



Informazioni sul controllo degli accessi in base al ruolo

SnapManager for SAP

NetApp
April 19, 2024

Sommario

- Informazioni sul controllo degli accessi in base al ruolo 1
- Abilitare il controllo degli accessi in base al ruolo 2
- Impostare ruoli e funzionalità di controllo degli accessi in base al ruolo 2

Informazioni sul controllo degli accessi in base al ruolo

RBAC (role-based access control) consente di controllare chi ha accesso alle operazioni SnapManager. RBAC consente agli amministratori di gestire gruppi di utenti definendo ruoli e assegnando utenti a tali ruoli. Si consiglia di utilizzare RBAC SnapManager in ambienti in cui RBAC è già in uso.

RBAC include i seguenti componenti:

- Risorse: Volumi e LUN che conservano i file di dati che compongono il database.
- Funzionalità: Tipi di operazioni che possono essere eseguite su una risorsa.
- Utenti: Persone alle quali si concedono funzionalità.
- Ruoli: Un insieme di risorse e funzionalità consentite sulle risorse. Assegnare un ruolo specifico a un utente che deve eseguire tali funzionalità.

Attivare RBAC in SnapDrive. È quindi possibile configurare funzionalità specifiche per ruolo nell'interfaccia grafica utente o nell'interfaccia della riga di comando di Operations Manager Web. I controlli RBAC vengono eseguiti nel server DataFabric Manager.

La tabella seguente elenca alcuni ruoli e le attività tipiche, come impostato in Operations Manager.

Ruolo	Attività tipiche
Amministratore di base SAP	<ul style="list-style-type: none">• Creazione, manutenzione e monitoraggio di un database Oracle che risiede su un host• Pianificazione e creazione di backup del database• Garantire che i backup siano validi e possano essere ripristinati• Cloning di database
Amministratore del server	<ul style="list-style-type: none">• Configurazione di aggregati e sistemi storage• Monitoraggio dei volumi per lo spazio libero• Provisioning dello storage su richiesta degli utenti• Configurazione e monitoraggio del mirroring del disaster recovery
Storage architect	<ul style="list-style-type: none">• Prendere decisioni architetturali sullo storage• Pianificazione della crescita della capacità dello storage• Pianificazione delle strategie di disaster recovery• Delegare le funzionalità ai membri del team

Se RBAC è in uso (vale a dire che Operations Manager è installato e RBAC è attivato in SnapDrive), l'amministratore dello storage deve assegnare le autorizzazioni RBAC a tutti i volumi e i sistemi di storage per i file di database.

Abilitare il controllo degli accessi in base al ruolo

Il RBAC (Role-Based Access Control) di SnapManager viene attivato tramite SnapDrive. All'installazione di SnapDrive, RBAC viene disattivato per impostazione predefinita. Dopo aver attivato RBAC in SnapDrive, SnapManager esegue le operazioni con RBAC attivato.

A proposito di questa attività

Il `snapdrive.config` File in SnapDrive (file in RBAC) imposta molte opzioni, una delle quali attiva RBAC.

La documentazione di SnapDrive contiene dettagli su SnapDrive.

Fasi

1. Aprire `snapdrive.conf` in un editor.
2. Attivare RBAC modificando il valore di `rbac-method` parametro da **native** a **dfm**.

Il valore predefinito per questo parametro è **native**, Che disattiva RBAC.

["Documentazione sul sito di supporto NetApp"](#)

Impostare ruoli e funzionalità di controllo degli accessi in base al ruolo

Dopo aver attivato RBAC (role-based access control) per SnapManager utilizzando SnapDrive, è possibile aggiungere utenti e funzionalità RBAC ai ruoli per eseguire operazioni SnapManager.

Cosa ti serve

È necessario creare un gruppo nel server Data Fabric Manager e aggiungerlo ai sistemi di storage primario e secondario. Eseguire i seguenti comandi:

- `dfm group create smsap_grp`
- `dfm group add smsap_grpprimary_storage_system`
- `dfm group add smsap_grpsecondary_storage_system`

A proposito di questa attività

È possibile utilizzare l'interfaccia Web di Operations Manager o l'interfaccia a riga di comando del server Data Fabric Manager (CLI) per modificare le funzionalità e i ruoli RBAC.

La tabella elenca le funzionalità RBAC necessarie per eseguire le operazioni SnapManager:

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Creazione del profilo o aggiornamento del profilo	SD.Storage.Read (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset)
Protezione del profilo	DFM.Database.Write (smsap_grp) SD.Storage.Read (smsap_grp) SD.Config.Read (smsap_grp) SD.Config.Write (smsap_grp) SD.Config.Delete (smsap_grp) GlobalDataProtection	Nessuno
Creazione del backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Delete (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Write (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Delete (SMSAP_profile dataset)
Creazione del backup (con DBverify)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Write (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Delete (SMSAP_profile dataset) SD.snapshot.Clone (SMSAP_profile dataset)
Creazione di backup (con RMAN)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Write (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Delete (SMSAP_profile dataset) SD.snapshot.Clone (SMSAP_profile dataset)

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Ripristino del backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp) SD.Snapshot.Restore (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Write (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Delete (SMSAP_profile dataset) SD.snapshot.Clone (SMSAP_profile dataset) SD.Snapshot.Restore (SMSAP_profile dataset)
Eliminazione del backup	SD.Snapshot.Delete (smsap_grp)	SD.Snapshot.Delete (SMSAP_profile dataset)
Verifica del backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Clone (SMSAP_profile dataset)
Montaggio di backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.Snapshot.Clone (SMSAP_profile dataset)
Dismount del backup	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile dataset)
Creazione di cloni	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.snapshot.Clone (SMSAP_profile dataset)
Eliminare i cloni	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile dataset)

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Suddivisione dei cloni	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smsap_grp) SD.snapshot.Clone (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.Storage.Write (smsap_grp)	SD.Storage.Read (SMSAP_profile dataset) SD.Snapshot.Read (SMSAP_profile dataset) SD.snapshot.Clone (SMSAP_profile dataset) SD.Snapshot.Delete (SMSAP_profile dataset) SD.Storage.Write (SMSAP_profile dataset)

Per ulteriori informazioni sulla definizione delle funzionalità RBAC, consultare la *Guida all'amministrazione di Gestione operazioni di Unified Manager di OnCommand*.

Fasi

1. Accedere alla console di Operations Manager.
2. Dal menu Setup, selezionare **Roles** (ruoli).
3. Selezionare un ruolo esistente o crearne uno nuovo.
4. Per assegnare le operazioni alle risorse di storage del database, fare clic su **Add Capabilities** (Aggiungi funzionalità).
5. Nella pagina Edit Role Settings (Modifica impostazioni ruolo), per salvare le modifiche apportate al ruolo, fare clic su **Update** (Aggiorna).

Informazioni correlate

["Guida all'amministrazione di OnCommand Unified Manager Operations Manager"](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.