



スキャナプールを設定

ONTAP 9

NetApp
April 24, 2024

目次

スキャナプールを設定	1
スキャナプールの概要の設定	1
単一クラスタにスキャナプールを作成する	1
MetroCluster 構成でスキャナプールを作成	2
単一のクラスタにスキャナポリシーを適用する	5
MetroCluster 構成でスキャナポリシーを適用	6
スキャナプールの管理用コマンド	8

スキャナプールを設定

スキャナプールの概要の設定

スキャナプールは、SVM に接続できる Vscan サーバと特権ユーザを定義します。スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。



SMBサーバでエクスポートポリシーを使用する場合は、各Vscanサーバをエクスポートポリシーに追加する必要があります。

単一クラスタにスキャナプールを作成する

スキャナプールは、SVM に接続できる Vscan サーバと特権ユーザを定義します。個々のSVM用またはクラスタ内のすべてのSVM用のスキャナプールを作成できます。

必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個々のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、Vscan サーバが SVM への接続に使用するドメインユーザアカウントが含まれている必要があります。
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

手順

1. スキャナプールを作成します。

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

- 個々の SVM 用のプールの場合はデータ SVM、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。
- 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
- 各特権ユーザのドメイン名とユーザ名を指定します。すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前のスキャナプールを作成します SP をクリックします 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. スキャナプールが作成されたことを確認します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します SP スキャナプール：

```
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
```

を使用することもできます vserver vscan scanner-pool show コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

MetroCluster 構成でスキャナプールを作成

MetroCluster 構成の各クラスタには、クラスタのプライマリとセカンダリの SVM に対応するプライマリとセカンダリのスキャナプールを作成する必要があります。

必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個々のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、Vscan サーバが SVM への接続に使用するドメインユーザアカウントが含まれ

ている必要があります。

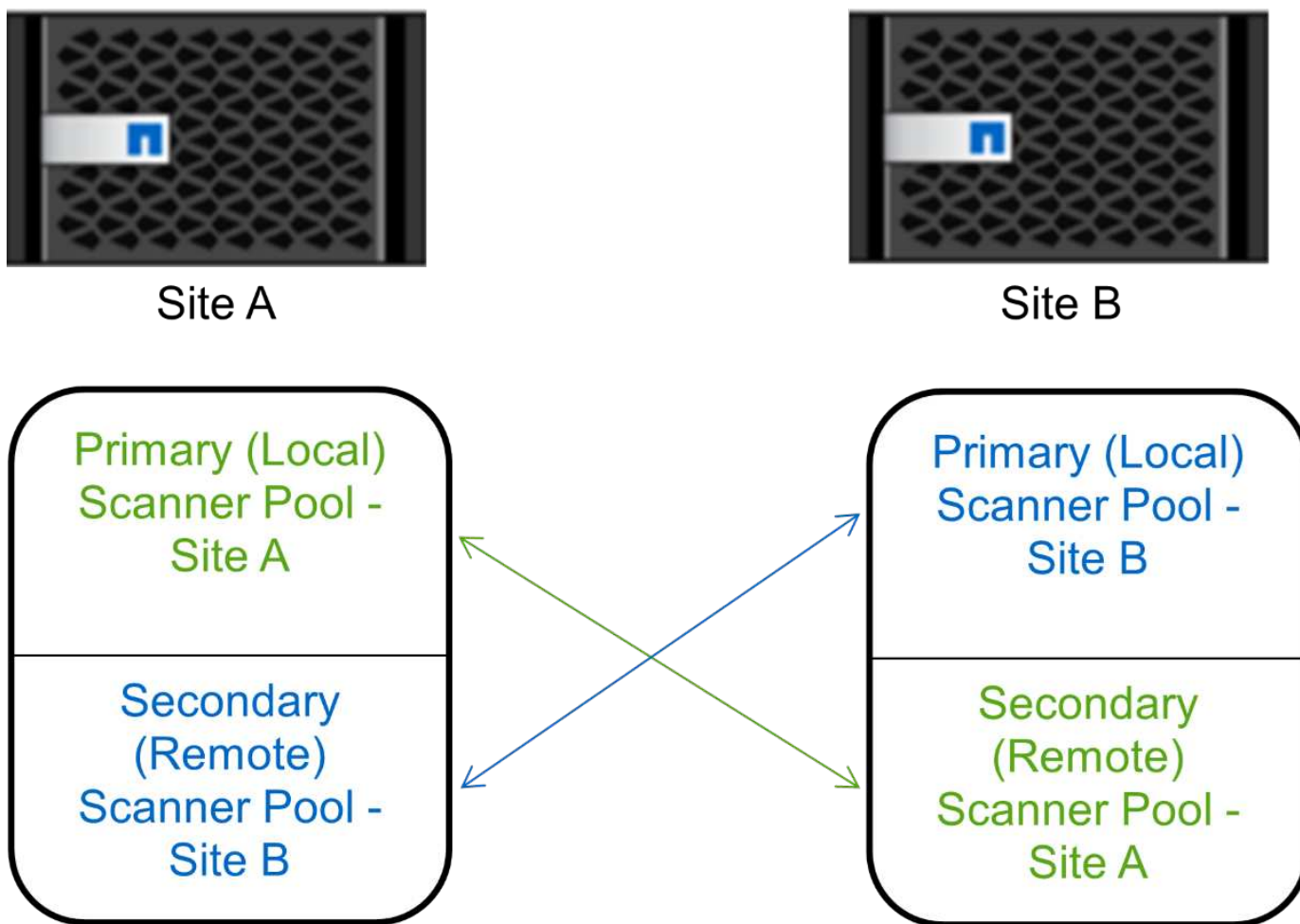
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

このタスクについて

MetroCluster 構成は、物理的に分離された 2 つのミラークラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータおよび SVM 設定を同期的にレプリケートします。クラスタがオンラインのときは、ローカルクラスタのプライマリ SVM がデータを提供します。リモートクラスタがオフラインのときは、ローカルクラスタのセカンダリ SVM がデータを提供します。

つまり、MetroCluster構成の各クラスタにプライマリとセカンダリのスキャナプールを作成する必要があり、クラスタがセカンダリSVMからデータの提供を開始すると、セカンダリプールがアクティブになります。ディザスタリカバリ（DR）の設定はMetroClusterと同様です。

この図は、一般的なMetroCluster / DR構成を示しています。



手順

1. スキャナプールを作成します。

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

- 個々の SVM 用のプールの場合はデータ SVM、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。

- 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
- 各特権ユーザのドメイン名とユーザ名を指定します。



スキャナプールの作成は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、MetroCluster 構成の各クラスタにプライマリとセカンダリのスキャナプールを作成します。

```
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. スキャナプールが作成されたことを確認します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、スキャナプールの詳細を表示します 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
```

を使用することもできます `vserver vscan scanner-pool show` コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

単一のクラスタにスキャナポリシーを適用する

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。スキャナプールが定義するVscanサーバがSVMに接続できるようにするには、スキャナプールをアクティブ化する必要があります。

このタスクについて

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。

手順

1. スキャナポリシーを適用します。

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

スキャナポリシーには次のいずれかの値が設定されます。

- Primary スキャナプールをアクティブにします。
- Secondary プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
- Idle スキャナプールを非アクティブにします。

次の例は、というスキャナプールを示しています SP をクリックします vs1 SVMがアクティブ：

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

2. スキャナプールがアクティブであることを確認します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、の詳細を表示します SP スキャナプール：

```
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
```

を使用できます vserver vscan scanner-pool show-active コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

MetroCluster 構成でスキャナポリシーを適用

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。MetroCluster 構成では、各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用する必要があります。

このタスクについて

- 1つのスキャナプールに適用できるスキャナポリシーは1つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。
- ディザスタリカバリおよびMetroCluster構成では、ローカルクラスタとリモートクラスタ内のすべてのスキャナプールにスキャナポリシーを適用する必要があります。
- ローカルクラスタ用に作成するポリシーでは、でローカルクラスタを指定する必要があります cluster

パラメータリモートクラスタ用に作成するポリシーでは、`cluster` パラメータこれにより、災害発生時にリモートクラスタがウィルススキャン処理をテイクオーバーできるようになります。

手順

1. スキャナポリシーを適用します。

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

スキャナポリシーには次のいずれかの値が設定されます。

- Primary スキャナプールをアクティブにします。
- Secondary プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。
- Idle スキャナプールを非アクティブにします。



スキャナポリシーの適用は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

次のコマンドは、MetroCluster 構成の各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用します。

```
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. スキャナプールがアクティブであることを確認します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、スキャナプールの詳細を表示します `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
```

を使用できます `vserver vscan scanner-pool show-active` コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

スキャナプールの管理用コマンド

スキャナプールを変更および削除し、スキャナプールの特権ユーザと Vscan サーバを管理できます。また、スキャナプールに関する概要情報を確認することもできます。

状況	入力するコマンド
スキャナプールを変更	<code>vserver vscan scanner-pool modify</code>
スキャナプールを削除します	<code>vserver vscan scanner-pool delete</code>
スキャナプールに特権ユーザを追加する	<code>vserver vscan scanner-pool privileged-users add</code>
スキャナプールから特権ユーザを削除します	<code>vserver vscan scanner-pool privileged-users remove</code>
スキャナプールに Vscan サーバを追加する	<code>vserver vscan scanner-pool servers add</code>
スキャナプールから Vscan サーバを削除します	<code>vserver vscan scanner-pool servers remove</code>
スキャナプールの概要と詳細を表示します	<code>vserver vscan scanner-pool show</code>
スキャナプールの特権ユーザを表示します	<code>vserver vscan scanner-pool privileged-users show</code>

すべてのスキャナプールの Vscan サーバを表示します

```
vserver vscan scanner-pool servers show
```

これらのコマンドの詳細については、マニュアルページを参照してください。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。