite server di identità quali LDAP (Lightweight Directory Access Protocol) e NIS (Network Information Service).

Oracle ZFS Storage Appliance RESTful API

È possibile utilizzare Oracle ZFS Storage Appliance RESTful API per gestire Oracle ZFS Storage Appliance. L'architettura RESTful si basa su un modello client-server strutturato che consente di reindirizzare i servizi in modo trasparente mediante hub e router standard nonché altri sistemi di rete senza eseguire la configurazione del client.

Oracle ZFS Storage Appliance RESTful API utilizza le stesse credenziali di autenticazione delle interfacce BUI e CLI. Tutte le richieste provenienti dai client esterni vengono autenticate

singolarmente utilizzando le credenziali dell'appliance e vengono eseguite mediante una connessione HTTPS sulla porta 215. L'interfaccia API RESTful supporta le sessioni HTTPS che prevedono un timeout predefinito di 15 minuti definibile dall'utente.

Per informazioni sulla gestione di Oracle ZFS Storage Appliance con l'interfaccia API RESTful, consultare *Oracle ZFS Storage Appliance RESTful API Guide*.

Aggiornamenti del sistema

Per usufruire dei miglioramenti alla sicurezza più recenti, Oracle consiglia di mantenere aggiornato il software del sistema.

Gli aggiornamenti del sistema vengono applicati come intere sostituzioni binarie del software del sistema. Prima dell'aggiornamento, viene creata un'istantanea del pool del sistema in esecuzione. In questo modo un amministratore può eseguire il rollback alla versione precedente, se necessario.

Aggiornamenti rinviati

Un aggiornamento rinviato è una funzione o parte di una funzionalità inclusa in un aggiornamento del sistema, ma non è attivata quando viene eseguito l'aggiornamento del sistema. L'amministratore decide quando o se applicare gli aggiornamenti rinviati. Gli aggiornamenti non applicati durante un aggiornamento del sistema rimangono disponibili durante i successivi aggiornamenti del sistema. Non è possibile selezionare i singoli aggiornamenti da applicare. Quando si sceglie di applicare gli aggiornamenti ritardati, è possibile applicarli tutti o nessuno. Dopo aver applicato un aggiornamento, non è possibile eseguire il rollback a una versione precedente del software del sistema.

Bundle di supporto

Se il sistema è registrato per il supporto Phone Home e si verifica un grave guasto, lo stato del sistema viene inviato a My Oracle Support dove viene esaminato dal personale dell'assistenza tecnica e dove può essere creato un bundle di supporto. Le informazioni sullo stato del sistema inviate a My Oracle Support non contengono dati sull'utente, ma solo informazioni sulla configurazione.

Backup della configurazione

Le configurazioni del sistema possono essere salvate in locale per essere ripristinate in un secondo momento. Questi backup non contengono dati sull'utente; vengono salvate solo le impostazioni della configurazione.

Utenti dell'appliance

Esistono due tipi di utenti di Oracle ZFS Storage Appliance:

- **Utenti dei servizi di dati**: utenti che accedono alle risorse di file e blocco utilizzando i protocolli supportati, quali NFS (Network File System), SMB (Server Message Block), iSCSI (Fibre Channel, Internet Small Computer System Interface), HTTP (Hypertext Transfer Protocol) e FTP (File Transfer Protocol).
- **Utenti amministrativi**: utenti che gestiscono la configurazione e i servizi dell'appliance.

Questa sezione è destinata ai soli utenti amministrativi.

Ruoli per gli utenti amministrativi

È possibile concedere privilegi agli amministratori assegnando loro ruoli personalizzati. Un ruolo è una raccolta di privilegi che è possibile assegnare a un amministratore. È possibile creare diversi ruoli per l'amministratore e l'operatore, con diversi livelli di autorizzazione. È opportuno assegnare ai membri dello staff i ruoli appropriati in base alle loro esigenze, evitando di assegnare privilegi non necessari.

L'uso dei ruoli è più sicuro dell'uso condiviso di password amministrative di accesso completo, ad esempio tramite la comunicazione della password root a tutti gli utenti. I ruoli concedono agli utenti solo determinati insiemi di autorizzazioni. È inoltre possibile identificare i ruoli utente per i singoli nomi utente nei log di controllo. Per impostazione predefinita, è disponibile un ruolo denominato "Basic administration", contenente un numero minimo di autorizzazioni.

Di seguito sono indicati gli utenti amministrativi possibili.

- **Utenti locali**: vengono salvate tutte le informazioni sugli account in Oracle ZFS Storage Appliance.
- **Utenti di directory**: vengono utilizzati gli account NIS o LDAP e le impostazioni di autorizzazione aggiuntive vengono salvate nell'appliance. L'accesso all'appliance deve essere concesso in modo esplicito agli utenti NIS/LDAP esistenti, che possono quindi eseguire il login e amministrare l'appliance. L'accesso non può essere concesso per impostazione predefinita.

Ambiti amministrativi

Le autorizzazioni consentono agli utenti di eseguire attività specifiche, come la creazione di condivisioni, il reboot dell'appliance e l'aggiornamento del software del sistema. I gruppi di autorizzazioni sono denominati ambiti. Ciascun ambito può essere dotato di un insieme di filtri opzionali che consentono di limitare il numero di autorizzazioni. Ad esempio, anziché utilizzare un'autorizzazione per il riavvio di tutti i servizi, è possibile utilizzare un filtro per consentire il riavvio solo del servizio HTTP.

Liste di controllo dell'accesso

Oracle ZFS Storage Appliance fornisce il controllo dell'accesso ai file tramite le liste di controllo dell'accesso (ACL), ossia meccanismi che consentono o negano l'accesso a un determinato file o a una determinata directory.

Il modello di ACL fornito da Oracle ZFS Storage Appliance si basa sul modello di ACL di NFSv4 derivato dalla semantica di Windows ACL. Si tratta di un modello di ACL completo che consente un accesso capillare a file e directory. Ogni file e directory nell'appliance di storage dispone di un'ACL e tutte le decisioni relative al controllo dell'accesso sia per SMB che per NFS vengono sottoposte agli stessi algoritmi per determinare gli utenti a cui è consentito o negato l'accesso ai file e alle directory.

Un'ACL è costituita da una o più ACE (Access Control Entries). Ciascuna ACE contiene una voce per le autorizzazioni che l'ACE concede o nega e indica l'utente a cui l'ACE viene applicata e i flag dei livelli di eredità utilizzati.

Eredità dell'ACL

Le ACL di NFSv4 consentono l'eredità delle singole ACE ai nuovi file e directory creati. L'eredità delle ACE è controllata da diversi flag del livello di eredità impostati da un amministratore sull'ACL durante la relativa configurazione iniziale.

Determinazione dell'accesso all'ACL

Le ACL di NFSv4 dipendono dall'ordine e vengono elaborate dall'alto in basso. Una volta concessa, un'autorizzazione non può essere revocata da un'ACE successiva. Una volta negata, un'autorizzazione non può essere concessa da un'ACE successiva.

ACL per il livello di condivisione di SMB

Un'ACL per il livello di condivisione di SMB è associata a un'ACL di un file o di una directory nella condivisione per determinare le autorizzazioni effettive del file. L'ACL per il livello di condivisione fornisce un altro livello di controllo dell'accesso superiore alle ACL del file e offre configurazioni per il controllo dell'accesso più sofisticate. Le ACL per il livello di condivisione vengono impostate quando il file system viene esportato utilizzando il protocollo SMB. Se il file system non viene esportato utilizzando il protocollo SMB, l'impostazione dell'ACL per il livello di condivisione non ha alcun effetto. Per impostazione predefinita, le ACL per il livello di condivisione concedono il controllo completo a tutti gli utenti.

Proprietà dell'ACL ZFS

Il comportamento e le proprietà di ereditarietà dell'ACL sono applicabili solo per i client NFS. I client SMB utilizzano l'esatta semantica Windows che ha la precedenza sulle proprietà ZFS. La differenza consiste nel fatto che i client NFS utilizzano la semantica POSIX, al contrario dei client SMB. Le proprietà sono compatibili principalmente con POSIX.

Servizi di dati

Nella seguente tabella viene fornita una descrizione e vengono indicate le porte utilizzate per ciascun servizio di dati.

TABELLA 1 Servizi di dati

SERVIZIO	DESCRIZIONE	PORTE USATE
NFS	Accesso al file system mediante i protocolli NFSv3 e NFSv4	111 e 2049
iSCSI	Accesso al LUN mediante il protocollo iSCSI	3260 e 3205
SMB	Accesso al file system mediante il protocollo SMB	SMB su NetBIOS 139 SMB su TCP 445 Datagramma NetBIOS 138 Nome servizio NetBIOS 137
Virus Scan	Scansione antivirus nel file system	
FTP	Accesso al file system mediante il protocollo FTP	21
HTTP	Accesso al file system mediante il protocollo HTTP	80

SERVIZIO	DESCRIZIONE	PORTE USATE
HTTPS	Per le connessioni sicure in entrata	443
NDMP	Servizio host NDMP	10000
Remote Replication	Replica remota	216 e 217
Encryption	Cifratura trasparente per i file system e i LUN	
Shadow Migration	Migrazione dati shadow	
SFTP	Accesso al file system mediante il protocollo SFTP	218
TFTP	Accesso al file system mediante il protocollo TFTP	
Storage Area Network	Gruppi di destinazioni e responsabili avvio di una rete SAN (Storage Area Network)	

Numero minimo di porte necessarie

Per rendere sicura una rete, è possibile creare firewall. I numeri di porta vengono utilizzati per creare firewall e identificare in modo univoco una transazione su una rete specificando l'host e il servizio.

Nell'elenco seguente vengono indicate le porte minime necessarie per la creazione dei firewall.

Porte in entrata

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

Porte di entrata aggiuntive in caso di utilizzo di condivisione dei file HTTP (in genere non necessarie):

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

Porte in uscita

- tcp/80 (WEB)

Nota - Per la replica, utilizzare i tunnel GRE (Generic Routing Encapsulation), se possibile. Ciò consente di eseguire il traffico sulle interfacce backend e di evitare il firewall dove il traffico potrebbe essere rallentato. Se i tunnel GRE non sono disponibili sul core NFS, è necessario eseguire la replica sull'interfaccia frontend. In questo caso, anche le porte 216 e 217 devono essere aperte.

Opzioni di autenticazione e cifratura NFS

Per impostazione predefinita, le condivisioni NFS vengono allocate con l'autenticazione RPC AUTH_SYS. È anche possibile configurarle per essere condivise con la sicurezza Kerberos. Utilizzando l'autenticazione AUTH_SYS, l'ID utente (UID) e l'ID gruppo (GID) UNIX del client vengono trasmessi senza autenticazione sulla rete dal server NFS. Poiché questo meccanismo di autenticazione può essere facilmente aggirato da qualsiasi utente con accesso root a un client, è preferibile utilizzare una delle altre modalità di sicurezza disponibili.

È possibile specificare ulteriori controlli dell'accesso per ciascuna condivisione in modo da consentire o negare l'accesso alle condivisioni per host, domini DNS o reti specifiche.

Modalità di sicurezza

Le modalità di sicurezza vengono impostate per ciascuna condivisione. Nell'elenco riportato di seguito vengono descritte le impostazioni disponibili per la sicurezza Kerberos.

- **krb5**: autenticazione dell'utente finale tramite Kerberos V5.
- **krb5i**: krb5 con aggiunta della protezione dell'integrità (i pacchetti di dati sono a prova di manomissione).
- **krb5p**: krb5i con l'aggiunta della protezione della privacy (i pacchetti dati sono a prova di manomissione e cifrati).

Nell'impostazione della modalità di sicurezza è anche possibile specificare combinazioni di tipi Kerberos. Le modalità di sicurezza combinate consentono l'attivazione dei client con qualsiasi tipo Kerberos elencato.

Tipi Kerberos

- **sys**: autenticazione del sistema.
- **krb5**: solo Kerberos v5, i client devono essere attivati utilizzando questo tipo.
- **krb5:krb5i**: Kerberos v5, con integrità, i client possono essere attivati utilizzando qualsiasi tipo elencato.
- **krb5i**: solo integrità di Kerberos v5, i client devono essere attivati utilizzando questo tipo.
- **krb5:krb5i:krb5p**: Kerberos v5, con integrità o privacy, i client possono essere attivati utilizzando qualsiasi tipo elencati.
- **krb5p**: solo privacy di Kerberos v5, i client devono essere attivati utilizzando questo tipo.

Servizi di dati iSCSI

Quando si configura un LUN in Oracle ZFS Storage Appliance, è possibile esportare il volume su una destinazione iSCSI. Il servizio iSCSI consente ai responsabili avvio iSCSI di accedere alle destinazioni utilizzando il protocollo iSCSI.

Questo servizio supporta l'individuazione, la gestione e la configurazione mediante il protocollo iSNS. Il servizio iSCSI supporta sia l'autenticazione unidirezionale (dove la destinazione autentica il responsabile avvio) che l'autenticazione bidirezionale (dove la destinazione e il responsabile avvio si autenticano a vicenda) tramite CHAP (Challenge-Handshake Authentication Protocol). Il servizio supporta inoltre la gestione dei dati dell'autenticazione CHAP in un database RADIUS (Remote Authentication Dial-In User Service).

Il sistema esegue in primo luogo l'autenticazione, quindi l'autorizzazione, in due operazioni indipendenti. Se il responsabile avvio locale è dotato di un nome CHAP e di un valore segreto CHAP, il sistema esegue l'autenticazione. Se il responsabile avvio locale non dispone di proprietà CHAP, il sistema non esegue alcuna autenticazione e, pertanto, tutti i responsabili avvio sono idonei per l'autorizzazione.

Il servizio iSCSI consente di specificare un elenco globale dei responsabili avvio che è possibile utilizzare nei gruppi di responsabili avvio. Quando si utilizza iSCSI e l'autenticazione CHAP, è possibile utilizzare RADIUS come protocollo iSCSI che trasferisce tutte le autenticazioni CHAP al server RADIUS selezionato.

Supporto RADIUS

RADIUS è un sistema che consente id utilizzare un server centralizzato per eseguire l'autenticazione CHAP per conto dei nodi di storage. Quando si utilizza iSCSI e l'autenticazione CHAP, è possibile selezionare RADIUS per il protocollo iSCSI, che può essere applicato sia a iSCSI che a iSER (iSCSI Extensions for RDMA) e trasferisce tutte le autenticazioni CHAP al server RADIUS selezionato.

Per consentire a Oracle ZFS Storage Appliance di eseguire l'autenticazione CHAP utilizzando RADIUS, è necessario che si verifichino le condizioni elencate di seguito.

- L'appliance deve specificare l'indirizzo del server RADIUS e un valore segreto da utilizzare per la comunicazione con tale server RADIUS.
- Il server RADIUS deve avere una voce (ad esempio, nel file dei client) che indichi l'indirizzo dell'appliance e lo stesso valore segreto di cui sopra.
- Il server RADIUS deve avere una voce (ad esempio, nel file degli utenti) che indichi il nome CHAP e il valore segreto CHAP corrispondente per ciascun responsabile avvio.

- Se il responsabile avvio utilizza il proprio nome IQN come nome CHAP (configurazione consigliata) e l'appliance non richiede una voce Initiator separata per ciascuna casella Initiator, il server RADIUS può eseguire tutte le operazioni di autenticazione.
- Se il responsabile avvio utilizza un nome CHAP separato, l'appliance deve avere una voce Initiator per il responsabile avvio che specifica il mapping da un nome IQN al nome CHAP. Tale voce Initiator non deve specificare il valore segreto CHAP per il responsabile avvio.

Servizi di dati SMB

Il protocollo SMB, anche denominato CIFS (Common Internet File System), fornisce in primo luogo l'accesso condiviso ai file su una rete Microsoft Windows. Fornisce anche l'autenticazione.

Le opzioni SMB elencate di seguito presentano implicazioni relativamente alla sicurezza.

- **Restrict Anonymous Access to Share List**: questa opzione richiede ai client di effettuare l'autenticazione utilizzando SMB prima di ricevere un elenco di condivisioni. Se questa opzione è disabilitata, i client anonimi possono accedere all'elenco di condivisioni. Per impostazione predefinita, questa opzione è disabilitata.
- **SMB Signing Enabled**: questa opzione consente l'interoperabilità con i client SMB utilizzando la funzione di firma SMB. Se questa opzione è abilitata, verrà eseguita la verifica della firma di un pacchetto firmato. Se l'opzione è disabilitata, un pacchetto privo di firma verrà accettato senza verifica della firma. Per impostazione predefinita, questa opzione è disabilitata.
- **SMB Signing Required**: questa opzione può essere utilizzata quando è necessaria la firma SMB. Quando l'opzione è abilitata, tutti i pacchetti SMB devono essere firmati oppure verranno rifiutati. I client che non supportano la firma SMB non possono connettersi al server. Per impostazione predefinita, questa opzione è disabilitata.
- **Enable Access-based Enumeration**: l'impostazione di questa opzione determina il filtraggio delle voci di directory in base alle credenziali del client. Se il client non dispone dell'accesso a un file o una directory, tale file verrà omesso dall'elenco di voci restituite al client. Per impostazione predefinita, questa opzione è disabilitata.

Autenticazione della modalità Domain di Active Directory

In modalità Domain gli utenti vengono definiti in Microsoft Active Directory (AD). I client SMB possono connettersi a Oracle ZFS Storage Appliance utilizzando l'autenticazione Kerberos o NTLM.

Quando un utente si connette con un nome host completamente qualificato di Oracle ZFS Storage Appliance, i client Windows nello stesso dominio o in un dominio sicuro utilizzano l'autenticazione Kerberos; altrimenti utilizzano l'autenticazione NTLM.

Quando un client SMB utilizza l'autenticazione NTLM per connettersi all'appliance, le credenziali dell'utente vengono inoltrate al controller del dominio AD per l'autenticazione. Questo tipo di autenticazione è denominata autenticazione pass-through.

Se i criteri di sicurezza Windows che limitano l'autenticazione NTLM sono definiti, i client Windows devono connettersi all'appliance con un nome host completamente qualificato. Per ulteriori informazioni, consultare questo articolo di Microsoft Developer Network:

`http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx`

Dopo l'autenticazione viene creato un "contesto di sicurezza" per la sessione SMB dell'utente. L'utente rappresentato dal contesto di sicurezza ha un descrittore di sicurezza (SID) univoco. Il SID denota la proprietà del file e viene utilizzato per determinare i privilegi di accesso al file.

Autenticazione della modalità Workgroup

In modalità Workgroup gli utenti vengono definiti a livello locale in Oracle ZFS Storage Appliance. Quando un client SMB si connette a un'appliance in modalità Workgroup, gli hash del nome utente e della password di tale utente vengono utilizzati per autenticare l'utente in locale.

Il livello di compatibilità con LAN Manager (LM) viene utilizzato per specificare il protocollo utilizzato quando l'appliance è in modalità Workgroup.

L'elenco seguente mostra il comportamento di Oracle ZFS Storage Appliance per ciascun livello di compatibilità con LM.

- Livello 2: accetta l'autenticazione LM, NTLM e NTLMv2.
- Livello 3: accetta l'autenticazione LM, NTLM e NTLMv2.
- Livello 4: accetta l'autenticazione NTLM e NTLMv2.
- Livello 5: accetta solo l'autenticazione NTLMv2.

Una volta autenticato correttamente l'utente Workgroup, viene creato un contesto di sicurezza. Viene creato un SID univoco per gli utenti definiti nell'appliance utilizzando una combinazione del SID del computer e dell'UID dell'utente. Tutti gli utenti locali sono definiti come utenti UNIX.

Gruppi locali e privilegi

I gruppi locali sono i gruppi di utenti del dominio che forniscono privilegi aggiuntivi a tali utenti. Gli amministratori possono ignorare le autorizzazioni del file per modificare la proprietà dei file. Gli operatori di backup possono ignorare i controlli di accesso ai file per il backup e il ripristino dei file.

Operazioni amministrative tramite Microsoft Management Console

Per accertarsi che l'accesso alle operazioni amministrative sia consentito solo agli utenti appropriati, esistono alcune limitazioni di accesso alle operazioni eseguite in remoto utilizzando Microsoft Management Console (MMC).

L'elenco riportato di seguito mostra gli utenti e le relative operazioni consentite.

- **Utenti standard**: elencano le condivisioni.
- **Membri del gruppo di amministratori**: elencano i file aperti e i file chiusi, disconnettono le connessioni utente, visualizzano i servizi e il log eventi. I membri del gruppo di amministratori possono anche impostare e modificare le ACL per il livello di condivisione.

Virus Scan

Il servizio Virus Scan esegue la scansione per individuare i virus a livello di file system. Quando si accede a un file da un protocollo qualsiasi, il servizio Virus Scan esegue la scansione del file e, se viene rilevato un virus, nega l'accesso e mette il file in quarantena. La scansione viene eseguita da un motore esterno contattato da Oracle ZFS Storage Appliance. Il motore esterno non è incluso nel software dell'appliance.

Una volta eseguita la scansione del file con le ultime definizioni dei virus, non vengono eseguite nuove scansioni finché il file non viene modificato. La scansione antivirus viene fornita principalmente per i client SMB che potrebbero introdurre virus. È possibile utilizzare la scansione antivirus anche per i client NFS, ma a causa della modalità di funzionamento del protocollo NFS, non è possibile rilevare un virus rapidamente come nel client SMB.

Motore ritardato per attacchi temporizzati

SMB non implementa un motore ritardato per impedire gli attacchi temporizzati. Si basa sulla struttura crittografica di Oracle Solaris.

Cifratura dei dati in rete

Il servizio SMB utilizza la versione 1 del protocollo SMB, che non supporta la cifratura dei dati in rete.

Servizi di dati FTP

FTP consente l'accesso al file system dai client FTP. Il servizio FTP non consente login anonimi e gli utenti devono eseguire l'autenticazione con il nome del servizio configurato.

Il protocollo FTP supporta le impostazioni di sicurezza riportate di seguito. Queste impostazioni sono condivise tra tutti i file system per cui è consentito l'accesso al protocollo FTP.

- **Enable SSL/TLS**: consente le connessioni FTP cifrate con SSL/TLS e garantisce la cifratura della transazione FTP. Per impostazione predefinita, questa opzione è disabilitata. Il server FTP utilizza un certificato di sicurezza autofirmato o un certificato fornito dal cliente.
- **Permit root login**: consente i login FTP per l'utente root. Questa opzione è disattivata per impostazione predefinita, in quanto l'autenticazione FTP utilizza testo semplice, che crea un rischio di sicurezza rispetto alle intrusioni in rete.
- **Maximum number of allowable login attempts**: numero di tentativi di login non riusciti prima che una connessione FTP venga interrotta. Per riprovare, l'utente dovrà riconnettersi. L'impostazione predefinita è 3.
- **Logging Level**: il dettaglio del log.

FTP supporta i log elencati di seguito.

- **proftpd**: eventi FTP che includono tentativi di login riusciti e non riusciti.
- **proftpd_xfer**: log di trasferimento dei file.
- **proftpd_tls**: eventi FTP correlati alla cifratura SSL/TLS.

Servizi di dati HTTP

Il protocollo HTTP fornisce l'accesso ai file system che utilizzano i protocolli HTTP e HTTPS e WebDAV (Web based Distributed Authoring and Versioning) con estensione HTTP. Questo protocollo consente ai client di accedere ai file system condivisi mediane un browser Web o come file system locale, se il software del client lo supporta.

Il server HTTPS utilizza un certificato di sicurezza autofirmato o un certificato fornito dal cliente. Per ottenere un certificato fornito dal cliente, generare una richiesta di firma certificato

(CSR, Certificate Signing Request) e inviarla all'autorità di certificazione per la firma. Una volta che il certificato firmato viene restituito dall'autorità di certificazione, è possibile installarlo sull'appliance. Se un certificato è firmato da un'autorità di certificazione non radice, occorre ottenere certificati anche da una seconda autorità di certificazione e di livello più alto. Per maggiori informazioni sulla gestione dei certificati, fare riferimento alla *guida di amministrazione di Oracle ZFS Storage Appliance.*

Sono disponibili le proprietà elencate di seguito.

- **Require Client Login**: è necessario eseguire l'autenticazione dei client prima che sia consentito l'accesso alla condivisione e che ai file creati sia assegnata la proprietà. Se questa opzione non è impostata, i file creati saranno di proprietà del servizio HTTP, con utente "nobody”.
- **Protocols**: selezionare i metodi di accesso da supportare: HTTP, HTTPS o entrambi.
- **HTTP Port (per le connessioni in ingresso)**: porta HTTP; l'impostazione predefinita è la porta 80.
- **HTTPS Port (per le connessioni sicure in ingresso)**: porta HTTP. La porta predefinita è la 443.

Quando l'opzione Require Client Login è abilitata, Oracle ZFS Storage Appliance nega l'accesso ai client che non forniscono credenziali di autenticazione valide per un utente locale, un utente NIS o un utente LDAP. L'autenticazione Active Directory non è supportata. È supportata solo l'autenticazione HTTP di base. A meno che non si utilizzi HTTPS, il nome utente e la password vengono trasmessi senza cifratura e questo potrebbe non essere appropriato per tutti gli ambienti. Se l'opzione Require Client Login è disabilitata, l'appliance non tenta di eseguire l'autenticazione delle credenziali.

Indipendentemente dall'autenticazione, le autorizzazioni non vengono mascherate dai file e dalle directory create. I nuovi file creati prevedono autorizzazioni in lettura e scrittura per tutti gli utenti. Le nuove directory create prevedono autorizzazioni in lettura, scrittura ed esecuzione per tutti gli utenti.

Servizi di dati NDMP

Il protocollo Network Data Management Protocol (NDMP) consente a Oracle ZFS Storage Appliance di partecipare alle operazioni di backup e ripristino basate su NDMP controllate da un client NDMP remoto denominato Data Management Application (DMA). Utilizzando NDMP, è possibile eseguire il backup e il recupero dei dati degli utenti dell'appliance (ad esempio, i dati memorizzati in condivisioni create dall'amministratore sull'appliance) sia in dispositivi collegati in locale, come le unità nastro, che in sistemi remoti. È possibile eseguire il backup e il recupero dei dispositivi collegati in locale tramite DMA.

Servizi di dati per la replica remota

La replica remota di Oracle ZFS Storage Appliance facilita la replica di progetti e condivisioni. Questo servizio consente di visualizzare le appliance che hanno replicato i dati in un'appliance specifica e per controllare in quali appliance è possibile replicare una determinata appliance.

Quando questo servizio è abilitato, l'appliance riceve gli aggiornamenti di replica da altre appliance e invia aggiornamenti di replica per i progetti e le condivisioni locali in base alle azioni configurate. Quando il servizio è disabilitato, gli aggiornamenti di replica in ingresso non riescono e non viene replicato alcun progetto o condivisione locale.

La password root per l'appliance remota è necessaria per configurare le destinazioni della replica remota per l'appliance. Tali destinazioni vengono utilizzate per impostare una connessione peer di replica che consente la comunicazione tra le appliance.

Durante la creazione della destinazione, la password root viene utilizzata per confermare l'autenticità della richiesta, nonché produrre e scambiare chiavi di sicurezza che verranno utilizzate per identificare le appliance in comunicazioni successive.

Le chiavi generate vengono memorizzate in modo persistente come parte della configurazione dell'appliance. La password root non viene mai memorizzata in modo persistente né trasmessa senza cifratura. Tutte le comunicazioni dell'appliance, incluso questo scambio iniziale di identità, sono protette mediante SSL.

La funzione di replica offline di Oracle ZFS Storage Appliance riduce tempo, risorse e potenziali errori di dati quando risponde a un set di dati di grandi dimensioni su una rete con ampiezza di banda limitata. La replica offline esporta il flusso di replica su un file nel server NFS, che è possibile spostare fisicamente su un sito di destinazione remoto o facoltativamente copiare su un supporto esterno per la spedizione. Sul sito di destinazione, l'amministratore importa il file contenente il flusso di replica nell'appliance di destinazione.

Per limitare l'accesso al flusso di replica esportato, esporre la condivisione NFS solo all'indirizzo IP delle appliance di origine e di destinazione. Per cifrare i dati, abilitare la cifratura su disco per la condivisione NFS sul server NFS. Per ulteriori informazioni, fare riferimento alla documentazione del server NFS. Si noti che il flusso di replica esportato non viene mai cifrato dall'appliance.

Utilizzo della cifratura dei dati

NOTE SULLA LICENZA: *la cifratura può essere valutata gratuitamente, ma la funzionalità richiede l'acquisto separato di una licenza indipendente per l'uso in produzione. La cifratura è disponibile solo su licenza su Oracle*

ZFS Storage ZS5-4, Oracle ZFS Storage ZS5-2, Oracle ZFS Storage ZS4-4 e Oracle ZFS Storage ZS3-4. Una volta trascorso il periodo di valutazione, tale funzionalità deve essere concessa in licenza o disattivata. Oracle si riserva il diritto di verificare la conformità alla concessione della licenza in qualsiasi momento. Per informazioni, consultare la documentazione "Oracle Software License Agreement ("SLA") e Entitlement for Hardware Systems with Integrated Software Options".

Oracle ZFS Storage Appliance offre la cifratura dei dati trasparente per singole condivisioni (file system e LUN) e per le condivisioni create all'interno di progetti.

Gestione delle chiavi di cifratura

L'appliance include un keystore integrato LOCAL e consente di stabilire una connessione al sistema OKM (Oracle Key Manager). Ogni progetto o condivisione cifrata richiede una chiave di wrapping dai keystore LOCAL o OKM. Le chiavi di cifratura dei dati vengono gestite tramite l'appliance di storage e vengono memorizzate in modo permanente e cifrate mediante la chiave di wrapping dal keystore LOCAL o OKM.

OKM è un sistema di gestione chiavi completo (KMS, Key Management System) in grado di soddisfare le esigenze aziendali in rapida crescita che richiedono la cifratura dei dati basata su storage. Sviluppata per garantire la conformità agli standard aperti, questa funzionalità offre la capacità, la scalabilità e l'interoperabilità necessarie per gestire le chiavi di cifratura a livello centrale su infrastrutture di storage ampiamente distribuite ed eterogenee.

OKM è in grado di risolvere le problematiche specifiche relative alla gestione delle chiavi di storage, tra cui:

- **Conservazione delle chiavi a lungo termine**: OKM assicura che i dati dell'archivio siano sempre disponibili e conserva in modo sicuro le chiavi di cifratura durante il ciclo di vita completo dei dati.
- **Interoperabilità**: OKM fornisce l'interoperabilità necessaria per supportare una vasta gamma di dispositivi di storage collegati al mainframe o a sistemi aperti utilizzando un servizio di gestione delle chiavi di storage.
- **Alta disponibilità**: grazie a clustering con N nodi attivo, bilanciamento dinamico del carico e failover automatizzato, OKM fornisce alta disponibilità indipendentemente dal fatto che le appliance si trovino nello stesso luogo o che siano distribuite nel resto del mondo.
- **Alta capacità**: OKM gestisce un numero elevato di dispositivi di storage e un numero perfino maggiore di chiavi di storage. Una coppia di appliance in un singolo cluster può fornire servizi di gestione delle chiavi per migliaia di dispositivi di storage e milioni di chiavi di storage.
- **Configurazione flessibile delle chiavi**: le chiavi di ciascun cluster OKM possono essere generate in modo automatico o create singolarmente per un keystore LOCAL o OKM. Gli amministratori della sicurezza hanno il compito di fornire i nomi delle chiavi che, quando

combinati con il keystore, associano una determinata chiave di wrapping a un progetto o a una condivisione.

Conservazione delle chiavi

Le condivisioni e i progetti che utilizzano chiavi OKM in stato disattivato rimangono accessibili. Per impedire l'uso di una chiave OKM, l'amministratore di OKM deve eliminare la chiave in modo esplicito.

Per garantire l'accessibilità alle condivisioni e ai progetti cifrati, eseguire il backup delle configurazioni dell'appliance e dei valori delle chiavi del keystore LOCAL. Se una chiave non risulta più disponibile, tutte le condivisioni o i progetti che utilizzano tale chiave non saranno accessibili. Se la chiave di un progetto non è disponibile, non sarà possibile creare nuove condivisioni nel progetto specifico.

Le chiavi possono risultare non più disponibili per i motivi riportati di seguito.

- Le chiavi sono state eliminate.
- È stato eseguito il rollback a una release che non supporta la cifratura.
- È stato eseguito il rollback a una release in cui le chiavi non sono configurate.
- Sono stati ripristinati i valori predefiniti.
- Il server OKM non è disponibile.

Ciclo di vita delle chiavi di cifratura

Il ciclo di vita delle chiavi di cifratura è flessibile in quanto è possibile modificare le chiavi in qualsiasi momento, senza mettere fuori linea i servizi di dati.

Quando una chiave viene eliminata dal keystore, tutte le condivisioni che utilizzano tale chiave vengono disinstallate e i dati corrispondenti diventano inaccessibili. È necessario eseguire il backup delle chiavi nel keystore OKM utilizzando i servizi di backup di OKM. Il backup delle chiavi nel keystore LOCAL è incluso nell'ambito del backup di configurazione del sistema. Per il keystore LOCAL è anche possibile fornire la chiave in base al valore nella fase di creazione per consentire di memorizzarla in un sistema esterno, che fornisce una funzionalità alternativa di backup/ripristino per chiave.

Servizio dati di migrazione shadow

La migrazione shadow consente la migrazione automatica dei dati da origini esterne o interne e controlla la migrazione automatica in background. Indipendentemente dal fatto che il servizio

sia o meno abilitato, la migrazione dei dati viene eseguita in modo sincrono per le richieste in banda. Lo scopo principale del servizio consiste nel consentire l'ottimizzazione del numero di thread dedicati alla migrazione in background.

Gli accessi NFS su un'origine NFS non sono soggetti al controllo dell'utente di Oracle ZFS Storage Appliance. Gli accessi della migrazione shadow non possono pertanto essere sicuri. Se il server prevede una richiesta Kerberos o simile, l'accesso all'origine viene rifiutato.

Servizi di dati SFTP

SSH File Transfer Protocol (SFTP) consente l'accesso dai file system dai client SFTP. Poiché i login anonimi non sono consentiti, gli utenti devono eseguire l'autenticazione con il servizio con il nome configurato.

Quando si crea una chiave SFTP, è necessario includere la proprietà dell'utente con un'assegnazione utente valida. Le chiavi SFTP sono raggruppate per utente e vengono autenticate tramite SFTP con il nome dell'utente.

Nota - Per motivi di sicurezza, è necessario ricreare le chiavi SFTP esistenti che non includono la proprietà dell'utente, anche se verranno autenticate.

Servizi di dati TFTP

Trivial File Transfer Protocol (TFTP) è un protocollo semplice per il trasferimento dei file. È progettato per essere piccolo e facile da implementare, ma non dispone della maggior parte delle funzioni di sicurezza del protocollo FTP. Il protocollo TFTP consente di leggere e scrivere file solo da un server remoto. Non può elencare directory e attualmente non prevede regole per l'autenticazione degli utenti.

Storage Area Network

In una rete SAN (Storage Area Network) i gruppi di destinazioni e responsabili avvio definiscono gli insiemi di destinazioni e responsabili avvio che è possibile associare a un numero di unità logica (LUN, Logical Unit Number). Un LUN associato a un gruppo di destinazioni è accessibile solo tramite le destinazioni di tale gruppo. Un LUN associato a un gruppo di responsabili avvio è accessibile solo dai responsabili avvio di tale gruppo. I gruppi di destinazioni e responsabili avvio vengono applicati a un LUN quando si crea un LUN. La

creazione del LUN non può essere completata correttamente senza definire almeno un gruppo di destinazioni e un gruppo di responsabili avvio.

Oltre all'autenticazione CHAP (Challenge-Handshake Authentication Protocol), che può essere selezionata solo per l'accesso del responsabile avvio iSCSI/iSER, non viene eseguita alcuna autenticazione.

Nota - L'uso del gruppo di responsabile avvio predefinito può determinare l'esposizione del LUN a responsabili avvio non desiderati o in conflitto.

Servizi di directory

Questa sezione descrive i servizi di directory che è possibile configurare sull'appliance e le relative ramificazioni per la sicurezza.

Network Information Service

Network Information Service (NIS) è un servizio di denominazione per la gestione centralizzata delle directory. Oracle ZFS Storage Appliance può fungere da client NIS per gli utenti e i gruppi per consentire agli utenti NIS di eseguire il login a FTP e HTTP/WebDAV. È anche possibile concedere agli utenti di NIS privilegi per l'amministrazione dell'appliance. L'appliance integra le informazioni del servizio NIS con le proprie impostazioni dei privilegi.

Lightweight Directory Access Protocol

Oracle ZFS Storage Appliance utilizza il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare sia gli utenti amministrativi che gli utenti dei servizi di dati (FTP, HTTP). La sicurezza LDAP su SSL è supportata dall'appliance. Il protocollo LDAP consente di recuperare informazioni su utenti e gruppi e può essere utilizzato nei modi indicati di seguito.

- Fornisce interfacce utente che accettano e visualizzano nomi per utenti e gruppi.
- Associa i nomi a utenti e gruppi, per protocolli di dati, come NFSv4, che utilizzano i nomi.
- Definisce l'appartenenza al gruppo da utilizzare nel controllo dell'accesso.
- Se necessario, consente il passaggio dei dati di autenticazione utilizzati per l'autenticazione amministrativa e di accesso ai dati.

Le connessioni LDAP possono essere utilizzate come meccanismo di autenticazione. Ad esempio, quando un utente tenta di autenticarsi presso Oracle ZFS Storage Appliance,

l'appliance può tentare di autenticarsi presso il server LDAP con le credenziali di tale utente come meccanismo di verifica dell'autenticazione.

Sono disponibili diversi controlli per la sicurezza della connessione LDAP.

- Autenticazione da appliance a server:
  - L'appliance è anonima.
  - L'appliance esegue l'autenticazione utilizzando le credenziali Kerberos dell'utente.
  - L'appliance esegue l'autenticazione utilizzando il nome utente e la password "proxy" specificati.
- Autenticazione da server ad appliance (per accertarsi che sia stato contattato il server corretto):
  - Non sicura.
  - Il server viene autenticato utilizzando Kerberos.
  - Il server viene autenticato utilizzando un certificato TLS.

I dati trasmessi su una connessione LDAP vengono cifrati se si utilizza Kerberos o TLS; in tutti gli altri casi non vengono cifrati. Quando si utilizza TLS, la prima connessione effettuata durante la configurazione non è sicura. In tale fase il certificato del server viene raccolto e utilizzato per l'autenticazione delle connessioni di produzione successive.

Non è possibile importare un certificato Certificate Authority da utilizzare per autenticare più server LDAP, né importare manualmente un determinato certificato del server LDAP.

È supportata solo la versione raw di TLS (LDAPS). Non sono supportate connessioni STARTTLS, che iniziano con una connessione LDAP non sicura, quindi cambiano in una connessione sicura. I server LDAP che richiedono un certificato client non sono supportati.

Mapping di identità

I client possono accedere alle risorse di file su Oracle ZFS Storage Appliance utilizzando SMB o NFS, utilizzando ciascuno un ID utente univoco. Gli utenti di SMB/Windows sono dotati di SID (Security Descriptor), mentre gli utenti di UNIX/Linux sono dotati di UID (User ID). Gli utenti possono inoltre essere membri di gruppi identificati da SID di gruppo (per gli utenti di Windows) o GID (Group ID) per gli utenti di UNIX/Linux.

Negli ambienti in cui si accede alle risorse di file utilizzando entrambi i protocolli, è spesso opportuno stabilire equivalenze di identità nei casi in cui, ad esempio, un utente di UNIX sia equivalente a un utente di Active Directory. Questa operazione è importante per determinare i diritti di accesso alle risorse di file nell'appliance.

Esistono due tipi diversi di mapping di identità che coinvolgono servizi di directory quali Active Directory, LDAP e NIS. È necessario seguire con attenzione le procedure di sicurezza consigliate per il servizio di directory in uso.

Identity Management for UNIX

Microsoft offre una funzione denominata Identity Management for UNIX (IDMU). Questo software è disponibile per Windows Server 2003 e viene fornito con Windows Server 2003 R2 e versioni successive. Questa funzione è parte di un software precedentemente denominato Services for UNIX, quando venduto separatamente.

L'uso principale di IDMU consiste nel supportare Windows come server NIS/NFS. IDMU consente all'amministratore di specificare un numero di parametri correlati a UNIX: UID, GID, shell di login, home directory e simili per i gruppi. Questi parametri vengono resi disponibili utilizzando AD in uno schema simile ma non uguale a RFC 2307 e tramite il servizio NIS.

Quando si utilizza la modalità di mapping IDMU, il servizio di mapping di identità utilizza questi attributi UNIX per creare mapping tra le identità Windows e UNIX. Questo approccio è molto simile al mapping basato su directory, ad eccezione del fatto che il servizio di mapping di identità esegue query sullo schema di proprietà creato dal software IDMU anziché supportare uno schema personalizzato. Quando si utilizza questo approccio, non è possibile utilizzare altri mapping basati su directory.

Mapping basato su directory

Il mapping basato su directory implica l'annotazione di un oggetto LDAP o Active Directory con informazioni sulle modalità di mapping dell'identità a un'identità equivalente nella piattaforma opposta. Questi attributi aggiuntivi associati all'oggetto devono essere configurati.

Mapping basato sul nome

Il mapping basato sul nome implica la creazione di diverse regole per il mapping delle identità in base al nome. Tali regole stabiliscono le equivalenze tra identità Windows e identità UNIX.

Mapping effimero

Se per un determinato utente non è possibile utilizzare una regola di mapping basata sul nome, a tale utente vengono assegnate credenziali temporanee tramite un mapping effimero, a meno che non sia bloccato da un mapping di rifiuto. Quando un utente di Windows con un nome

UNIX effimero crea un file sul sistema, i client Windows che accedono al file utilizzando SMB rilevano che il file è di proprietà di tale identità Windows. I client NFS, tuttavia, rilevano che il file è di proprietà di "nobody".

Impostazioni del sistema

Nella sezione seguente sono descritte le impostazioni di sicurezza del sistema disponibili.

Phone Home

Il servizio Phone Home viene utilizzato per gestire la registrazione di Oracle ZFS Storage Appliance nonché il servizio di supporto remoto Phone Home. In questi messaggi non vengono trasmessi dati o metadati sull'utente.

La registrazione connette Oracle ZFS Storage Appliance con il portale di inventario di Oracle, dal quale è possibile gestire l'apparecchiatura Oracle. Per utilizzare il servizio Phone Home, è necessario effettuare la registrazione.

Il servizio Phone Home comunica con il supporto Oracle per fornire quanto indicato di seguito.

- **Report dei problemi**: il sistema segnala a Oracle i problemi attivi per la risposta automatica del servizio. A seconda della natura del problema, è possibile che venga aperto un caso di supporto.
- **Heartbeat**: ogni giorno vengono inviati a Oracle messaggi heartbeat per indicare che il sistema è attivo e funzionante. Il supporto Oracle potrebbe segnalare al contatto tecnico un account in cui uno dei sistemi attivati non ha inviato alcun messaggio heartbeat per un periodo troppo prolungato.
- **Configurazione di sistema**: a Oracle vengono inviati messaggi periodici in cui sono descritte la configurazione e le versioni software e hardware correnti, nonché la configurazione di storage.

Tag servizio

I tag servizio facilitano l'inventario e il supporto dei prodotti consentendo l'invio di query a Oracle ZFS Storage Appliance su dati simili a quelli indicati di seguito.

- Numero di serie del sistema
- Tipo di sistema
- Numeri di versione software

È possibile registrare i tag servizio presso il supporto Oracle per tenere traccia facilmente dell'apparecchiatura Oracle e per velocizzare le chiamate del servizio. I tag servizio sono abilitati per impostazione predefinita.

Simple Mail Transfer Protocol

Simple Mail Transport Protocol (SMTP) invia tutti i messaggi di posta generati da Oracle ZFS Storage Appliance, in genere in risposta agli avvisi configurati. SMTP non accetta messaggi di posta esterni, ma invia solo messaggi generati automaticamente dall'appliance stessa.

Per impostazione predefinita, il servizio SMTP utilizza DNS (record MX) per determinare dove inviare i messaggi di posta. Se DNS non è configurato per il dominio dell'appliance oppure se i record MX DNS del dominio di destinazione per la posta in uscita non sono configurati correttamente, l'appliance può essere configurata per inoltrare tutti i messaggi di posta tramite un server di posta in uscita.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) fornisce due funzioni in Oracle ZFS Storage Appliance: le informazioni sullo stato dell'appliance possono essere trasmesse da SNMP e gli avvisi possono essere configurati per l'invio di trap SNMP. Le versioni v1, v2c e v3 di SNMP sono disponibili se è abilitato questo servizio. L'appliance supporta un massimo di 128 interfacce di rete fisica e logica.

Messaggio syslog

Un messaggio syslog è un messaggio di piccolo evento trasmesso da Oracle ZFS Storage Appliance a uno o più sistemi remoti. Syslog fornisce le due funzioni dell'appliance indicate di seguito.

- Gli avvisi possono essere configurati per l'invio di messaggi syslog a uno o più sistemi remoti.
- I servizi nell'appliance che supportano syslog possono essere dotati di messaggi syslog inoltrati a sistemi remoti.

È possibile configurare syslog per l'uso del formato di output classico descritto da RFC 3164 oppure per l'uso del formato di output più recente con versione descritto da RFC 5424. I messaggi syslog vengono trasmessi come datagrammi UDP. Pertanto, sono soggetti a essere eliminati dalla rete o possono non essere inviati affatto se la memoria del sistema di invio è

insufficiente o la rete è sufficientemente congestionata. Gli amministratori devono pertanto considerare la possibilità che in scenari di problemi complessi in una rete alcuni messaggi siano mancanti o siano stati eliminati.

Il messaggio contiene gli elementi indicati di seguito.

- Una utility che descrive il tipo di componente del sistema che ha emesso il messaggio.
- Un'indicazione della gravità della condizione associata al messaggio.
- A timestamp describing the time of the associated event in UTC.
- Un nome host che descrive il nome canonico dell'appliance.
- Un tag che descrive il nome del componente del sistema che ha emesso il messaggio.
- Un messaggio che descrive l'evento stesso.

System Identity

Questo servizio fornisce la configurazione per il nome e la posizione del sistema. In caso di spostamento dell'appliance in una posizione diversa in rete o di ridefinizione del relativo scopo, potrebbe essere necessario modificare queste informazioni.

Disk Scrubbing

La pulizia dei dischi dovrebbe essere eseguita regolarmente per consentire a Oracle ZFS Storage Appliance di rilevare e correggere i dati danneggiati su disco. La pulizia dei dischi è un processo in background che legge i dischi durante i periodi di inattività per rilevare errori di lettura irreversibili in settori a cui non si accede di frequente. Il rilevamento tempestivo di questi errori in settori latenti è importante per ridurre la perdita di dati.

Preventing Destruction

Quando la funzione Prevent Destruction è abilitata, non è possibile eliminare la condivisione o il progetto. Ciò include l'eliminazione di una condivisione tramite cloni dipendenti, l'eliminazione di una condivisione in un progetto o l'eliminazione di un pacchetto di replica. Tuttavia non ha effetto sulle condivisioni eliminate tramite gli aggiornamenti della replica. Se una condivisione viene eliminata in Oracle ZFS Storage Appliance che rappresenta l'origine per la replica, viene eliminata la condivisione corrispondente sulla destinazione, anche se questa proprietà è impostata.

Per eliminare la condivisione, è necessario prima disattivare in modo esplicito la proprietà come operazione separata. Questa proprietà è disattivata per impostazione predefinita.

Log di sicurezza

In questa sezione vengono descritte le funzioni di registrazione correlate alla sicurezza.

Log di controllo

Nel log di controllo vengono registrati gli eventi dell'attività dell'utente, inclusi il login e il logout dalle interfacce BUI e CLI, nonché le azioni amministrative. La tabella seguente mostra alcuni esempi di voci del log di controllo come vengono visualizzati nell'interfaccia BUI:

TABELLA 2 Record del log di controllo

Ora	Utente	Host	Riepilogo	Annotazione sessione
2013-10-12 05:20:24	root	galaxy	Disabled ftp service	
2013-10-12 03:17:05	root	galaxy	User logged in	
2013-10-11 22:38:56	root	galaxy	Browser session timed out	
2013-10-11 21:13:35	root	<console>	Enabled ftp service	

Log Phone Home

Se si utilizza Phone Home, in questo log sono riportati gli eventi di comunicazione con il supporto Oracle. La tabella seguente mostra un esempio di voce di Phone Home come viene visualizzata nell'interfaccia BUI:

TABELLA 3 Record del log Phone Home

Ora	Descrizione	Risultato
2013-10-12 05:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK

Ulteriori informazioni

È possibile trovare informazioni di prodotto complete per Oracle ZFS Storage Appliance nella seguente posizione:

https://docs.oracle.com

Quando si utilizza l'interfaccia BUI per configurare Oracle ZFS Storage Appliance, è possibile fare clic sul collegamento Help in alto a destra in tutte le schermate per visualizzare la Guida per la schermata specifica.