



Configurare i pool di scanner

ONTAP 9

NetApp
April 24, 2024

Sommario

- Configurare i pool di scanner 1
 - Panoramica sulla configurazione dei pool di scanner 1
 - Creare un pool di scanner su un singolo cluster 1
 - Creazione di pool di scanner nelle configurazioni MetroCluster 2
 - Applicare un criterio scanner a un singolo cluster 5
 - Applicare i criteri dello scanner nelle configurazioni MetroCluster 6
 - Comandi per la gestione dei pool di scanner 8

Configurare i pool di scanner

Panoramica sulla configurazione dei pool di scanner

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Un criterio dello scanner determina se un pool di scanner è attivo.



Se si utilizza un criterio di esportazione su un server SMB, è necessario aggiungere ciascun server Vscan al criterio di esportazione.

Creare un pool di scanner su un singolo cluster

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. È possibile creare un pool di scanner per una singola SVM o per tutte le SVM in un cluster.

Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

Fasi

1. Creazione di un pool di scanner:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
- Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
- Specificare il dominio e il nome utente per ciascun utente con privilegi. Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando crea un pool di scanner denominato SP su vs1 SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users cifs\u1,cifs\u2
```

2. Verificare che il pool di scanner sia stato creato:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di SP pool di scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool  
SP  
  
Vserver: vs1  
Scanner Pool: SP  
Applied Policy: idle  
Current Status: off  
Cluster on Which Policy Is Applied: -  
Scanner Pool Config Owner: vserver  
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27  
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-  
27.fsct.nb  
List of Privileged Users: cifs\u1, cifs\u2
```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Creazione di pool di scanner nelle configurazioni MetroCluster

È necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, corrispondente alle SVM primarie e secondarie sul cluster.

Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

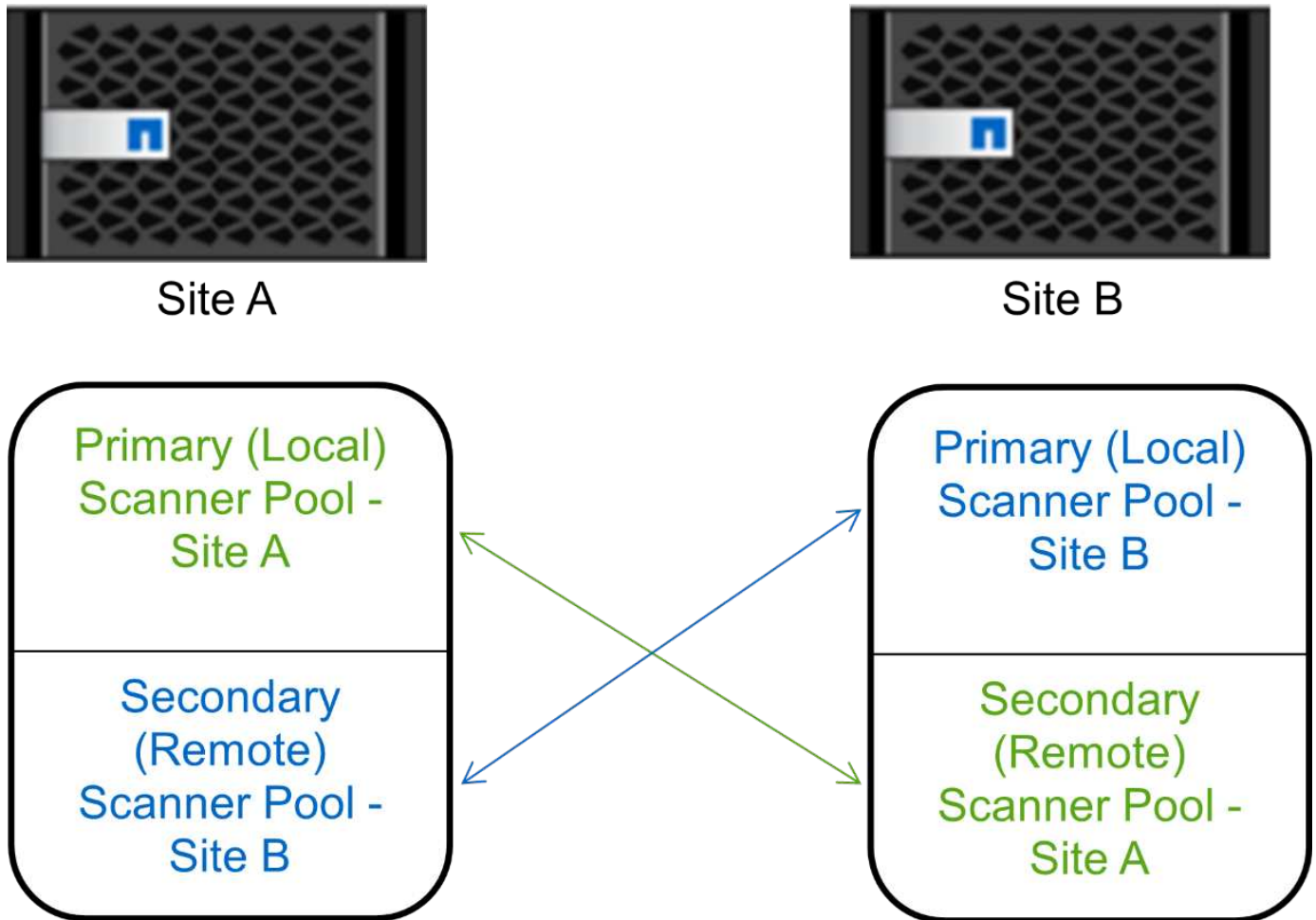
A proposito di questa attività

Le configurazioni MetroCluster proteggono i dati implementando due cluster mirrorati fisicamente separati. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. Una SVM primaria sul cluster locale serve i dati quando il cluster è online. Una SVM secondaria sul cluster locale serve i dati quando il

cluster remoto non è in linea.

Ciò significa che è necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, il pool secondario diventa attivo quando il cluster inizia a servire i dati dalla SVM secondaria. Per il disaster recovery (DR), la configurazione è simile a quella di MetroCluster.

Questa figura mostra una tipica configurazione MetroCluster/DR.



Fasi

1. Creazione di un pool di scanner:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
- Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
- Specificare il dominio e il nome utente per ciascun utente con privilegi.



È necessario creare tutti i pool di scanner dal cluster contenente la SVM primaria.

Per un elenco completo delle opzioni, vedere la pagina man del comando.

I seguenti comandi creano pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verificare che i pool di scanner siano stati creati:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli del pool di scanner pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Applicare un criterio scanner a un singolo cluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario attivare un pool di scanner prima che i server Vscan definiti possano connettersi a una SVM.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.

Fasi

1. Applicare un criterio scanner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool  
scanner_pool -scanner-policy primary|secondary|idle -cluster  
cluster_to_apply_policy_on
```

Un criterio dello scanner può avere uno dei seguenti valori:

- **Primary** specifica che il pool di scanner è attivo.
- **Secondary** Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di scanner primario è connesso.
- **Idle** specifica che il pool di scanner non è attivo.

Nell'esempio seguente viene indicato il nome del pool di scanner `SP` su `vs1` SVM è attivo:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1  
-scanner-pool SP -scanner-policy primary
```

2. Verificare che il pool di scanner sia attivo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di `SP` pool di scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa del comando, vedere la pagina man del comando.

Applicare i criteri dello scanner nelle configurazioni MetroCluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario applicare un criterio dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.
- Per le configurazioni di disaster recovery e MetroCluster, è necessario applicare un criterio dello scanner a ogni pool di scanner nel cluster locale e nel cluster remoto.
- Nel criterio creato per il cluster locale, è necessario specificare il cluster locale in `cluster` parametro. Nel criterio creato per il cluster remoto, è necessario specificare il cluster remoto in `cluster` parametro. Il cluster remoto può quindi rilevare le operazioni di scansione dei virus in caso di disastro.

Fasi

1. Applicare un criterio scanner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

Un criterio dello scanner può avere uno dei seguenti valori:

- **Primary** specifica che il pool di scanner è attivo.
- **Secondary** Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di

scanner primario è connesso.

- ° Idle specifica che il pool di scanner non è attivo.



È necessario applicare tutti i criteri dello scanner dal cluster contenente la SVM primaria.

I seguenti comandi applicano i criteri dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Verificare che il pool di scanner sia attivo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli del pool di scanner pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Comandi per la gestione dei pool di scanner

È possibile modificare ed eliminare i pool di scanner e gestire gli utenti con privilegi e i server Vscan per un pool di scanner. È inoltre possibile visualizzare informazioni riepilogative sul pool di scanner.

Se si desidera...	Immettere il seguente comando...
Modificare un pool di scanner	<code>vserver vscan scanner-pool modify</code>
Eliminare un pool di scanner	<code>vserver vscan scanner-pool delete</code>
Aggiungere utenti con privilegi a un pool di scanner	<code>vserver vscan scanner-pool privileged-users add</code>
Eliminare gli utenti con privilegi da un pool di scanner	<code>vserver vscan scanner-pool privileged-users remove</code>
Aggiungere server Vscan a un pool di scanner	<code>vserver vscan scanner-pool servers add</code>
Eliminare i server Vscan da un pool di scanner	<code>vserver vscan scanner-pool servers remove</code>
Visualizza riepilogo e dettagli di un pool di scanner	<code>vserver vscan scanner-pool show</code>
Visualizzare gli utenti con privilegi per un pool di scanner	<code>vserver vscan scanner-pool privileged-users show</code>
Visualizzare i server Vscan per tutti i pool di scanner	<code>vserver vscan scanner-pool servers show</code>

Per ulteriori informazioni su questi comandi, consulta le pagine man.

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.