

IBM System Storage N シリーズ



Data ONTAP 7.3

ファイル・アクセスおよびプロトコルの管理ガイド

IBM System Storage N シリーズ



Data ONTAP 7.3

ファイル・アクセスおよびプロトコルの管理ガイド

お願い

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： GC27-2207-03

IBM System Storage N series

Data ONTAP 7.3

File Access and Protocols Management Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2009.8

© Copyright International Business Machines Corporation 2008, 2009.

著作権情報

Copyright © 1994–2008 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions copyright © 2008 IBM Corporation. All rights reserved. Printed in the U.S.A.

U.S. Government Users Restricted Rights—Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, copyright © Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display this text:

This product includes software developed by the University of California, Berkeley and its contributors.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software contains materials from third parties licensed to NetApp Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>).
Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995–1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitraka Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

Portions Copyright © 1995 University of Southern California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California, Information Sciences Institute. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

Portions of this product are derived from version 2.4.11 of the libxml2 library, copyright © 1994–2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

NetApp modified the libxml2 software on December 6, 2001, to enable it to compile cleanly on Windows, Solaris, and Linux. The changes have been sent to the maintainers of libxml2. The unmodified libxml2 software can be downloaded from <http://www.xmlsoft.org/>.

Software derived from copyrighted material of the World Wide Web Consortium is subject to the following license and disclaimer:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.

Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: “Copyright © [\$date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>”

Notice of any changes or modifications to the W3C files, including the date changes were made.

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED “AS IS,” AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Portions copyright © 2007-2008 LSI Corporation and QLogic Corporation. All rights reserved.

Portions copyright © 1995-1998 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION).

Software derived from copyrighted material of NetApp, Inc. is subject to the following license and disclaimer:

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

商標情報

ここには、該当する商標帰属表示がすべてリストされています。

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

追加情報については、次の Web サイトにアクセスしてください。
<http://www.ibm.com/ibm/licensing/contact/>.

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのもと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

本書について

ここでは、本書に記載される事項、本書の対象読者、本書で使用する特殊用語、情報の伝達のために本書で使用するコマンド、キーボード、および書体の規則、その他の情報の検索と使用に関する詳細について説明します。

本書は、Data ONTAP ソフトウェアを実行するストレージ・システム上のファイル・アクセス・プロトコルを構成、操作、および管理する方法について説明します。本書は、サポートされるすべてのストレージ・システム・モデルに適用されます。

対象読者

ここでは、本書の対象読者、および読者の事前知識と経験に関する前提について説明します。

本書は、ストレージ・システムのクライアント上で稼働するオペレーティング・システム、例えば UNIX および Windows、に精通しているシステム管理者を対象にしています。また本書では、読者がストレージ・システムを構成する方法、およびファイルの共有または転送に Network File System (NFS)、Common Internet File System (CIFS)、Hypertext Transport Protocol (HTTP)、File Transport Protocol (FTP)、および Web-based Distributed Authoring and Versioning (WebDAV) を使用する方法に精通していることも前提にしています。本ガイドでは、基本的なシステムまたはネットワーク管理に関するトピック、例えば IP アドレッシング、ルーティング、ネットワーク・トポロジーなどは扱いません。ストレージ・システムの特徴に重点を置いて説明します。

サポートされる機能

IBM® System Storage™ N シリーズ・ストレージ・システムは、NetApp® Data ONTAP® ソフトウェアによって運用されます。この製品のソフトウェア資料に記載されている機能の一部は、IBM によって提供されておらず、サポートもされていません。詳細については、IBM 担当員または販売店にお問い合わせください。サポートされる機能に関する情報は、次の Web サイトでも確認することができます。

www.ibm.com/storage/support/nas/

現在入手可能な N シリーズの製品および機能のリストは、次の Web サイトで確認することができます。

www.ibm.com/storage/nas/

情報、ヘルプ、およびサービスの利用

ヘルプ、サービス、技術支援、または IBM 製品に関する詳しい情報が必要な場合は、IBM がさまざまな形で提供している支援をご利用いただけます。このセクションでは、IBM と IBM 製品に関する追加情報の入手先、IBM N シリーズ製品で問題が発生した場合の対処方法、およびサービスが必要になった場合の連絡先について記載しています。

依頼する前に

連絡する前に、以下の手順を実行して、必ずお客様自身で問題の解決を試みてください。

- すべてのケーブルをチェックし、適切に接続されていることを確認します。
- 電源スイッチをチェックして、システムの電源がオンになっていることを確認します。
- ご使用のシステムに付属の資料に記載のトラブルシューティング情報を参照し、システムに付属の診断ツールを使用します。

資料の使用

N シリーズ・ハードウェア製品に関する情報は、印刷資料およびシステムに付属の Documentation CD で参照することができます。次の IBM NAS サポート Web サイトで、同じ資料を PDF ファイルとして入手可能です。

www.ibm.com/storage/support/nas/

Data ONTAP ソフトウェアの資料は、次の IBM NAS サポート Web サイトで PDF ファイルとして入手可能です。

www.ibm.com/storage/support/nas/

Web サイト

IBM は WWW に、最新の技術情報を入手したり、デバイス・ドライバおよび更新をダウンロードできるページを設けています。

- NAS 製品情報については、次の Web サイトにアクセスしてください。

www.ibm.com/storage/nas/

- NAS サポート情報については、次の Web サイトにアクセスしてください。

www.ibm.com/storage/support/nas/

- AutoSupport 情報については、次の Web サイトにアクセスしてください。

www.ibm.com/storage/support/nas/

- 資料の最新版については、次の Web サイトにアクセスしてください。

www.ibm.com/storage/support/nas/

オンライン技術サポートへのアクセス

IBM N シリーズ製品のオンライン技術サポートについては、次の Web サイトにアクセスしてください。

www.ibm.com/storage/support/nas/

ハードウェアのサービスとサポート

ハードウェアのサービスは、IBM Integrated Technology Services を通じてご利用いただけます。サポートの電話番号については、次の Web サイトにアクセスしてください。

www.ibm.com/planetwide/

サポートされるサーバーおよびオペレーティング・システム

IBM N シリーズ製品は、さまざまなサーバー、およびさまざまなオペレーティング・システムに接続します。サポートされる接続の最新情報を確認するには、次の Web サイトから「Interoperability Matrices」へのリンクを選択してください。

www.ibm.com/storage/support/nas/

ファームウェア更新

あらゆるデバイスと同様に、最新レベルのファームウェアを実行することをお勧めします。最新レベルのファームウェアは、次の Web サイトにアクセスしてダウンロードすることができます。

www.ibm.com/storage/support/nas/

IBM に技術サポートを依頼する前に、ご使用のマシンに最新レベルのファームウェアがインストールされていることを確認してください。ファームウェアの更新に関する詳細情報については、ご使用の Data ONTAP のバージョンの「*Data ONTAP Upgrade Guide*」を参照してください。

用語

本書で説明する概念を理解するために、ここで定義する用語の知識が必要になることがあります。

一般的なストレージ・システム用語

- Data ONTAP を実行するストレージ・システムは、ファイラー、アプライアンス、ストレージ・アプライアンス、またはシステム と呼ばれる場合があります。Data ONTAP 用の FilerView グラフィカル・ユーザー・インターフェースの名前は、これらの一般的な使用法の 1 つを反映しています。
- コントローラー またはストレージ・コントローラー は、Data ONTAP オペレーティング・システムを実行し、ディスク・サブシステムを制御するストレージ・システムのコンポーネントを指します。コントローラーまたはストレージ・コントローラーは、ストレージ・アプライアンス、アプライアンス、ストレージ・エンジン、ヘッド、CPU モジュール、またはコントローラー・モジュール と呼ばれる場合もあります。

アクティブ/アクティブ構成の用語

- アクティブ/アクティブ構成 は、2 つのシステムの一方に障害が発生した場合にデータを相互に提供するように構成された、1 対のストレージ・システム です。Data ONTAP の資料およびその他の情報リソースでは、アクティブ/アクティブ構成はクラスター またはアクティブ/アクティブ・ペア として参照される場合があります。
- アクティブ/アクティブ構成では、システムはノード と呼ばれることがよくあります。一方のノードはローカル・ノードと呼ばれる場合があり、他方のノードはパートナー・ノード またはリモート・ノード と呼ばれます。
- コントローラー・フェイルオーバー は、クラスター・フェイルオーバー、または *CFO* とも呼ばれ、2 つのストレージ・システムが相互のデータをテークオーバーできるようにして、データ可用性を向上するテクノロジーを指します。
- ファブリック接続 *MetroCluster* は、*syncmirror_local* ライセンスと *cluster_remote* ライセンスを実行するアクティブ/アクティブ構成を指します。この構成では、ノードは 2 対のファイバー・チャネル・スイッチに接続され、ノード間の距離は 500 メートルを超えます。
- *FC* ダイレクト接続トポロジーは、ホストが直接ストレージ・システムに接続されているトポロジーです。ダイレクト接続されたシステムは、ファブリックあるいは *FC* スイッチを使用しません。
- *FC* デュアル・ファブリック・トポロジーは、各ホストがストレージ・システムに接続された 2 つの物理的に独立したファブリックに接続されるトポロジーです。それぞれの独立したファブリックは、複数の *FC* スイッチから構成することが可能です。2 つの論理的に独立したファブリックにゾーニングされたファブリックは、デュアル・ファブリック接続ではありません。
- *FC* シングル・ファブリック・トポロジーは、ホストがシングル *FC* ファブリックでストレージ・システム に接続されているトポロジーです。ファブリックは複数の *FC* スイッチから構成することが可能です。
- *iSCSI* ダイレクト接続トポロジーは、ホストが直接ストレージ・コントローラーに接続されているトポロジーです。ダイレクト接続されたシステムは、ネットワークあるいはイーサネット・スイッチを使用しません。
- *iSCSI* ネットワーク接続トポロジーは、ホストがイーサネット・スイッチからストレージ・コントローラーに接続されているトポロジーです。ネットワークは、どの構成にも複数のイーサネット・スイッチを含むことができます。
- ミラーリングされたアクティブ/アクティブ構成 は、標準アクティブ/アクティブ構成と同様ですが、データのコピー (プレックス) が 2 つ存在する点が異なります。これはデータ・ミラーリング とも呼ばれます。
- リモート・ストレージ は、リモート・ノードの場所にありながら、ローカル・ノードからアクセス可能なストレージを指します。
- シングル・ストレージ・コントローラー構成は、1 つのストレージ・コントローラーのみが使用されているトポロジーです。シングル・ストレージ・コントローラー構成は、Single Point of Failure (単一障害点) を持ち、*FC SAN* 構成で *cfmodes* をサポートしません。
- 標準アクティブ/アクティブ構成 は、パートナー・ノードに障害が発生したときに、片方のノードがパートナーを自動的にテークオーバーするようにセットアップされた構成を指します。

- ストレッチ *MetroCluster* は、syncmirror_local ライセンスと cluster_remote ライセンスを実行するアクティブ/アクティブ構成を指します。この構成では、ノード間の距離は最大 500 メートルであり、ノード間でスイッチは使用されません。この構成は、スイッチなしの *MetroCluster* とも呼ばれます。

ストレージ・ハードウェアの用語

- *AT-FCX* は、一部のディスク・シェルフで使用する、拡張された FC-AL からシリアル ATA (SATA) へのブリッジを指します。
- ディスク・シェルフ は、ストレージ・システムのディスク・サブシステム・コンポーネントのユニットを指します。
- *ESH (Embedded Switching Hub)* ディスク・シェルフ・モジュールは、単一のドライブに障害が起こってもループが停止しないように、FC-AL ループをインテリジェントに管理する手段を備えたコンポーネントを指します。また、ディスク・シェルフの環境データを伝達する、格納装置サービス・プロセッサも内蔵しています。
- *ESH2* ディスク・シェルフ・モジュールは、第 2 世代の ESH モジュールを指します。
- *ESH4* ディスク・シェルフ・モジュールは、第 3 世代の ESH モジュールを指します。
- ディスク用 *FC HBA* または *FC HBA* は、ノードをスイッチあるいはディスクに接続するファイバー・チャネル・ホスト・バス・アダプターを指します。
- ホスト・バス・アダプター (HBA) は、ホスト I/O バスを SCSI 環境でコンピューターのメモリー・システムに接続する FC あるいは iSCSI の入出力アダプターです。
- ターゲット・アダプターは、ストレージ・システム上にあり、ホストからのデータを受信する入出力アダプターです。既にストレージ・システム・コントローラーに取り付けられているターゲット・アダプターは、内蔵アダプターです。システムの使用可能なスロットの 1 つに別々に取り付けられているターゲット・アダプターはターゲット拡張アダプターです。内蔵アダプターは、ディスク・シェルフに接続するイニシエーター・モードで機能するように構成することも可能です。ほとんどの ストレージ・システム は、イニシエーター・モードで機能する拡張アダプターの使用もサポートします。

一般用語

- 入力 (*enter*) という用語は、キーボードのキーを 1 つ以上押してから Enter キーを押すこと、またはグラフィカル・インターフェースのフィールドをクリックしてその中に情報を入力することを意味します。
- 入力 (*type*) という用語は、キーボードのキーを 1 つ以上押すことを意味します。

コマンド行インターフェースの代替としての FilerView

FilerView グラフィカル・ユーザー・インターフェースを使用すれば、多くの一般的なタスクを実行でき、また Web ブラウザーからストレージ・システム を表示および管理できます。

Data ONTAP 管理者としてのタスクは、ストレージ・システムのコンソール、構成ファイル内、または Telnet セッションまたはリモート・シェル接続を経由して、コマンドを入力することによって実行できます。

多くの一般的なタスクを実行する他の方式は、FilerView を使用することです。FilerView はすべてのストレージ・システムに付属しており、使いやすく、Data ONTAP の機能と FilerView でその機能を使用する方法を説明するヘルプが組み込まれています。

FilerView を使用したストレージ・システムへのアクセス、および FilerView ヘルプに関する詳細情報については、「*System Administration Guide*」を参照してください。

コマンド、キーボード、および書体の規則

本書では、お客様のコマンド入力を容易にするコマンド、キーボード、および書体の規則を用いています。

コマンド規則

UNIX ワークステーション上で実行されるコマンドを示す例では、ご使用の UNIX のバージョンによってコマンド構文や出力が異なる場合があります。

キーボード規則

- キーの組み合わせを説明するときに、本書では個々のキーを区切るためにハイフン (-) を使用します。例えば、「Ctrl-D」は「Ctrl」キーと「D」キーを同時に押すことを意味します。
- 本書では、復帰に相当するデジタルを生成するキーを示すために「Enter」という用語を使用しますが、一部のキーボードではこのキーは「Return」という名前になっています。

字体の規則

次の表では、本書で使用されている字体の規則を説明します。

規則	情報のタイプ
イタリック・フォント	特別な注意を必要とする語句または文字。 ユーザーが指定する必要がある情報のプレースホルダー。例えば、ガイドで <code>arp -d hostname</code> コマンドを入力するように述べている場合は、「arp -d」という文字と、その後ホストの実際の名前を付けて入力します。 相互参照の資料タイトル。

規則	情報のタイプ
モノスペース・フォント	コマンド名、オプション名、キーワード、およびデーモン名。 システム・コンソールまたはその他のコンピューター・モニターに表示される情報。 ファイルの内容。
太字モノスペース・フォント	ユーザーが入力する語句または文字。大文字で入力する必要がない場合は、ユーザーが入力する内容は常に小文字で表示されます。

特別メッセージ

本書には、確認を必要とする状況に対して警告するために、次のタイプのメッセージが記載されている場合があります。「危険」および「注意」の注記は、ハードウェア資料にのみ示されます (該当する場合)。

注: 注には、システムを効率的にインストールまたは操作するために役立つ重要な情報が記載されています。

重要: 「重要」の注記には、システム破損、データ損失、または装置の損傷を防ぐために従う必要がある指示が記載されています。

危険

「危険」の注記は、生命の危険や深刻な身体傷害を引き起こす可能性がある条件や手順について警告します。

注意:

「注意」の注記は、致命的ではなく深刻な危険のない身体傷害を引き起こす可能性がある条件や手順について警告します。

ファイル・アクセス管理の概要

Data ONTAP によって、異なるプロトコルのファイル・アクセスを管理することができます。

Data ONTAP がサポートするファイル・プロトコル

Data ONTAP は、NFS、CIFS、FTP、HTTP、および WebDAV を含むすべての一般的なファイル・プロトコルをサポートします。

Data ONTAP がファイルへのアクセスをコントロールする方法

Data ONTAP は、指定した認証ベースおよびファイル・ベースの制限によってファイルへのアクセスをコントロールします。

認証ベースの制限

認証ベースの制限によって、どのクライアント・マシンあるいはどのユーザーが、ストレージ・システム全体あるいは vFiler ユニットに接続できるかを指定することが可能です。

Data ONTAP は UNIX および Windows サーバー両方からの Kerberos 認証をサポートします。

ファイル・ベースの制限

ファイル・ベースの制限によって、どのユーザーがどのファイルにアクセス可能かを指定することができます。

ユーザーがファイルを作成すると、Data ONTAP はそのファイルに関するアクセス権のリストを生成します。アクセス権のリストの形式はそれぞれのプロトコルによって変化しますが、読み取り許可および書き込み許可のような共通のアクセス権を常に含んでいます。

ユーザーがファイルにアクセスを試みると、Data ONTAP は許可リストを使用してアクセスを認可するかを決定します。Data ONTAP は、ユーザーが実行している読み取りや書き込みのような操作、および以下の要因によってアクセスを認可あるいは拒否します。

- ユーザー・アカウント
- ユーザー・グループあるいはネットグループ
- クライアント・プロトコル
- クライアント IP アドレス
- ファイル・タイプ

検証プロセスの一部として、Data ONTAP は Lightweight Directory Access Protocol (LDAP)、ネットワーク情報サービス (NIS)、あるいはローカルのストレージ・システム情報の中から指定した参照サービスを使用して、ホスト名を IP アドレスにマッピングします。

NFS を使用したファイル・アクセス

ストレージ・システム上のファイル・システム・パスをエクスポートおよびアンエクスポートすることで、PC-NFS および WebNFS を含めた NFS クライアントによるマウントをそれぞれ有効または無効にすることができます。

ファイル・システム・パスのエクスポートあるいはアンエクスポート

`/etc/exports` ファイルの編集または `exportfs` コマンドの実行によって、ファイル・システム・パスをエクスポートあるいはアンエクスポートして NFS クライアントに有効あるいは無効にすることができます。

始める前に

セキュア NFS アクセスを (`sec=krb*` エクスポート・オプションの使用によって) サポートするために、最初に Kerberos v5 セキュリティー・サービスを有効にする必要があります。

このタスクについて

一度にいくつかのエクスポート・エントリーを永続的に変更する必要がある場合は、通常は直接 `/etc/exports` ファイルを編集するのが最も容易です。しかし、単一のエクスポート・エントリーを変更する必要がある場合や、あるいは一時的な変更を行う必要がある場合は、通常は `exportfs` コマンドを実行するのが最も容易です。

`/etc/exports` ファイルの編集

NFS の始動時に、どのファイル・システム・パスを Data ONTAP が自動的にエクスポートするかを指定するために、`/etc/exports` ファイルを編集します。詳細情報については、`na_exports(5)` のマニュアル・ページを参照してください。

始める前に

`nfs.export.auto-update` オプションが `on` (デフォルト) の場合、Data ONTAP はボリュームを作成、名前変更、あるいは削除するときに `/etc/exports` ファイルを自動的に更新します。詳細情報については、`na_options(1)` のマニュアル・ページを参照してください。

注: `/etc/exports` ファイルの最大エクスポート・エントリー数は 10,240 です。各エクスポート・エントリーの最大文字数は、行末文字を含めて 4,096 です。

このタスクについて

エクスポート・エントリーは、次の構文で成り立っています。

```
path -option[,option...]
```

エクスポート・エントリー構文で、*path* はファイル・システム・パス (例えば、ボリューム、ディレクトリー、あるいはファイルへのパス) で、*option* は以下の情報を指定するエクスポート・オプションです。

- どの NFS クライアントがどのアクセス権 (読み取り専用、読み取り/書き込み、あるいは root) を持っているか
 - ファイル・システム・パスにアクセスするすべての匿名ユーザーあるいは NFS クライアントの root ユーザーの、ユーザー ID (またはユーザー名)
 - NFS クライアント・ユーザーが、setuid および setgid 実行ファイルを作成できるか、およびファイル・システム・パスへのアクセス時に `mknod` コマンドを使用できるか
 - NFS クライアントがファイル・システム・パスにアクセスするためにサポートする必要があるセキュリティー・タイプ
 - エクスポートされたファイル・システム・パスに対応する、実際のファイル・システム・パス
1. ストレージ・システムへの root アクセス権を持つ NFS クライアント上で、`/etc/exports` ファイルをテキスト・エディターで開きます。
 2. 変更を行います。
 3. このファイルを保存します。

次のタスク

テキスト・エディターを使用して `/etc/exports` ファイルを編集する場合、`/etc/exports` ファイル内のすべてのファイル・システム・パスをエクスポートするか、あるいは現在エクスポートされているファイル・システム・パスと `/etc/exports` ファイルで指定したファイル・システム・パスを同期させるまでは、変更は有効にはなりません。

注:

`exportfs` コマンドを `-b`、`-p`、あるいは `-z` オプションを付けて実行することでも、`/etc/exports` ファイルを変更できます。

exportfs コマンドの使用

コマンド行からファイル・システム・パスをエクスポートあるいはアンエクスポートするには、`exportfs` コマンドを実行します。詳細情報については、`na_exportfs(1)` のマニュアル・ページを参照してください。

ファイル・システム・パスのエクスポート

対応するエントリーの `/etc/exports` ファイルへの追加の有無に関わらず、ファイル・システム・パスをエクスポートすることができます。さらに、`/etc/exports` ファイル内で指定されたすべてのファイル・システム・パスをエクスポートすることができます。

ファイル・システム・パスのエクスポート、および対応するエントリーの `/etc/exports` ファイルへの追加:

ファイル・システムをエクスポート、および対応するエントリーを `/etc/exports` ファイルに追加するには、`exportfs -p` コマンドを使用します。

コマンド `exportfs -p [options] path` を入力します。 *options* は、エクスポート・オプションのコンマ区切りのリストで (詳細情報については、`na_exports(5)` のマニュアル・ページを参照)、 *path* は、ファイル・システム・パスです (例えば、ボリューム、ディレクトリー、あるいはファイルへのパス)。

注: いずれのエクスポート・オプションも指定しない場合は、Data ONTAP は `rw` および `sec=sys` エクスポート・オプションを付けて、自動的にファイル・システム・パスをエクスポートします。

対応するエントリーの /etc/exports ファイルへの追加なしでのファイル・システム・パスのエクスポート:

対応するエクスポート・エントリーを `/etc/exports` ファイルに追加せずに、ファイル・システム・パスをエクスポートするには、`exportfs -io` コマンドを使用します。

コマンド `exportfs -io [options] path` を入力します。 *options* は、エクスポート・オプションのコンマ区切りのリストで (詳細情報については、`na_exports(5)` のマニュアル・ページを参照)、 *path* は、ファイル・システム・パスです (例えば、ボリューム、ディレクトリー、あるいはファイルへのパス)。

注: いずれのエクスポート・オプションも指定しない場合は、Data ONTAP は `/etc/exports` ファイル内のファイル・システム・パスのために指定されたエクスポート・オプションを (ある場合は) 使用します。

/etc/exports ファイルで指定されたすべてのファイル・システム・パスのエクスポート:

`/etc/exports` ファイルで指定されたすべてのファイル・システム・パスをエクスポートするには、`exportfs -a` コマンドを入力します。

ファイル・システム・パスのアンエクスポート

1 つのファイル・システム・パスをアンエクスポートし、状況に応じてそれに対応するエントリーを `/etc/exports` ファイルから削除することができます。さらに、対応するエントリーを `/etc/exports` ファイルから削除せずに、すべてのファイル・システム・パスをアンエクスポートすることができます。

1 つのファイル・システム・パスのアンエクスポート:

対応するエントリーを `/etc/exports` ファイルから削除せずに、1 つのファイル・システム・パスをアンエクスポートするには、`exportfs -u` コマンドを使用します。1 つのファイル・システム・パスをアンエクスポートし、それに対応するエントリーを `/etc/exports` ファイルから削除するには、`exportfs -z` コマンドを使用します。

1 つのファイル・システム・パスをアンエクスポートします。

以下の条件でファイル・システム・パスをアンエクスポートしたい場合、	以下を実行してください。
<code>/etc/exports</code> ファイルから対応するエントリーを削除しない	次のコマンドを入力します。 <code>exportfs -u path</code> ここで、 <i>path</i> はファイル・システム・パスです。

以下の条件でファイル・システム・パスをアンエクスポートしたい場合、	以下を実行してください。
/etc/exports ファイルから対応するエントリを削除する	次のコマンドを入力します。exportfs -z <i>path</i> ここで、 <i>path</i> はファイル・システム・パスです。

すべてのファイル・システム・パスのアンエクスポート:

/etc/exports ファイルから対応するエントリを削除することなくすべてのファイル・システム・パスをアンエクスポートするには、exportfs -ua コマンドを使用します。

次のコマンドを入力します。exportfs -ua

現在エクスポートされているファイル・システム・パスと /etc/exports ファイルで指定されているファイル・システム・パスの 同期

/etc/exports ファイルで指定されているすべてのファイル・システム・パスをエクスポートし、/etc/exports ファイルで指定されていないすべてのファイル・システム・パスをアンエクスポートするには、exportfs -r コマンドを入力します。

1 つ以上のファイル・システム・パスからの 1 つ以上の NFS クライアントの隔離の有効化および無効化

複数のファイル・システム・パスへの読み取り専用あるいは読み取り/書き込みアクセス権を、複数の NFS クライアントに一時的あるいは永続的に与えるために、隔離を使用することができます。

このタスクについて

隔離を有効あるいは無効にするときに、Data ONTAP は指定した NFS クライアントを新規のアクセス権のリスト (rw= または ro=) の最前部に移動させます。この再配列によって、オリジナルのエクスポート規則を変更することができます。

次のコマンドを入力します。exportfs -b enable | disable save | nosave allhosts | *clientid[:clientid...]* allpaths | *path[:path...]*

以下を実施したい場合、	以下を実行してください。
隔離を有効にする	enable オプションを指定します。
隔離を無効にする	disable オプションを指定します。
/etc/exports ファイルを更新する	save オプションを指定します。
/etc/exports ファイルの更新を防止する	nosave オプションを指定します。
すべての NFS クライアントに適用する	allhosts オプションを指定します。
すべてのエクスポートされたファイル・システム・パスに適用する	allpaths オプションを指定します。

以下を実施したい場合、	以下を実行してください。
NFS クライアントの特定のセットに適用する	コロン区切りの NFS クライアント ID のリストを指定します。
ファイル・システム・パスの特定のセットに適用する	コロン区切りのファイル・システム・パスのリストを指定します。

タスクの結果

Data ONTAP は、隔離を有効あるいは無効にする前にキュー内のすべての NFS 要求を処理し、その結果、すべてのファイル書き込みは確実に完了します。

エクスポートされたファイル・システム・パスの実際のファイル・システム・パスの表示

エクスポートされたファイル・システム・パスの実際のファイル・システム・パスを表示するには、`exportfs -s` コマンドを使用します。

このタスクについて

ファイル・システムの実際のパスは、`-actual` オプションを使用しなければ、そのエクスポートされたパスと同じです。詳細情報については、`na_exports(5)` のマニュアル・ページを参照してください。

注: NFSv4 は、`-actual` オプションをサポートしません。

コマンド `exportfs -s path` を入力します。`path` は、エクスポートされたファイル・システム・パスです。

ファイル・システム・パスのエクスポート・オプションの表示

エクスポート問題のデバッグの助けとなるファイル・システム・パスのエクスポート・オプションを表示するには、`exportfs -q` コマンドを使用します。

コマンド `exportfs -q path` を入力します。`path` は、ファイル・システム・パスです。

Data ONTAP は、指定したパスのエクスポート・オプションを表示します。

注: また Data ONTAP は、各オプションの規則 ID を表示しますが、診断コマンドを使用しない限り、規則 ID は必要ありません。詳細情報については、技術サポートにお問い合わせください。

アクセス・キャッシュの管理

Data ONTAP は、ファイル・システム・パスへの NFS クライアントのアクセスを認可あるいは拒否するときに、DNS の逆引きまたはネットグループの解析を実行しなければならない可能性を削減するために、アクセス・キャッシュを使用します。

NFS クライアントがファイル・システム・パスへのアクセスを試みるときには必ず、Data ONTAP はアクセスを認可するか拒否するかを判別する必要があります。

ほとんどの単純なケースを除いて (例えば、ファイル・システム・パスが `ro` あるいは `rw` オプションと一緒にエクスポートされた場合)、Data ONTAP は以下の条件に一致するアクセス・キャッシュの値によってアクセスを認可あるいは拒否します。

- ファイル・システム・パス
- NFS クライアントの IP アドレス、アクセス・タイプ、およびセキュリティー・タイプ

アクセス・キャッシュ・エントリーにこのような値が存在しない場合 (例えば、Data ONTAP が以前にアクセスの判別をしなかった場合や、この特定の NFS クライアント・ファイル・システム・パスの組み合わせに `exportfs -c` コマンドを使用してアクセス・キャッシュ・エントリーを作成しなかった場合)、Data ONTAP は以下の条件を比較した結果に応じてアクセスを認可あるいは拒否します。

- NFS クライアントの IP アドレス (あるいは、必要な場合はホスト名)、アクセス・タイプ、およびセキュリティー・タイプ
- ファイル・システム・パスのエクスポート・オプション

次に、Data ONTAP はこの比較の結果をアクセス・キャッシュに保管します。

DNS の逆引きまたはネットグループの解析を実行しなければならない可能性を削減するために、Data ONTAP はこの比較を 3 つのステージに分けます。NFS クライアントがファイル・システム・パスへのアクセス権を持っているかどうかを判別する必要がある場合のみ、この比較の連続するステージを実行します。

最初のステージでは、Data ONTAP は NFS クライアントの IP アドレスを、単一の IP アドレス、サブネット、および以前に Data ONTAP が解決して IP アドレスに変換したホスト名を含む、全体が IP アドレスで構成されたすべてのエクスポート規則と比較します。

2 番目のステージでは、Data ONTAP は NFS クライアントの IP アドレスで DNS の逆引きを実行し、次に NFS クライアントのホスト名を、サブドメインおよび Data ONTAP が IP アドレスに変換できていないホスト名を含むすべてのエクスポート規則と比較します。

3 番目のステージでは、Data ONTAP はネットグループを解析します。

Data ONTAP は、アクセス・キャッシュ内の情報がリブート後、およびテークオーバーあるいはギブバック後に使用可能なように、エントリー・キャッシュを 15 分ごとにディスクにバックアップします。

アクセス・キャッシュへのエントリーの追加

NFS クライアントがファイル・システム・パスへの特定のタイプのアクセス権を持っているかをチェックする (それと同時に対応するエントリーをアクセス・キャッシュに追加する) には、`exportfs -c` コマンドを使用します。

次のコマンドを入力します。 `exportfs -c clientaddr path [accesstype] [securitytype]`

パラメーター	説明
<code>clientaddr</code>	NFS クライアントの IP アドレス

パラメーター	説明
<i>path</i>	ファイル・システム・パス
<i>accesstype</i>	以下のオプションの 1 つ ro — 読み取り専用アクセス権 rw — 読み取り/書き込みアクセス権 root — root アクセス権
<i>securitytype</i>	以下のオプションの 1 つ sys — UNIX スタイルのセキュリティ none — セキュリティなし krb5 — Kerberos バージョン 5 認証 krb5i — Kerberos バージョン 5 保水性サービス krb5p — Kerberos バージョン 5 プライバシー・サービス

アクセス・タイプを指定しない場合、Data ONTAP は単純に NFS クライアントがファイル・システム・パスをマウントできるかどうかをチェックします。セキュリティ・タイプを指定しない場合、Data ONTAP は NFS クライアントのセキュリティ・タイプを sys と仮定します。

アクセス・キャッシュからのエントリーの削除

アクセス・キャッシュからエントリーを削除するには、`exportfs -f` コマンドを使用します。

アクセス・キャッシュからエントリーを削除するには、コマンド `exportfs -f path` を入力します。*path* は、アクセス・キャッシュからエントリーを削除するファイル・システム・パスを指定します。ファイル・システム・パスを指定しない場合、Data ONTAP はアクセス・キャッシュからすべてのエントリーを削除します。

タスクの結果

注: Data ONTAP は、ファイル・システム・パスをアンエクスポートした場合や、エントリーがタイムアウトした場合に、アクセス・キャッシュから自動的にエントリーを削除します。

アクセス・キャッシュ統計の表示

アクセス・キャッシュ統計を表示するには、`nfsstat -d` コマンドを入力します。

次のコマンドを入力します。`nfsstat -d`

タスクの結果

Data ONTAP は、以下のアクセス・キャッシュ統計を表示します。

```
access cache (hits, partial misses, misses)
access cache lookup requests (curr, total, max)
access cache nodes (found, created)
access cache requests (queued, unqueued)
access cache requests unqueued by (flush, restore)
access cache read requests (queued, unqueued)
access cache write requests (queued, unqueued)
access cache root requests (queued, unqueued)
access cache expired hits (total, read, write, root)
access cache inserts (full, partial, dup, subnet, restore)
access cache refreshes requested (total, read, write, root)
access cache refreshes done (total, read, write, root)
access cache errors (query, insert, nomem)
access cache nodes (flushed, harvested, harvestsfailed)
access cache nodes (allocated, free)
access cache qctx (allocated, free)
access cache persistence errors (total)
access cache persistence nodes handled (restored, saved)
access cache persistence rules deleted (total)
access cache persistence memchunks (allocated, freed)
```

これらのアクセス・キャッシュ統計に関する詳細情報については、`na_nfsstat(1)` のマニュアル・ページを参照してください。

アクセス・キャッシュ・パフォーマンスの最適化

アクセス・キャッシュ・パフォーマンスを最適化するために、可能な限り同一のエクスポート規則を再利用する必要があります。

このタスクについて

Data ONTAP は、同じ規則を指定するすべてのエクスポート・エントリーのために、単一のアクセス・キャッシュ・エントリーを保持します。

グループ規則の再利用

`ro,rw=@group1` 規則が以下のエクスポート・エントリーの両方に存在している場合でも、Data ONTAP は規則のための単一のアクセス・キャッシュ・エントリーを保持します。

```
/vol/a -sec=sys,ro,sec=sys,rw=@group1,sec=krb5,rw=@group2
```

```
/vol/b -sec=sys,ro,sec=sys,rw=@group1
```

アクセス・キャッシュ・タイムアウト値の設定

Data ONTAP がアクセス・キャッシュにエントリーを保持する期間を指定するには、`nfs.export.harvest.timeout` オプションを設定します。Data ONTAP がアクセス・キャッシュ・エントリーをリフレッシュする前に使用する期間を指定するには、`nfs.export.neg.timeout` および `nfs.export.pos.timeout` オプションを設定します。詳細情報については、`na_options(1)` のマニュアル・ページを参照してください。

NFS 用 Kerberos v5 セキュリティー・サービスの有効化

NFS 用 Kerberos v5 セキュリティー・サービスを有効にするには、`nfs setup` コマンドを使用します。

このタスクについて

Data ONTAP は、データのセキュリティおよびコントロールされたドメイン内のユーザー識別を確実にするために Kerberos v5 認証プロトコルを使用する、セキュア NFS アクセスを提供します。

NFS 用 Kerberos v5 を実装した Data ONTAP 環境は、Active Directory ベースおよび UNIX ベースの 2 つのタイプの Kerberos 鍵配布センター (KDC) をサポートします。

注: Data ONTAP 7.3.1 以降のリリースでは、Data ONTAP が NFS に UNIX ベースの KDC を、CIFS に Active Directory ベースの KDC を使用するように構成することができます。この構成は、Kerberos マルチ・レルム構成と呼ばれます。

KDC タイプ	説明
Active Directory ベース	NFS の Kerberos レルムは、Active Directory ベースの KDC です。CIFS は、Microsoft Active Directory 認証で構成する必要があります。その後、NFS は CIFS ドメイン・コントローラーを KDC として使用します。
UNIX ベース	NFS の Kerberos レルムは、MIT あるいは Heimdal KDC です。

注: Kerberos マルチ・レルム構成をサポートするために、Data ONTAP はプリンシパルとキータブ・ファイルの 2 つのセットを使用します。Active Directory ベースの KDC では、プリンシパルとキータブ・ファイルはそれぞれ Data ONTAP 7.3.1 より前のリリースと同じように `/etc/krb5auto.conf` および `/etc/krb5.keytab` にあります。しかし、UNIX ベースの KDC では、プリンシパルとキータブ・ファイルはそれぞれ `/etc/krb5.conf` および `/etc/UNIX_krb5.keytab` にあります。そのため、Data ONTAP 7.3.1 から、UNIX ベースの KDC のキータブ・ファイルは、`/etc/krb5.keytab` から `/etc/UNIX_krb5.keytab` に変更されました。

ただし、Data ONTAP が NFS のために UNIX ベースの KDC を使用するように構成された Data ONTAP 7.3.1 より前のリリースからアップグレードされた場合は、Data ONTAP は引き続き古いキータブ・ファイル (`/etc/krb5.keytab`) を使用します。そのようなリリースからアップグレードした後に CIFS を再構成する場合や、あるいは CIFS のために Active Directory ベースの KDC を構成した後に初めて NFS を構成する場合にのみ、新規の UNIX ベースの KDC のキータブ・ファイル (`/etc/UNIX_krb5.keytab`) を使用する必要があります。

Active Directory ベースの KDC を使用するための、NFS 用 Kerberos v5 セキュリティー・サービスの構成

Active Directory ベースの KDC を使用するには、`cifs setup` コマンドの前あるいは後に NFS 用 Kerberos v5 セキュリティー・サービスを構成します。

タスクの結果

セキュリティー・サービスのセットアップ手順によって、ご使用のストレージ・システムが Active Directory ベースの KDC に `nfs/hostname.domain@REALM` と呼ばれるサービス・プリンシパルとして追加されます。

CIFS 構成前に Active Directory ベースの KDC を使用するための、NFS 用 Kerberos v5 セキュリティー・サービスの構成

CIFS を構成するために `cifs setup` をまだ実行していない場合、構成情報を提供する必要があります。それをしない場合、構成情報はご使用の CIFS 構成から取得されます。

始める前に

Active Directory ベースのドメイン名サービスを使用するためにストレージ・システムを構成し、確実に Active Directory サーバーのみをリストするために `/etc/resolv.conf` ファイルを編集してください。

例えば、Active Directory サーバーが 172.16.1.180 および 172.16.1.181 の Kerberos レalmについて、以下の Active Directory サーバーのエントリーのみを含むように `/etc/resolv.conf` を変更します。

```
nameserver 172.16.1.180 nameserver 172.16.1.181
```

このレalmについて、他のすべての Active Directory サーバーのエントリーを削除することを確認してください。

このタスクについて

構成情報を入力するために既に `nfs setup` を使用している場合は、受信するプロンプトは以下の手順に示されたものと異なる可能性があります。

1. コマンド `nfs setup` を入力します。 `nfs setup` から、次のメッセージを受信します。

Enable Kerberos for NFS?

2. `y` を入力して続行します。

KDC のタイプを指定することを求められます。

The filer supports these types of Kerberos Key Distribution Centers (KDCs):
1 - UNIX KDC
2 - Microsoft Active Directory KDC
Enter the type of your KDC (1-2):

3. `2` を入力します。

ストレージ・システム名を指定するようにプロンプトが表示されます。

The default name of this filer will be 'SERVER'
Do you want to modify this name? [no]:

4. ストレージ・システム名のプロンプトを表示するには yes を入力し、デフォルトのストレージ・システム名「SERVER」を承認する場合は Enter を押してください。

ストレージ・システムの Active Directory サーバーのドメイン名を指定するプロンプトが表示されます。

Enter the Windows Domain for the filer []:

5. Active Directory サーバーのドメイン名を入力します。例えば、ドメイン名 ADKDC.LAB.DOCEXAMPLE.COM を入力します。入力したドメイン名は、Kerberos レalm名としても使用されます。ローカル管理者アカウントをセットアップするためのプロンプトが表示されます。
6. ローカル管理者アカウントの情報を入力します。

注: このステップは、Active Directory KDC の Kerberos 構成に影響はありません。

7. ローカル管理者アカウント情報を入力した後、以下の例のようなメッセージを受信することを確認してください。ADKDC.LAB.DOCEXAMPLE.COM is a Windows 2000(tm) domain.

このメッセージは、ストレージ・システムが Active Directory サーバーを検出できたこと、およびストレージ・システムが KDC サーバーとしてこのサーバーが機能できると判別したことを確認します。

このようなメッセージを受信しない場合、Active Directory サーバーに問題があるか、あるいはストレージ・システムの DNS サーバーが Active Directory サーバーではないことを示しています。ネットワーク構成を確認し、次に nfs setup をもう一度実行してください。

8. 以下のタイプのメッセージを受信したら、Active Directory のドメイン管理者の名前およびパスワードの情報を入力します。

In order to create this filer's domain account, you must supply the name and password of an administrator account with sufficient privilege to add the filer to the ADKDC.LAB.DOCEXAMPLE.COM domain. Please enter the Windows 2000 user [Administrator@ADKDC.LAB.DOCEXAMPLE.COM] Password for Administrator:

パスワードが正確で、指定したアカウントがストレージ・システム・ドメイン内に適切なアクセス権を持っている場合、以下のタイプのメッセージを受信します。

CIFS - Logged in as administrator@ADKDC.LAB.DOCEXAMPLE.COM.
Welcome to the ADKDC (ADKDC.LAB.DOCEXAMPLE.COM) Windows 2000(tm) domain.
Kerberos now enabled for NFS.
NFS setup complete.

タスクの結果

NFS セットアップの完了時に、出力テキストに以下のようなメッセージが表示される場合があります。この出力はインストール処理の成果物で、無視できます。

CIFS is not licensed.
(Use the "license" command to license it.)

CIFS 構成後に Active Directory ベースの KDC を使用するための、NFS 用 Kerberos v5 セキュリティー・サービスの構成

既に `cifs setup` を実行して Data ONTAP を CIFS のための Active Directory を使用するように構成している場合、`nfs setup` は、CIFS のために指定しているいくつかの構成情報を自動的に使用します。

このタスクについて

注: 構成情報を入力するために、既に `nfs setup` を使用している場合は、受信するプロンプトは以下の手順に示されたものと異なる可能性があります。

1. 次のコマンドを入力します。 `nfs setup`

`nfs setup` から、次のメッセージを受信します。

Enable Kerberos for NFS?

2. `y` を入力して続行します。

KDC のタイプを指定することを求められます。

The filer supports these types of Kerberos Key Distribution Centers (KDCs):
1 - UNIX KDC
2 - Microsoft Active Directory KDC
Enter the type of your KDC (1-2):

3. `2` を入力します。

以下のメッセージを受信します。

Kerberos now enabled for NFS.
NFS setup complete.

タスクの結果

Data ONTAP は、Active Directory ベースの KDC Kerberos over NFS について構成されました。

UNIX ベースの KDC を使用するための、NFS 用 Kerberos v5 セキュリティー・サービスの構成

UNIX ベースの KDC を使用するために NFS 用 Kerberos v5 セキュリティー・サービスを構成するには、ストレージ・システムのプリンシパル (レルム・ユーザー ID) を作成、およびキータブ (キー・テーブル・ファイル) を生成し、UNIX ベースの KDC を使用するように Data ONTAP を構成します。

始める前に

以下の要件を満たしていることを確認してください。

- NFS クライアントおよび UNIX ベースの KDC が、root および少なくとも 1 つの root ではないクライアントのクライアント・プリンシパルを使用して、セットアップされている。
- NFS アクセスが、クライアントおよび既存のネットワーク・サーバーについて確認されている。

セキュア NFS をセットアップして使用する前に、ストレージ・システムで DNS を有効にすることを強く推奨します。ホスト・コンポーネントがまだ完全に限定されていないドメイン名で、かつ DNS が有効にされていない場合、DNS を後で有効にするために、すべての NFS サーバーのプリンシパル名を変更する必要があります。

注: CIFS クライアントを UNIX ベースの KDC で認証することはできません (これは、所有制限のために、CIFS クライアントをサポートする UNIX ベースの Kerberos 実装環境がないためです)。ただし、Data ONTAP 7.3.1 以降のリリースでは Kerberos マルチ・レルム機能を提供しており、NFS クライアントの認証に UNIX ベースの KDC を使用するように NFS を構成している一方で、同時に CIFS クライアントの認証に Microsoft Active Directory ベースの KDC を使用するように CIFS を構成することができます。

このタスクについて

以下の手順は、ストレージ・システムを `nfs/hostname.domain@REALM` と呼ばれるサービス・プリンシパルとして、どのように標準的な UNIX ベースの KDC に追加するかという例で示しています。

プリンシパルの作成およびキータブ・ファイルの生成

プリンシパルの作成およびキータブ・ファイルの生成には、`kadmin` コマンドを使用します。

始める前に

ストレージ・システムでいずれかのバージョンの Kerberos が現在有効になっている場合は、まず `nfs setup` を実行して無効にする必要があります。Kerberos が有効な場合、次のプロンプトが表示されます。

Disable Kerberos for NFS?

応答 (y あるいは n) に関わらず、ストレージ・システムは NFS セットアップを終了します。Kerberos を無効にすることを選択した場合、ストレージ・システムは最初に現在の構成済み Kerberos 実装をすべて無効にします。UNIX ベースの Kerberos については、`nfs.kerberos.file_keytab.enable` オプションは `off` に設定されています。

1. UNIX ベースの Kerberos v5 サービスをサポートする UNIX あるいは Linux システムで `kadmin` コマンドを入力するか、あるいは KDC にログインしている場合は `kadmin.local` コマンドを入力します。
2. `kadmin` あるいは `kadmn.local` コマンド行で、コマンド `ank -randkey nfs/hostname.domain` を入力します。`hostname` は、NFS サーバーのプリンシパル名で、`domain` は、NFS サーバーのプリンシパルのドメインです。

NFS サーバーのためのプリンシパルが作成されます。例えば、
nfs/server.lab.my_company.com@LAB.MY_COMPANY.COM を作成した場合、レ
ームは @LAB.MY_COMPANY.COM です。

ご使用の KDC ソフトウェアが、des3* あるいは aes128* 暗号化タイプのような
Data ONTAP がサポートしないデフォルトの暗号化タイプでプリンシパルを作成
する場合、des-cbc-md5:normal のような Data ONTAP がサポートする暗号化タ
イプを指定するために、ank コマンドを -e パラメーターと一緒に呼び出す必要
があります。例えば、次のコマンドは des-cbc-md5 暗号化タイプでプリンシパル
を作成します。kadmin: ank -e des-cbc-md5:normal -randkey
nfs/server.lab.my_company.com

詳細情報については、ご使用の KDC ソフトウェアの資料を参照してください。

3. kadmн あるいは kadmн.local コマンド行で、コマンド xst -k/tmp/
filer.UNIX_krb5.conf nfs/hostname.domain を入力します。ここで hostname
および domain はそれぞれ、ステップ 2 で作成したサーバー・プリンシパルの
ホスト名およびサーバー・プリンシパルのドメインです。例えば、次を入力しま
す。kadmin: xst -k/tmp/filer.UNIX_krb5.conf nfs/
server.lab.my_company.com

サーバー・プリンシパル nfs/
server.lab.my_company.com@LAB.MY_COMPANY.COM ためのキータブが作成さ
れます。KVNO 3 暗号化タイプ DES-CBC-CRC が、キータブ
WRFILE:/tmp/filer.UNIX_krb5.conf に追加されます。

ご使用の KDC ソフトウェアが、des3* あるいは aes128* 暗号化タイプのような
Data ONTAP がサポートしないデフォルトの暗号化タイプでキータブを作成する
場合、des-cbc-md5:normal のような Data ONTAP がサポートする暗号化タイプ
を指定するために、xst コマンドを -e パラメーターと一緒に呼び出す必要があ
ります。例えば、次のコマンドは des-cbc-md5 暗号化タイプでキータブを作成し
ます。xst -k /tmp/filer.keytab -e des-cbc-md5:normal nfs/
filer.lab.mycompany.com

詳細情報については、ご使用の KDC ソフトウェアの資料を参照してください。

4. NFS サーバーで、次のコマンドを入力します。cp /tmp/
filer.UNIX_krb5.keytab /net/filer/vol/vol0/etc/krb5.UNIX_krb5.keytab

キータブがストレージ・システムにコピーされます。

重要: いったんキータブがストレージ・システムにコピーされると、ボリュー
ムの /etc サブディレクトリーをエクスポートしないようにしてください。/etc
サブディレクトリーをエクスポートすると、クライアントがキー情報を読み取る
ことができ、ストレージ・システムとしてなりすますことができます。

5. krb5.conf ファイルをストレージ・システムにコピーするには、以下のうち 1 つ
を実行します。MIT KDC ソフトウェアが稼働している UNIX クライアント
で、次のコマンドを入力します。cp /etc/krb5.conf /net/filer/vol/vol0/etc/
krb5.conf SEAM が稼働している Solaris クライアントで、次のコマンドを入力
します。cp /etc/krb5/krb5.conf /net/filer/vol/vol0/etc/krb5.conf

NFS 用 Kerberos v5 セキュリティー・サービスの有効化

NFS 用 Kerberos v5 セキュリティー・サービスを有効にするには、`nfs setup` コマンドを使用します。

始める前に

`nfs setup` コマンドによって、サーバー・プリンシパルおよびキータブ・ファイルを作成する前に、UNIX ベースの KDC のためにストレージ・システムを構成することができます。ただし、Kerberos を使用する前に、サーバー・プリンシパルおよびキータブ・ファイルを作成する必要があります。

このタスクについて

1. 次のコマンドを入力します。`nfs setup`

`nfs setup` から、次のメッセージを受信します。

```
Enable Kerberos for NFS?
```

2. `y` を入力して続行します。

KDC のタイプを指定することを求められます。

```
The filer supports these types of Kerberos Key Distribution Centers (KDCs):
1 - UNIX KDC
2 - Microsoft Active Directory KDC
Enter the type of your KDC (1-2):
```

3. `1` を入力します。

サーバー・プリンシパル・ファイルおよびキータブ・ファイルがセットアップされていない場合は、いくつかの警告のうちの 1 つを受信しますが、セットアップ・プロセスは継続します。

フレッシュ・インストールの後に `nfs setup` を実行している場合、以下の警告メッセージを受信します。

```
There is no /etc/krb5.conf file yet. You will need to establish one.
Unix KDC uses the keytab file /etc/UNIX_krb5.keytab. There is no /etc/UNIX_krb5.keytab
file yet. You will need to establish one.
```

`cifs setup` を実行した後に `nfs setup` を実行している場合、(そして Active Directory ベースの KDC を使用するために CIFS を構成している場合)、以下の警告メッセージを受信します。

```
There is no /etc/krb5.conf file yet. You will need to establish one.
You have an existing keytab file /etc/krb5.keytab. Your new keytab file for Unix KDC
would be /etc/UNIX_krb5.keytab. NOTE: If CIFS Active Directory based authentication
has been configured on this filer at any point in the past, the /etc/krb5.keytab might
belong to CIFS. Do you want to rename your existing keytab file /etc/krb5.keytab to
the new keytab file /etc/UNIX_krb5.keytab.
(Yes/No)? n
Unix KDC uses the keytab file /etc/UNIX_krb5.keytab. There is no /etc/UNIX_krb5.keytab
file yet. You will need to establish one.
```

Data ONTAP 7.3.1 以前のリリースから Data ONTAP をアップグレードした後、初めて `nfs setup` を実行している場合、以下の警告メッセージを受信します。

```
Your new keytab file for Unix KDC would be /etc/UNIX_krb5.keytab.  
NOTE: If CIFS Active Directory based authentication has been configured on this  
filer at any point in the past, the /etc/krb5.keytab might belong to CIFS. Do you  
want to rename your existing keytab file /etc/krb5.keytab to the new keytab file  
/etc/UNIX_krb5.keytab. (Yes/No)? y  
/etc/krb5.keytab renamed to /etc/UNIX_krb5.keytab
```

最後の 2 つのプロンプトのいずれかに否定的な応答をした場合は、`nfs setup` はキータブ・ファイルの名前変更なしで処理します。

4. プロンプト `Enter the Kerberos realm name.` を受信した場合は、UNIX ベースの KDC のためのレルム名を入力してください。レルム名は、NFS サーバーの Kerberos プリンシパル名 (NFS サーバー・プリンシパルのために指定した名前) のレルム固有の部分です。例えば、`MY_COMPANY.COM` を入力します。入力したレルム名は、`nfs.kerberos.realm` オプションの値を変更することで、後で確認あるいは変更することができます。`options nfs.kerberos.realm realm_name` 例 `options nfs.kerberos.realm LAB.MY_COMPANY.COM`

注: Data ONTAP は、UNIX ベースの KDC については小文字のレルム名をサポートしますが、Active Directory KDC についてはサポートしません。

5. 次のプロンプトを受信した場合は、ホスト・インスタンスを入力してください。
`Enter the host instance of the NFS server principal name [default:
server.lab.my_company.com]:`

例 `server.lab.my_company.com`

DNS が有効に設定されている場合、ホストの完全修飾ドメイン名を入力したことを確認するために使用されます。名前の一部を入力し、ホストが DNS に入力されている場合は、欠落したドメイン情報は入力情報に追加されます。

入力したホスト・インスタンスは、`nfs.kerberos.principal` オプションを使用して確認することができます。

```
options nfs.kerberos.principal
```

`nfs setup` コマンドはホスト・インスタンスおよびレルム名に関する入力情報を Kerberos プリンシパルの特定に使用します。プリンシパルは、`nfs setup` エントリーから、以下に記載されているように導き出されます。

```
nfs/value from nfs.kerberos.principal@value from nfs.kerberos.realm
```

いったんホスト・インスタンスを入力して `nfs setup` を終了すると、ストレージ・システムは生成したキー・テーブルを使用するように構成されます。この構成を後で変更する場合は、もう一度 `nfs setup` を実行します。

NFS クライアントが Kerberos v5 セキュリティー・サービスをサポートするかの判別

NFS クライアントで Kerberos v5 セキュリティー・サービスを使用する前に、NFS クライアントが RFC1964 および RFC2203 をサポートすることを確認してください。

このタスクについて

Kerberos v5 セキュリティーをサポートする NFS クライアントのリストは、生産ラボラトリーあるいは Connectathon (www.connectathon.org) のようなインターオペラビリティ・テスト・イベントのいずれかでテストされた、広範囲で使用されている NFS クライアントを含みます。

例えば、以下の NFS クライアントは Kerberos v5 をサポートします。

オペレーティング・システム	Kerberos v5 をサポートするバージョン	必要なソフトウェアおよび可用性情報
AIX	NFSv2、NFSv3、または NFSv4 が稼働している AIX 5.3	AIX 5L 拡張パックおよび Web ダウンロード・パック、IBM から入手可能
Linux	NFSv2、NFSv3、または NFSv4 が稼働している Linux 2.6	追加のソフトウェアは必要ありません。
Solaris	NFSv2、または NFSv3 が稼働している Solaris 2.6	Sun エンタープライズ認証メカニズム (SEAM) 1.0、Sun Microsystems の Solaris Easy Access Server (SEAS) 3.0 製品バンドルから入手可能
	NFSv2、または NFSv3 が稼働している Solaris 7	SEAM 1.0、Sun Microsystems の SEAS 3.0 製品バンドルから入手可能
	NFSv2、または NFSv3 が稼働している Solaris 8	SEAM 1.0.1、 www.sun.com の Sun Microsystems の Solaris 8 Admin Pack または Solaris 8 Encryption Pack から入手可能
	NFSv2、または NFSv3 が稼働している Solaris 9	追加のソフトウェアは必要ありません。
	NFSv2、NFSv3、または NFSv4 が稼働している Solaris 10	追加のソフトウェアは必要ありません。
Windows	NFSv2、または NFSv3 が稼働している Windows クライアント	Hummingbird NFS Maestro バージョン 7 または NFS Maestro Solo バージョン 7
	NFSv2、NFSv3、または NFSv4 が稼働している Windows クライアント	Hummingbird NFS Maestro Client バージョン 8 または NFS Maestro Solo バージョン 8

マウント問題のデバッグ

マウント問題をデバッグするために、マウント・サービスの統計を表示し、mountd 要求をトレースすることができます。

マウント・サービス統計の表示

マウント・サービス統計を表示するには、nfsstat -d コマンドを入力します。

タスクの結果

Data ONTAP は、以下のマウント・サービス統計を表示します。

```
v2 mount (requested, granted, denied, resolving)
```

```
v2 unmount (requested, granted, denied)
```

```
v2 unmount all (requested, granted, denied)
```

```
v3 mount (requested, granted, denied, resolving)
```

```
v3 unmount (requested, granted, denied)
```

```
v3 unmount all (requested, granted, denied)
```

```
mount service requests (curr, total, max, redriven)
```

詳細情報については、na_nfsstat(1) のマニュアル・ページを参照してください。

mountd 要求のトレース

mountd 要求をトレースするには、/etc/syslog.conf ファイルに *.debug エントリーを追加し、nfs.mountd.trace オプションを on に設定します。

このタスクについて

DOS アタックの間に何度も syslog にヒットする可能性があるため、このオプションはデバッグ・セッションの間のみ有効にするべきです。

デフォルトでは、nfs.mountd.trace オプションは off です。

syslog.conf ファイルへのエントリーの追加に関する詳細情報については、na_syslog.conf(5) のマニュアル・ページを参照してください。

nfs.mountd.trace に関する詳細情報については、na_options(1) のマニュアル・ページを参照してください。

NFS 統計の表示

すべての NFS バージョンについて NFS 統計を表示するには、`nfsstat` コマンドを使用します。

このタスクについて

`nfsstat` コマンドを使用して、すべてのクライアントに関する NFS 統計を表示することができます。あるいは、`nfs.per_client_stats.enable` オプションが `on` の場合、`nfsstat -h` または `nfsstat -l` コマンドを使用して、クライアントごとの NFS 統計を表示することができます。

NFS 統計の表示に加えて、`nfsstat` コマンドを使用して NFS 統計をリセットすることができます。

詳細情報については、`na_nfsstat(1)` のマニュアル・ページ、および次のトピックを参照してください。

マウント・サービス統計の表示

NFSv4 オープン権限委任統計の表示

NFS 統計を表示するには、次のコマンドを入力します。`nfsstat`

NFSv3 の有効化あるいは無効化

`nfs.v3.enable` オプションを `on` あるいは `off` に設定することで、それぞれ NFSv3 を有効あるいは無効にすることができます。(このオプションは、デフォルトでは `on` です。)

このタスクについて

デフォルトでは、NFSv3 は有効、NFSv4 は無効です。

以下を実施したい場合、	以下を実行してください。
NFSv3 を有効にする	次のコマンドを入力します。 <code>options nfs.v3.enable on</code>
NFSv3 を無効にする	次のコマンドを入力します。 <code>options nfs.v3.enable off</code>

NFSv4 クライアントのサポート

NFSv4 クライアントのサポートは、NFSv4 プロトコルの有効化あるいは無効化、NFSv4 ユーザー ID ドメインの指定、NFSv4 ACL およびファイルの権限委任の管理、およびファイルとレコードのロックの構成を含みます。

NFSv4 の Data ONTAP サポートについて

Data ONTAP は SPKM3 および LIPKEY セキュリティー・メカニズムを除く NFSv4 のすべての必須機能をサポートします。

この機能は、以下の項目で構成されます。

- **COMPOUND**— クライアントが単一のリモート・プロシージャ・コール (RPC) 要求で、複数のファイル操作を要求することを許可します。
- **Open delegation**— サーバーが、読み取りおよび書き込みアクセスに関して一部のタイプのクライアントへファイル制御の代行を委任することを許可します。
- **Pseudo-fs**— ストレージ・システム上のマウント・ポイントを決定するために NFSv4 サーバーによって使用されます。NFSv4 にはマウント・プロトコルがありません。
- **Locking**— リース・ベース。NFSv4 には個別の ネットワーク・ロック・マネージャー (NLM) あるいは ネットワーク状況モニター (NSM) プロトコルがありません。
- **Named attributes**— Windows NT ストリームと同様です。

NFSv4 プロトコルに関する詳細については、「RFC 3050」について Web で検索してください。RFC 3050 は「Internet Engineering Task Force (IETF) Request for Comments」規格で「Network File System (NFS) version 4 Protocol」と表題をつけられており、NFSv4 プロトコルを定義しています。

NFSv4 の Data ONTAP サポートの制限

NFSv4 に関する Data ONTAP サポートの制限について認識しておく必要があります。

- **SPKM3** および **LIPKEY** セキュリティー・メカニズムはサポートされません。
- 委任機能はすべてのクライアント・タイプでサポートされません。
- **UTF8** ボリューム以外のボリュームで、非 ASCII 文字での名前はストレージ・システムに拒否されます。
- すべてのファイル・ハンドルは永続的です。サーバーは揮発性のファイル・ハンドルを提供しません。
- マイグレーションおよびレプリカの生成はサポートしません。
- すべての推奨される属性は、以下を除いてサポートされます。
 - **archive**
 - **hidden**
 - **homogeneous**
 - **mimetype**
 - **quota_avail_hard**
 - **quota_avail_soft**
 - **quota_used**
 - **system**
 - **time_backup**

注: **quota*** 属性はサポートされませんが、Data ONTAP は **RQUOTA** サイド・バンド・プロトコルによって、ユーザーおよびグループ **quota** をサポートします。

- NFSv4 は、ユーザー・データグラム・プロトコル (UDP) トランスポート・プロトコルを使用しません。

NFSv4 を有効にし、NFS over TCP を `options nfs.tcp.enable` を `off` に設定することで無効にした場合、NFSv4 は事実上は無効になります。

NFSv4 における `pseudo-fs` のマウント・ポイントへの影響

NFSv4 は、`pseudo-fs` (ファイル・システム) をマウント・ポイントの判別のためにストレージ・システムへのエントリー・ポイントとして使用します。 `pseudo-fs` は、セキュリティのために複数のポートではなく 1 つのポートを使用することを許可します。すべての NFSv4 サーバーは `pseudo-fs` の使用をサポートします。

`pseudo-fs` が NFSv4 で使用されているために、NFSv3 と NFSv4 の間でマウント・ポイントの不整合が生じる可能性があります。

後述の例では、以下のボリュームを使用します。

- `/vol/vol0` (ルート)
- `/vol/vol1`
- `/vol/home`

例 1

NFSv3 で `/vol/vol0` からの完全パスを使用しておらず、`filer:/` をマウントしている場合、マウント・ポイントは `filer:/vol/vol0` です。つまり、NFSv3 では、パスが `/vol` で始まっていない場合、Data ONTAP がパスの先頭に `/vol/vol0` を追加します。

NFSv4 では、`/vol/vol0` からの完全パスを使用しておらず、`filer:/` をマウントしている場合、`/vol/vol0` ではなく `pseudo-fs` のルートをマウントします。Data ONTAP は、パスの先頭に `/vol/vol0` を追加しません。

そのため、NFSv3 で `filer:/n/filer` をマウントして、NFSv4 で同じマウントを試行した場合、異なるファイル・システムをマウントすることになります。

例 2

NFSv4 `pseudo-fs` を実装する Data ONTAP では、ノード「/」および「`/vol`」は常に存在し、`pseudo-fs` へのあらゆる参照の共通接頭部を形成します。「`/vol`」で始まらない参照は無効です。

この例では、`/vol/vol0/home` ディレクトリーが存在します。NFSv3 では、`filer:/home/users` をマウントしている場合、`/home` は `/vol/vol0/home` ディレクトリーと認識されます。NFSv4 では、`filer:/home/users` をマウントしている場合、`/home` はボリューム `/vol/home` とは解釈されず、`pseudo-fs` ツリーの無効なパスであると認識されます。

NFSv4 の有効化あるいは無効化

`nfs.v4.enable` オプションを `on` あるいは `off` に設定することで、それぞれ NFSv4 を有効あるいは無効にすることができます。(デフォルトでは、このオプションは `off` に設定されています。)

以下を実施したい場合、	以下を実行してください。
NFSv4 を有効にする	次のコマンドを入力します。options nfs.v4.enable on
NFSv4 を無効にする	次のコマンドを入力します。options nfs.v4.enable off

NFSv4 のためのユーザー ID ドメインの指定

ユーザー ID ドメインを指定するには、nfs.v4.id_domain オプションを設定します。

このタスクについて

デフォルトで Data ONTAP が NFSv4 ユーザー ID のマッピングに使用するドメインは、NIS ドメインです (設定されている場合)。NIS ドメインが設定されていない場合、DNS ドメインが使用されます。例えば、複数のユーザー ID ドメインがある場合は、ユーザー ID ドメインを設定する必要がある場合があります。

次のコマンドを入力します。options nfs.v4.id_domain domain

NFSv4 ACL の管理

NFSv4 アクセス制御リスト (ACL) の有効化、無効化、設定、変更、および表示が可能です。

NFSv4 ACL の動作の仕方

NFSv4 ACL を使用しているクライアントは、システム上のファイルおよびディレクトリーの ACL を設定および表示することができます。新規のファイルあるいはサブディレクトリーが ACL を持つディレクトリー内に作成されると、新規のファイルまたはサブディレクトリーは、適切な継承フラグを持つタグがついた ACL 内のすべての ACL エントリー (ACE) を継承します。

アクセス・チェックのために、CIFS ユーザーは UNIX ユーザーにマッピングされています。マッピングされた UNIX ユーザーおよびそのユーザーのグループのメンバーシップは、ACL をチェックされます。

ファイルあるいはディレクトリーが ACL を持っている場合、その ACL はたとえばファイルあるいはディレクトリーへのアクセスに使用されているプロトコルが NFSv2、NFSv3、NFSv4、あるいは CIFS のどれであってもアクセス権のコントロールに使用され、またシステムで NFSv4 が使用可能になっていなくても使用されます。

ファイルおよびディレクトリーは、ACE に適切な継承フラグを持つタグがついている限り、(場合によっては適切な変更をして) 親ディレクトリーの NFSv4 ACL から ACE を継承します。

ファイルあるいはディレクトリーが、NFSv4 要求の結果として作成されると、その結果ファイルの ACL は、ファイル作成要求が ACL を含んでいたか、あるいは標準 UNIX ファイル・アクセス許可のみであったか、および親ディレクトリーが ACL を持っていたかどうかによって決まります。

- 要求が ACL を含んでいた場合、その ACL が使用されます。

- 要求が標準 UNIX ファイル・アクセス許可のみを含んでおり、親ディレクトリーが ACL を持つ場合、親ディレクトリーの ACL の ACE に適切な継承フラグを持つタグがついていれば、新規のファイルあるいはディレクトリーに継承されます。

注: 親 ACL は、`nfs.v4.acl.enable` が `off` に設定されている場合も継承されます。

- 要求が標準 UNIX ファイル・アクセス許可のみを含んでおり、親ディレクトリーが ACL を持っていない場合、クライアントのファイル・モードは 標準 UNIX ファイル・アクセス許可に設定されます。
- 要求が標準 UNIX ファイル・アクセス許可のみを含んでおり、親ディレクトリーが継承不可の ACL を持つ場合、要求に受け渡されたモード・ビットに基づくデフォルトの ACL が新規のオブジェクトで設定されます。

qtree のセキュリティの意味は、そのセキュリティ・スタイルおよび ACL (NFSv4 あるいは NTFS) によって決定されます。

UNIX セキュリティ・スタイルの qtree

- NFSv4 ACL およびモード・ビットが有効です。
- NTFS ACL は有効ではありません。
- Windows クライアントは属性の設定ができません。

NTFS セキュリティ・スタイルの qtree

- NFSv4 ACL は有効ではありません。
- NTFS ACL およびモード・ビットが有効です。
- UNIX クライアントは属性の設定ができません。

混合のセキュリティ・スタイルの qtree

- NFSv4 ACL およびモード・ビットが有効です。
- NTFS ACL は有効です。
- Windows および UNIX クライアントの両方が属性を設定できます。

注: qtree 内のファイルおよびディレクトリーは、NFSv4 ACL または NTFS ACL のいずれかを持つことができますが、両方を持つことはできません。Data ONTAP は、必要に応じて 1 つのタイプを他方のタイプに再マップします。

NFSv4 ACL を有効にする利点

NFSv4 ACL を有効にすることには多くの利点があります。

以下は、NFSv4 ACL を有効にすることの利点を示しています。

- ファイルおよびディレクトリーについて、より詳細なユーザー・アクセスのコントロール
- より良い NFS セキュリティ
- 改良された CIFS とのインターオペラビリティ
- ユーザーあたり 16 グループという NFS の制限の除去

NFSv4 ACL と Windows (NTFS) ACL 間の互換性

NFSv4 ACL は Windows のファイル・レベルの ACL (NTFS ACL) とは異なりますが、Data ONTAP は Windows プラットフォーム上で表示できるように NFSv4 ACL を Windows ACL にマッピングすることができます。

NFS クライアントに表示された Windows ACL を持つファイルに関するアクセス権は「表示」許可であり、ファイル・アクセスをチェックするのに使用されるアクセス権は Windows ACL のものです。

注: Data ONTAP は、POSIX ACL をサポートしません。

NFSv4 ACL の有効化および無効化

NFSv4 ACL を有効あるいは無効にするには、`nfs.v4.acl.enable` オプションをそれぞれ `on` あるいは `off` に設定します。このオプションは、デフォルトでは `off` に設定されています。

始める前に

`nfs.v4.acl.enable` オプションは、NFSv4 ACL の設定および表示をコントロールしますが、アクセス権限のチェックするためのこれらの ACL の適用はコントロールしません。詳細情報については、`na_options(1)` のマニュアル・ページを参照してください。

NFSv4 ACL を有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
NFSv4 ACL を有効にする	次のコマンドを入力します。 <code>options nfs.v4.acl.enable on</code>
NFSv4 ACL を無効にする	次のコマンドを入力します。 <code>options nfs.v4.acl.enable off</code>

NFSv4 ACL の設定あるいは変更

NFSv4 ACL を設定あるいは変更するには、`setacl` コマンドを使用します。

始める前に

NFSv4 および NFSv4 ACL が有効にされている必要があります。それらが有効にされた後、NFSv4 を使用しているクライアントから ACL を設定あるいは変更することができます。

次のコマンドを入力します。`setfacl -m user:nfsuser:rwx a`

NFSv4 ACL の表示

NFSv4 ACL を表示するには、`getfacl` コマンドを使用します。

次のコマンドを入力します。`getfacl filename`

ファイルの NFSv4 ACL の表示

```
ss> getfacl a
# file: a
# owner: nfs4user
# group: engr
# group: engr
user::rw-
user:nfs4user:rwx          #effective:rwx
group::r--                 #effective:r--
mask:rwx
other:r--
```

同じファイルについて `ls -l` コマンドを実行すると、以下が表示されます。

```
-rw-r--r--+ 1 nfs4user 0 May 27 17:43 a
```

この出力での `+` は、Solaris クライアントがこのファイルに ACL が設定されていると認識したことを示します。

NFSv4 オープン権限の委任の管理

NFSv4 オープン権限の委任を有効あるいは無効に設定することができ、また NFSv4 オープン権限の委任の統計を取得することができます。

NFSv4 のオープン権限の委任の動作の仕方

Data ONTAP は、読み取りおよび書き込みのオープン権限の委任を RFC 3530 に従ってサポートします。

RFC 3530 に示されているように、NFSv4 クライアントがファイルを開く際、Data ONTAP はオープンおよび書き込み要求の処理をファイルを開いているクライアントに委任することができます。オープン権限の委任には、読み取りと書き込みの 2 つのタイプがあります。読み取りオープン権限の委任により、クライアントは読み取りのためにファイルをオープンする要求を処理することができますが、他への読み取りアクセスは拒否されません。書き込みオープン権限の委任は、クライアントがすべてのオープン要求を処理することを許可します。

権限の委任は、便宜的ロックが有効に設定されているかどうかに関わらず、すべてのスタイルの `qtree` 内のファイル上で動作します。

クライアントへのファイル操作の権限委任は、委任の期限が切れた場合や、ストレージ・システムが他のクライアントから以下の要求を受信した場合に、再呼び出しすることが可能です。

- ファイルへの書き込み、書き込みのためのファイル・オープン、あるいは「読み取り拒否」のためのファイル・オープン
- ファイル属性の変更
- ファイル名変更
- ファイル削除

リースの期限が切れると委任の状態は取り消され、すべての関連する状態は「soft (ソフト)」とマークされます。これは、前に委任を保持していたクライアントによってリースの期限が更新される前に、ストレージ・システムが別のクライアントから

この同じファイルに対する競合するロック要求を受信した場合、競合するロックが認可されることを意味します。競合するロックがなく、委任を保持しているクライアントがリースの期限を更新した場合は、ソフト・ロックはハード・ロックに変更され、競合するアクセスが発生した場合に削除されることはありません。ただし、権限の委任はリースの期限の更新時に、再度認可はされません。

サーバーがリブートすると、権限委任の状態は失われます。クライアントは、権限委任要求のプロセス全体をもう一度実行する必要はなく、再接続によって権限委任状態を取り戻すことができます。読み取り権限委任を保持したクライアントがリブートすると、すべての権限委任の状態に関する情報は、再接続時にストレージ・システム・キャッシュからフラッシュされます。クライアントは新規の権限委任を確立するために、権限委任要求を発行する必要があります。

NFSv4 読み取りオープン権限委任の有効化あるいは無効化

NFSv4 読み取りオープン権限委任を有効あるいは無効にするには、`nfs.v4.read_delegation` オプションをそれぞれ `on` あるいは `off` に設定します。デフォルトでは、このオプションは `off` に設定されています。

このタスクについて

読み取りオープン権限委任を有効にすることで、ファイルのオープンおよびクローズに関連する、メッセージ・オーバーヘッドの多くを除去することができます。読み取りオープン権限委任を有効にするものの欠点は、サーバーおよびそのクライアントが、サーバーのリブートまたは再始動、クライアントのリブートまたは再始動、あるいはネットワーク分割の発生の後に、委任を復旧させる必要があることです。

読み取りオープン権限委任を有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
読み取りオープン権限委任を有効にする	次のコマンドを入力します。 <code>options nfs.v4.read_delegation on</code>
読み取りオープン権限委任を無効にする	次のコマンドを入力します。 <code>options nfs.v4.read_delegation off</code>

次のタスク

オープン権限委任オプションは、変更してすぐに有効になります。NFS をリブートあるいは再始動する必要はありません。

NFSv4 書き込みオープン権限委任の有効化あるいは無効化

書き込みオープン権限委任を有効あるいは無効にするには、`nfs.v4.write_delegation` オプションをそれぞれ `on` あるいは `off` に設定します。デフォルトでは、このオプションは `off` です。

このタスクについて

書き込みオープン権限委任を有効にすることで、ファイルのオープンおよびクローズに加えてファイルおよびレコードのロックに関連する、メッセージ・オーバーヘッドの多くを除去することができます。書き込みオープン権限委任を有効にするこ

との欠点は、サーバーおよびそのクライアントが、サーバーのリブートまたは再始動、クライアントのリブートまたは再始動、あるいはネットワーク分割の発生後に、委任を復旧させるために追加のタスクを実行する必要があることです。

書き込みオープン権限委任を有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
書き込みオープン権限委任を有効にする	次のコマンドを入力します。options nfs.v4.write_delegation on
書き込みオープン権限委任を無効にする	次のコマンドを入力します。options nfs.v4.write_delegation off

次のタスク

オープン権限委任オプションは、変更してすぐに有効になります。NFS をリブートあるいは再始動する必要はありません。

NFSv4 オープン権限委任統計の表示

NFSv4 オープン権限委任要求に関する情報を表示するには、`nfsstat` コマンドを使用します。

タスクの結果

`nfsstat` コマンドが返す結果は、エラーのために拒否された要求だけではなく、認可されたオープン権限委任要求も含みます。

次のタスク

ストレージ・システムが拒否したオープン権限委任要求に関する情報については、システム・ログ・ファイルを確認してください。

すべてのクライアントに関する NFSv4 オープン権限委任統計の表示:

すべてのクライアントに関する NFSv4 オープン権限委任情報を表示するには、`nfsstat -l` コマンドを入力します。

次のコマンドを入力します。`nfsstat -l count`

タスクの結果

ストレージ・システムは、指定した数までの各クライアントに関する個々の NFSv4 オープン権限委任統計を返します。数を指定しない場合は、ストレージ・システムは各クライアントによって実行された NFS 操作の総数の順番で、最初の 256 クライアントに関する統計を返します。

特定のクライアントに関する NFSv4 オープン権限委任統計の表示:

特定のクライアントに関する NFSv4 オープン権限委任情報を表示するには、`nfsstat -h` コマンドを使用します。

次のコマンドを入力します。`nfsstat -h hostname or ip_address`

タスクの結果

ストレージ・システムは、特定のクライアントに関する個々の NFSv4 オープン権限委任統計を返します。

vFiler ユニットに関する NFSv4 オープン権限委任統計の表示:

vFiler ユニットに関する NFSv4 オープン権限委任統計を表示するには、vFiler ユニットのコンテキストで `nfsstat -d` コマンドを実行します。

次のコマンドを入力します。 `vfiler run filename nfsstat -d`

ストレージ・システムに関する NFSv4 オープン権限委任統計の表示:

ストレージ・システムに関する NFSv4 オープン権限委任情報を表示するには、`nfsstat -d` コマンドを入力します。

次のコマンドを入力します。 `nfsstat -d`

タスクの結果

ストレージ・システムは、現在のおよび再呼び出しされた NFSv4 オープン権限委任を含めた、ストレージ・システムによってハンドルされた NFSv4 オープン権限委任の総数を返します。ストレージ・システムによってハンドルされた現在の NFSv4 オープン権限委任のみを表示するには、`lock status` コマンドを使用します。

NFSv4 ファイルおよびレコードのロックの構成

ロックのリース期間および猶予期間を指定することで、NFSv4 ファイルおよびレコードのロックを構成することができます。

NFSv4 ファイルおよびレコード・ロックについて

NFSv4 クライアントの場合、Data ONTAP は NFSv4 バイト範囲のファイル・ロック・メカニズムをサポートし、すべてのファイル・ロックの状態はリース・ベース・モデルの下で維持されます。

RFC 3530 に従って、Data ONTAP は NFS クライアントによって保持されるすべての状態に関する単一のリース期間を定義します。クライアントが定義された期間内にリースを更新しない場合は、クライアントのリースに関連するすべての状態はサーバーによって解放される可能性があります。クライアントは、リースを明示的に更新するか、あるいはファイルの読み取りのような操作の実行によって自動的に更新することができます。

さらに、Data ONTAP は猶予期間を定義します。これは、サーバーのリカバリー中にクライアントのロック状態をレクラメーション処理する特別な処理の期間です。

用語	定義 (RFC 3530 を参照)
リース	Data ONTAP が変更不可でクライアントに対するロックを認可する期間。
猶予期間	サーバーのリカバリー中にクライアントが Data ONTAP からのロック状態のレクラメーション処理を試行する期間。

用語	定義 (RFC 3530 を参照)
ロック	特に断りがない限り、ファイル (共有) ロックと同様に両方のレコード (バイト範囲) ロックを参照します。

Data ONTAP はアクティブ/アクティブではない構成で最大 64K のファイル・ロックの状態を、またアクティブ/アクティブ構成で最大 32K のファイル・ロックの状態を維持します。これらの状態について、Data ONTAP は単一のクライアントに関して最大 16K のファイル・ロックの状態を維持します。

注: リカバリー中は、Data ONTAP は新規のロック要求を認可できる前にリース期間および猶予期間の有効期限が切れるのを待つ必要があります。

NFSv4 ロックのリース期間の指定

NFSv4 ロックのリース期間 (Data ONTAP が変更不可でクライアントに対するロックを認可する期間) を指定するには、`nfs.v4.lease_seconds` オプションを設定します。

このタスクについて

デフォルトでは、このオプションは 30 に設定されています。このオプションの最小値は 10 です。このオプションの最大値はロック猶予期間で、`locking.lease_seconds` オプションで設定することができます。

RFC 3530 で指定されているように、「短いリースは早いサーバーの復旧に良い」一方で「長いリースは大規模なインターネット・サーバーが非常に多くのクライアントを取り扱うには親切で寛大」です。

次のコマンドを入力します。 `options nfs.v4.lease_seconds n`

<i>n</i>	秒単位でのリース期間です。
----------	---------------

NFSv4 ロックの猶予期間の指定

NFSv4 ロックの猶予期間 (サーバーの復旧中にクライアントが Data ONTAP からロック状態を取り戻そうとする期間) を指定するには、`locking.grace_lease_seconds` オプションを設定します。このオプションは、ロックのリース期間および猶予期間の両方を指定することに注意してください。

このタスクについて

デフォルトでは、このオプションは 45 に設定されています。

次のコマンドを入力します。 `options locking.grace_lease_seconds n`

<i>n</i>	秒単位での猶予期間です。
----------	--------------

PC-NFS クライアントのサポート

PC-NFS クライアントをサポートするには、pcnfsd デーモンを有効にし、ストレージ・システムのローカル・ファイルに PC-NFS エントリーを作成し、そして PC-NFS ユーザーがストレージ・システム上に作成するファイルおよびディレクトリーのための `umask` を定義します。

pcnfsd デーモンの動作の仕方

Data ONTAP の pcnfsd デーモンは、PC-NFS バージョン 1 または 2 を使用してクライアントの認証サービスを提供します。認証された PC-NFS ユーザーは、NFS ユーザーと同様にストレージ・システム上にファイル・システム・パスをマウントすることができます。pcnfsd デーモンは、プリンター・サービスをサポートしません。

pcnfsd デーモンが認証要求を受信すると、ユーザー・パスワードを検証するためにローカル・ファイルまたは NIS マップを使用できます。使用されるローカル・ファイルは、`/etc/shadow` ファイルまたは `/etc/passwd` ファイルです。使用される NIS マップは、`passwd.adjunct` または `passwd.byname` です。シャドー・ソースが使用可能な場合、Data ONTAP はそれを使用します。シャドー・ソースは、パスワード・データベースの代わりに、暗号化されたユーザー情報を含みます。

以下のリストは、PC-NFS バージョン 1 および 2 のユーザーの認証に、pcnfsd デーモンがローカル・ファイルまたは NIS マップをどのように使用するかを示しています。

シャドー・ソースが使用可能な場合、Data ONTAP はユーザーのパスワードを判別するのに、`/etc/shadow` ファイルまたは `passwd.adjunct` NIS マップを使用します。

シャドー・ソースが使用可能ではない場合、Data ONTAP はユーザーのユーザー ID (UID)、プライマリーのグループ ID (GID)、およびパスワードを判別するのに、`/etc/passwd` ファイルまたは `passwd.byname` NIS マップを使用します。

pcnfsd デーモンが PC-NFS バージョン 2 の認証要求を受信すると、`/etc/group` ファイルまたは `group.byname` NIS マップを検索し、ユーザーが属するすべてのグループを判別します。

pcnfsd デーモンの有効化あるいは無効化

pcnfsd デーモンを有効あるいは無効にするには、`pcnfsd.enable` オプションをそれぞれ `on` あるいは `off` に設定します。

始める前に

pcnfsd デーモンを有効にする前に、ストレージ・システム上で NFS を有効に設定する必要があります。

このタスクについて

PC-NFS ユーザーがストレージ・システム上のファイル・システム・パスにマウントを試みる際に、ストレージ・システムに PC-NFS ユーザーを認証させたい場合、pcnfsd デーモンを有効にします。他のコンピューターにユーザーを認証させたい場

合は、pcnfsd デーモンを有効にする必要はありません。他のコンピューターに認証されたユーザーは、ストレージ・システムに認証されたユーザーと同じように、ストレージ・システム上のファイル・システム・パスにアクセスすることができます。

pcnfsd デーモンを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
pcnfsd デーモンを有効にする	次のコマンドを入力します。options pcnfsd.enable on
pcnfsd デーモンを無効にする	次のコマンドを入力します。options pcnfsd.enable off

ストレージ・システムのローカル・ファイルでの PC-NFS ユーザー・エントリーの作成

ストレージ・システムのローカル・ファイルに PC-NFS ユーザー・エントリーを作成するには、すべての PC-NFS ユーザーを適切に認証している UNIX ホストから /etc/passwd、/etc/shadow、および /etc/group ファイルをストレージ・システムにコピーします。

このタスクについて

PC-NFS ユーザーの認証およびグループ・メンバーシップの判別にローカル・ファイルを使用したい場合は、ストレージ・システムのローカル・ファイルに PC-NFS ユーザー・エントリーを作成します。

PC-NFS ユーザーが作成したファイルおよびディレクトリーの umask の定義

PC-NFS ユーザーが作成したファイルおよびディレクトリーの umask を定義するには、pcnfsd.umask オプションを設定します。

このタスクについて

NFS ユーザーと異なり、PC-NFS ユーザーは UNIX umask コマンドを実行して、デフォルトのファイル・アクセス権を決定するファイル・モード作成マスク (umask) を設定することができません。しかし、Data ONTAP によって、すべての PC-NFS ユーザーの umask を定義することが可能です。

それぞれのファイルのアクセス権は、3 つの 8 進数の値で定義され、所有者、グループ、およびその他へ適用されます。PC-NFS クライアントが新しいファイルを作成すると、Data ONTAP は定義した 3 桁の 8 進数である umask を 666 から引き算します。結果の 8 進数字がファイル・アクセス権として使用されます。

デフォルトでは、umask は 022 で、アクセス権の実効 8 進数字は 644 であることを意味します。これらのアクセス権はファイル所有者によるファイルの読み取りおよび書き込みを可能にし、またグループおよび他のユーザーによるファイルの読み取りを可能にします。

以下の表は、umask の各数字について説明しています。

umask の数字	説明
0	読み取りおよび書き込み許可
2	書き込み許可
4	読み取り専用許可
6	アクセス権なし

コマンド `options pcnfsd.umask umask` を入力します。ここで、*umask* は 3 桁の 8 進数です。

WebNFS クライアントのサポート

WebNFS クライアントをサポートするには、WebNFS プロトコルを有効にし、(オプションで) WebNFS ルート・ディレクトリーを設定します。

このタスクについて

WebNFS プロトコルを有効にすると、WebNFS クライアント・ユーザーは `nfs://` で始まる URL を指定して、ストレージ・システムからファイルを転送することができます。

WebNFS プロトコルの有効化あるいは無効化

WebNFS プロトコルを有効あるいは無効にするには、`nfs.webnfs.enable` オプションをそれぞれ `on` あるいは `off` に設定します。

WebNFS プロトコルを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
WebNFS プロトコルを有効にする	次のコマンドを入力します。 <code>options nfs.webnfs.enable on</code>
WebNFS プロトコルを無効にする	次のコマンドを入力します。 <code>options nfs.webnfs.enable off</code>

WebNFS ルート・ディレクトリーの設定

WebNFS ルート・ディレクトリーを設定するには、ルート・ディレクトリーの名前を指定します。次に、ルート・ディレクトリーを有効にします。

このタスクについて

WebNFS 検索のためにルート・ディレクトリーを設定した場合、WebNFS ユーザーは、絶対パス名の代わりにルート・ディレクトリーの相対パス名のみを指定することができます。例えば、WebNFS ルート・ディレクトリーが `/vol/vol1/web` の場合、WebNFS ユーザーは URL として `nfs://specs` を指定することで `/vol/vol1/web/specs` ファイルにアクセスすることができます。

WebNFS ルート・ディレクトリー名の指定

WebNFS ルート・ディレクトリーの名前を指定するには、`nfs.webnfs.rootdir` オプションを設定します。

コマンド `options nfs.webnfs.rootdir directory` を入力します。`directory` は、ルート・ディレクトリーの絶対パスです。

WebNFS ルート・ディレクトリーの有効化

WebNFS ルート・ディレクトリーを有効にするには、`nfs.webnfs.rootdir.set` オプションを `on` に設定します。

始める前に

有効にする前に、WebNFS ルート・ディレクトリーの名前を指定する必要があります。

次のコマンドを入力します。`options nfs.webnfs.rootdir.set on`

NFS over IPv6

Data ONTAP 7.3.1 から、NFS クライアントはご使用の ストレージ・システムから IPv6 ネットワーク上でファイルにアクセスすることができます。

NFS over IPv6 の有効化あるいは無効化

`nfs.ipv6.enable` オプションを `on` あるいは `off` に設定することで、NFS over IPv6 をそれぞれ有効あるいは無効にすることができます。

始める前に

`ip.v6.enable` オプションを `on` に設定することで、ストレージ・システム の IPv6 を有効にする必要があります。 ストレージ・システム での IPv6 の有効化に関する詳細情報については、「*Data ONTAP Network Management Guide*」を参照してください。

このタスクについて

NFS over IPv6 を有効にしており、次に `ip.v6.enable` オプションを `off` に設定することで IPv6 を ストレージ・システム で無効にする場合、NFS over IPv6 は自動的に無効になります。

1.

以下を実施したい場合、	以下を実行してください。
NFS over IPv6 を有効にする	次のコマンドを入力します。 <code>options nfs.ipv6.enable on</code>
NFS over IPv6 を無効にする	次のコマンドを入力します。 <code>options nfs.ipv6.enable off</code>

2. NFS を再始動します。コマンド `nfs off` を入力し、次にコマンド `nfs on` を入力します。

IPv6 アドレスのテキスト表記

RFC 3513 によると、IPv6 アドレスをテキスト・ストリングで表記する優先フォームは `x:x:x:x:x:x:x` です。ここで、`x` は「アドレスの 8 個の 16 ビット断片の 16 進値」を表します。

例:

`FEDC:BA98:7654:3210:FEDC:BA98:7654:3210`

`1080:0:0:0:8:800:200C:417A`

詳細情報については、RFC 3513 について Web で検索してください。

CIFS を使用したファイル・アクセス

CIFS クライアントがご使用のストレージ・システム上のファイルにアクセスすることを許可するために、CIFS サーバーを有効にして構成することができます。

ストレージ・システム上での CIFS の構成

cifs setup コマンドを使用して、ストレージ・システム上で CIFS を構成することができます。

サポートされる Windows クライアントおよびドメイン・コントローラー

Data ONTAP が稼働しているストレージ・システムは、Windows クライアントとドメイン・コントローラーの特定のセットに対してサービスを提供することができます。

サポートされる Windows クライアント:

- Windows Server 2008
- Windows Vista
- Windows Server 2003 R2
- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT
- Windows 98
- Windows 95

サポートされるドメイン・コントローラー:

- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 2000
- Windows NT

詳細情報については、<http://www.ibm.com/storage/support/nas/> にある IBM NAS サポート・サイトの Windows ファイル・サービス (CIFS) 互換性マトリックスを参照してください。

ここでは、以下のトピックで情報を入手することが可能です。

- Interoperability of Data ONTAP and new releases of Microsoft operating systems (Data ONTAP と Microsoft オペレーティング・システムの新規リリースとのインターオペラビリティ)

- Data ONTAP and Microsoft Service Packs Compatibility Matrix (Data ONTAP と Microsoft Service Pack の互換性マトリックス)
- Data ONTAP and Microsoft Security Updates (Data ONTAP と Microsoft セキュリティー・アップデート)

cifs setup コマンドが行うこと

CIFS の初期構成の実行に加えて、cifs setup コマンドによって、いくつかのタスクが実行可能になります。

cifs setup コマンドによって、以下のタスクが実行できます。

- CIFS クライアントがアクセス可能な CIFS サーバーの作成および命名
- CIFS サーバーのドメインまたはワークグループへの参加、あるいはそれらの間の移動
- CIFS のローカル・ユーザーおよびグループのデフォルト・セットの作成

注:

グループ検索サービスに NIS を使用する場合、NIS グループのキャッシュを無効にすることが深刻なパフォーマンス低下の原因になる可能性があります。nis.enable オプションを使用して NIS 検索を有効にする場合は必ず、nis.group_update.enable オプションを使用してキャッシュも有効にすることを強く推奨します。

これら 2 つのオプションを一緒に有効にしなかった場合、CIFS クライアントが認証を試みるときに、タイムアウトになる可能性があります。

NIS 構成の詳細については、ネットワーク管理ガイドを参照してください。

システムの初期設定

有効な CIFS ライセンスがある場合、Data ONTAP はストレージ・システムの初期セットアップ中に、自動的に cifs setup コマンドを呼び出します。cifs setup コマンドは、認証タイプ、使用する検索サービス、などの情報についてプロンプトを表示します。

CIFS の初期構成における cifs setup コマンドの使用について、cifs setup を実行するときに必要な情報のリストを含めて確認するには、「Data ONTAP ソフトウェア・セットアップ・ガイド」を参照してください。

WINS サーバーの指定

WINS サーバーを指定するには、無停止の cifs.wins_servers オプション、または CIFS サービスを停止する必要がある cifs setup コマンドを使用することができます。

このタスクについて

注: WINS サーバー・リストは追加式ではありません。3 つ目の WINS サーバーを追加した場合は、コンマ区切りリストに 3 つすべての IP アドレスを入力する必要があります、あるいは既存の 2 つの WINS サーバーは追加するサーバーに置き換えられます。

以下を実施したい場合、	以下を実行してください。
cifs.wins_servers オプションを使用して WINS サーバーを指定する	コマンド <code>options cifs.wins_servers servers</code> を入力します。 <i>servers</i> は、コンマ区切りの WINS サーバーのリストです。 cifs.wins_servers オプションの詳細情報については、options(1) のマニュアル・ページを参照してください。
cifs setup コマンドを使用して WINS サーバーを指定する	コマンド <code>cifs setup</code> を入力します。次に、プロンプトが表示されたら最大 4 つまで IPv4 WINS サーバーを指定します。cifs setup コマンドの詳細情報については、cifs(1) のマニュアル・ページを参照してください。

ストレージ・システム・ドメインの変更

Windows ドメイン認証についてストレージ・システムを構成済みで、ストレージ・システムを他のドメインに移動させたい場合、`cifs setup` コマンドを実行します。

始める前に

この手順を実行するために、あらゆる Windows サーバーをドメインに追加する権限を持つ管理アカウントが必要です。

このタスクについて

ストレージ・システムのドメインを変更した後、Data ONTAP は `BUILTIN\Administrators` グループのメンバーシップを更新して新しいドメインに反映させます。この変更により、新規のドメインが古いドメインの信頼されたドメインではない場合でも、新規ドメインの管理者グループがストレージ・システムを確実に管理することができます。

注: 実際に CIFS サーバーを新規のドメインあるいはワークグループに置くまでは、CIFS セットアップ処理を取り消し、次に `Ctrl+C` を押して `cifs restart` コマンドを入力することで古い設定に戻すことが可能です。

1. CIFS が現在稼働している場合は、次のコマンドを入力します。`cifs terminate`
2. `cifs setup` コマンドを実行します。`cifs setup`

以下のプロンプトが表示されます。

Do you want to delete the existing filer account information? (既存のファイル・アカウント情報を削除しますか?) [no] (いいえ)

3. 既存のアカウント情報を削除するには、次を入力してください。`yes`

注: DNS サーバー・エントリーのプロンプトに進むためには、既存のアカウント情報を削除する必要があります。

アカウント情報を削除した後、ストレージ・システムの名前変更をすることが可能になります。

The default name of this filer will be 'filer1'. (このファイラーのデフォルトの名前は「filer1」です。)

Do you want to modify this name? (この名前を変更しますか?) [no]: (いいえ)

- 現在のストレージ・システムの名前を保持する場合は、Enter を押します。そうでない場合は、**yes** を入力し、新しいストレージ・システム名を入力します。

Data ONTAP は、認証方式のリストを表示します。

Data ONTAP CIFS services support four styles of user authentication. Choose the one from the list below that best suits your situation.

(1) Active Directory domain authentication (Active Directory domains only)

(2) Windows NT 4 domain authentication (Windows NT or Active Directory domains)

(3) Windows Workgroup authentication using the filer's local user accounts

(4) /etc/passwd and/or NIS/LDAP authentication

Selection (1-4)? [1]:

- ドメイン認証についてデフォルトの方式 (Active Directory) を選択する場合は、Enter を押してください。そうでない場合は、新規の認証方式を選択してください。
- 残りの `cifs setup` プロンプトに応答してください。デフォルトの値を承認する場合は、Enter を押してください。終了と同時に、`cifs setup` ユーティリティーは CIFS を開始します。
- 変更を確認するには、コマンド `cifs domaininfo` を入力します。Data ONTAP は、ストレージ・システムのドメイン情報を表示します。

プロトコル・モードの変更

有効な CIFS ライセンスおよび有効な NFS ライセンスがある場合、プロトコル設定を `unix` (デフォルト) から `ntfs` あるいは `mixed` (マルチプロトコル) モードに変更することができます。

このタスクについて

プロトコル・モードは、NFS、CIFS、あるいは両方のクライアントがストレージ・システム上のファイルにアクセス権を持っているかを判別します。

`cifs setup` ユーティリティーを実行するか、`wafl.default_security_style` オプションを設定することで、プロトコル・モードを設定することができます。

`cifs setup` を使用してマルチプロトコル・モードに変更した場合、ファイルはすぐには NFS クライアントに使用可能になりません。 `cifs setup` を使用してマルチプロトコル・モードに変更した後にファイルを NFS クライアントに使用可能にするた

めには、root ボリューム qtree のセキュリティ・スタイルを unix に変更する必要があります。そして次に、chmod コマンドを使用して UNIX クライアントに必要なアクセス権を許可します。

注: Data ONTAP がそのユーザーの UNIX ユーザー ID を CIFS 資格情報にマッピングするのに成功し、(CIFS 資格情報によって) ユーザーがファイルにアクセス可能であると確認した場合、NFS クライアントは Windows ACL によってもファイルへのアクセス権を取得することができます。例えば、Data ONTAP が UNIX root ユーザーを BUILTIN\Administrators グループのユーザーへのマッピングに成功した場合、UNIX root ユーザーはセキュリティ・スタイルに関わらず、Windows ユーザーがアクセスできるファイルと同じファイルにアクセスすることができます。

以下を実施したい場合、	以下を実行してください。
cifs setup ユーティリティーを使用したプロトコル・モードの変更	次のコマンドを入力します。cifs terminatecifs setup 次に、プロトコル・モードを変更するためのプロンプトに従います。
wafl.default_security_style オプションの設定によるプロトコル・モードの変更	次のコマンドを入力します。options wafl.default_security_style unix ntfs mixed

NTFS のみのストレージ・システムをマルチプロトコルのストレージ・システムに変更する効果

NTFS のみのストレージ・システムをマルチプロトコルのストレージ・システムに変更することは、いくつかの効果があります。

以下のような効果があります。

- ボリュームを作成する場合、デフォルトのセキュリティは **unix** です。
- wafl.default_security_style オプションは、**unix** に設定されています。

既存の ACL と、現行のボリュームおよび qtree のセキュリティ・スタイルは、変更なしで残ります。

注: ストレージ・システムをマルチプロトコルに変更した後も、ルート・ボリュームのセキュリティ・スタイルが ntfs のまま残るため、UNIX から root として接続した際にルート・ボリュームへのアクセスが拒否される可能性があります。root にマッピングされた Windows ユーザーに関して、ルート・ボリュームの ACL がフル・コントロールを許可すれば、アクセス権を取得できます。

cifs.nfs_root_ignore_acl オプションを on に設定することによっても、アクセス権を取得することができます。

マルチプロトコルのストレージ・システムを NTFS のみのストレージ・システムに変更する効果

マルチプロトコルのストレージ・システムを NTFS のみのストレージ・システムに変更することは、いくつかの効果があります。

以下のような効果があります。

- ストレージ・システムのルート・ディレクトリー (/etc) および /etc ディレクトリー内のファイルに既に ACL が存在している場合、ACL は変更なしで残ります。そうでない場合、これらの ACL は BUILTIN\Administrators グループがフル・コントロールを持つように作成されます。/etc/http ディレクトリー内にあるものはすべて「Everyone Read」に割り当てられます。
- 他のファイルおよびディレクトリーの ACL は変更なしで残ります。
- すべてのボリュームのセキュリティー・スタイルは、読み取り専用ボリュームを除いて、ntfs に変更されます。
- /etc ディレクトリーが qtree の場合、そのセキュリティー・スタイルは ntfs に変更されます。
- 他のすべての qtree に関するセキュリティー・スタイルは、変更なしで残ります。
- ボリュームまたは qtree を作成する場合、そのデフォルトのセキュリティー・スタイルは ntfs です。
- wapl.default_security_style オプションは ntfs に設定されています。

Windows ユーザー・アカウント名の指定

いくつかの Data ONTAP コマンドあるいは構成ファイルで、Windows ユーザー・アカウント名を指定することができます。

このタスクについて

以下の場所で Windows ユーザー・アカウント名を指定することができます。

- Windows ユーザーに関する情報を表示するための cifs sessions コマンドの引数として
- Windows 名を UNIX 名にマッピングするための /etc/usermap.cfg ファイル
- Windows ユーザーのための quota を設定するための /etc/quotas ファイル

構成ファイルで円記号 (¥) を含む UNIX 名を指定した場合、Data ONTAP はその名前を Windows ユーザー・アカウント名として扱います。例えば、/etc/quotas ファイルの corp¥john のような UNIX 名は、Windows ユーザー・アカウント名として解釈されます。

注: user@domain フォーマットを使用して Windows ユーザー・アカウント名を指定することができる唯一のコマンドは、cifs setup コマンドです。Windows ユーザー・アカウント名に関する、特定の構成ファイルに固有の規則もあります。これらの規則に関する追加情報については、このガイドの特定の構成ファイルに関するセクションを参照してください。

以下を実施したい場合、	以下を実行してください。
Windows 2000 より前のフォーマットで Windows 名を指定する	ドメイン名に円記号 (¥) とユーザー名を付加します。(例えば、corp¥john_smith)

以下を実施したい場合、	以下を実行してください。
Windows 2000 より前のフォーマットで Windows 2000 ユーザーの名前を指定する	NETBIOS 形式のドメイン名を使用し、ユーザー名が 20 文字を超えないことを確認します。例えば、 john_smith@engineering.my_company.com が Windows 2000 ユーザーで、このユーザーを engineering¥john_smith として Data ONTAP コマンドおよび構成ファイルで参照することができます。
ローカル・ユーザー・アカウントを指定する	ドメイン名を Windows 2000 より前のフォーマットでストレージ・システム名と置き換えます。(例えば、filer¥john_smith)

ストレージ・システム上での CIFS の再構成

初期セットアップの後で、もう一度 cifs setup ユーティリティを実行することで、CIFS を再構成することができます。

始める前に

CIFS を再構成する前に、セットアップに適切な必須の手順がすべて完了していることを確認してください。

- ストレージ・システムの再構成時に、ストレージ・システムのドメインを Windows NT ドメインから他のドメインに変更したい場合、ストレージ・システムをインストールしたいドメインのプライマリー・ドメイン・コントローラーとストレージ・システムが、通信をできるようにする必要があります。

ストレージ・システムのインストールには、バックアップ・ドメイン・コントローラーは使用できません。

- ストレージ・システムの名前を変更したい場合は、ドメイン・コントローラーに新規のコンピューター・アカウントを作成する必要があります。

(Windows 2000 の後の Windows のバージョンにのみ必要。)

- 同じドメイン内のストレージ・システムとドメイン・コントローラーは、同じ時間ソースで同期される必要があります。ストレージ・システム上の時間とドメイン・コントローラー上の時間が同期されていない場合、以下のエラー・メッセージが表示されます。

Clock skew too great

時間の同期サービスのセットアップ方法の詳細な手順については、「*Data ONTAP System Administration Guide*」を参照してください。

このタスクについて

cifs setup の実行によって変更可能な CIFS 構成の設定は、以下のとおりです。

- WINS サーバー・アドレス
- ストレージ・システムがマルチプロトコルか NTFS のみか

- ストレージ・システムが Windows ドメイン認証、Windows ワークグループ認証、あるいは UNIX パスワード認証を使用しているか
- ストレージ・システムが属するドメインあるいはワークグループ
- ストレージ・システム名

注: 進行中に `cifs setup` ユーティリティーを終了したい場合は、`Ctrl-C` を押します。次に、`cifs restart` コマンドを入力して、古い構成情報を使用して CIFS を再始動します。

1. コマンド `cifs terminate` を入力します。ストレージ・システムに対する CIFS サービスが停止します。
2. コマンド `cifs setup` を入力します。Data ONTAP は、CIFS を再構成するためのプロンプトのリストを表示する `cifs setup` プログラムを実行します。

ストレージ・システム上での SMB の構成

CIFS プロトコルに加えて、Data ONTAP はオリジナルの Server Message Block (SMB) プロトコルおよび SMB 2.0 プロトコルをサポートします。

オリジナルの SMB プロトコルのサポート

Data ONTAP は、オリジナルの SMB プロトコルをサポートします。このプロトコルは、CIFS をセキュリティ、ファイル、およびディスク管理の機能について拡張します。

Microsoft SMB プロトコルの仕様書によると、オリジナルの SMB プロトコルは以下の機能を含みます。

- Kerberos 認証を含む、新規の認証方式
- メッセージの署名
- 以前のバージョンのファイルの列挙およびそれらのファイルへのアクセス
- サーバーからの全データの読み取りあるいは書き戻しの必要なしでの、クライアントによるサーバー上のファイルの管理
- SMB トランスポートに、(NetBIOS over TCP/UDP に代わる) ダイレクト TCP、NetBIOS over Internetwork Packet Exchange (IPX)、NetBIOS 拡張ユーザー・インターフェース (NetBEUI) を使用する SMB 接続
- サーバーによって公開されたファイル・システム操作を要求するための、ファイル・システム・コントロール (FSCTL) のクライアント使用のサポート
- 存在するコマンドへの応答における拡張情報取得のサポート

詳細情報については、Microsoft SMB プロトコルの仕様書を参照してください。

SMB 2.0 プロトコルのサポート

オリジナルの SMB プロトコルのサポートに加えて、Data ONTAP はいくつかの機能拡張を提供する SMB 2.0 プロトコルをサポートします。

SMB 2.0 プロトコルは、完全に異なるパケット・フォーマットを使用する、オリジナルの SMB プロトコルのメジャー・リビジョンです。ただし、クライアントが SMB 2.0 プロトコルの使用を交渉するためにオリジナルの SMB プロトコルを使用

する可能性があるため、オリジナルの SMB プロトコル を使用しているサーバーおよびクライアントとの互換性は維持しています。

Microsoft SMB 2.0 プロトコルの仕様書によると、SMB 2.0 は以下の機能を組み込んでいます。

- 「クライアント接続が一時的に切断された後に復旧されるファイルへのオープン」を許可します。

オープンとは、「特定のユーザーのセキュリティ・コンテキストを使用した特定のクライアントから特定のサーバーに対する、特定のファイルあるいは名前付きパイプへの、現在確立されているアクセスに対応するランタイム・オブジェクト」です。クライアントとサーバーの両方がアクティブなアクセスを示すオープンを維持します。

- 「サーバーが、クライアントが常に持つ可能性がある未解決の同時操作の数のバランスを取ること」を許可します。
- 「共有、ユーザー、および同時オープン・ファイルの数に関するスケーラビリティ」を提供します。

特に、Data ONTAP は以下の SMB 2.0 機能をサポートします。

- 非同期メッセージング

Data ONTAP は非同期メッセージを使用して、SMB 2.0 クライアントに要求に関する暫定の応答を送信します。この要求はフル応答を無期限にブロックする可能性があるもので、以下のようなものがあります。

- CHANGE_NOTIFY 要求
- oplock 取り消しによってブロックされた CREATE 要求
- 既にロックされたバイト範囲にある LOCK 要求

- 永続的ハンドル

Data ONTAP は、永続的ハンドルを使用します。これは、短時間のネットワーク障害の発生からデータ損失を防ぐために、SMB 2.0 セッションが終了しても持続するファイル・ハンドルです。クライアントがファイルを開く場合、永続的ハンドルが必要かどうかを指定します。必要な場合、Data ONTAP は永続的ハンドルを作成します。次に、SMB 2.0 接続がダウンすると、Data ONTAP は別の SMB 2.0 接続上の同じユーザーによるレクラメーション処理のために、永続的ハンドルを有効にします。Data ONTAP の永続的ハンドルのサポートを、有効あるいは無効に設定することができます。また、ネットワーク障害の後、どれぐらいの期間 Data ONTAP が永続的ハンドルを保持するかを指定することも可能です。

- SHA-256 署名

Data ONTAP は、SMB 2.0 メッセージの署名のためにメッセージ認証コード (MAC) を作成するために、SHA-256 ハッシュ関数を使用します。SMB 2.0 署名を有効にする場合、Data ONTAP は有効な署名をもっている場合のみ SMB 2.0 メッセージを承認します。

- クレジット認可のアルゴリズム

Microsoft SMB 2.0 プロトコルの仕様書によると、「クレジットは、クライアントがサーバーに送信することができる未解決の要求の数を制限する」および「クライアントが、ストレージ・システムに複数の同時要求を送信することを許可することができる」と示されています。

- 複合要求

Microsoft SMB 2.0 プロトコルの仕様書によると、複合要求は、「基礎となるトランスポートへの処理依頼を行うための、単一の伝送要求へ複数の SMB 2.0 プロトコル要求を結合する方式」です。

さらに、ストレージ・システムの SMB 2.0 プロトコル・クライアントの機能を有効または無効に設定することができます。これは、ストレージ・システムが Windows サーバーとの通信に SMB 2.0 プロトコル を使用するか、SMB プロトコルを使用するかを判別します。

注: Data ONTAP は、SMB 2.0 プロトコルのオプション機能であるシンボリック・リンクをサポートしません。

詳細情報については、Microsoft SMB 2.0 プロトコルの仕様書を参照してください。

コンテキスト作成のサポート

Data ONTAP は、Microsoft SMB 2.0 プロトコルの仕様書で定義されたコンテキスト作成のサブセットをサポートします。

Data ONTAP は、以下のコンテキスト作成をサポートします。

- SMB2_CREATE_EA_BUFFER
- SMB2_CREATE_SD_BUFFER
- SMB2_CREATE_QUERY_MAXIMAL_ACCESS
- SMB2_CREATE_TIMEWARP_TOKEN
- SMB2_CREATE_DURABLE_HANDLE_REQUEST
- SMB2_CREATE_DURABLE_HANDLE_RECONNECT

Data ONTAP は、以下のコンテキスト作成をサポートしません。これらは既知のコース・ケースがありません。

- SMB2_CREATE_ALLOCATION_SIZE
- SMB2_CREATE_QUERY_ON_DISK_ID

ファイル・システム・コントロールのサポート

Data ONTAP は、Microsoft SMB 2.0 プロトコルの仕様書で定義されたファイル・システム・コントロール (FSCTL) のサブセットをサポートします。

Data ONTAP は、以下のファイル・システム・コントロールをサポートします。

- FSCTL_PIPE_TRANSCEIVE
- FSCTL_PIPE_PEEK
- FSCTL_GET_DFS_REFERRALS
- FSCTL_SRV_ENUMERATE_SNAPSHOTS

Data ONTAP は、以下のファイル・システム・コントロールをサポートしません。
これらは既知のユース・ケースがありません。

- FSCTL_SRV_REQUEST_RESUME_KEY
- FSCTL_SRV_COPYCHUNK

SMB 2.0 プロトコルの有効化

オリジナルの SMB プロトコルより SMB 2.0 プロトコルに適したファイル転送およびプロセス間通信のシナリオがいくつかあります。

Microsoft SMB 2.0 プロトコルの仕様書によると、このようなシナリオは以下の要件を組み込んでいます。

- 同時ファイル・オープン、共有の数、およびユーザー・セッションの数に関する、さらなるスケーラビリティ
- サーバーに対する未解決の要求の数に関する、サービス保証の質
- HMAC-SHA256 ハッシュ・アルゴリズムを使用した、より強固なデータ完全性の保護
- 非同質特性によるネットワーク全域でのスループットの向上
- 偶発的なネットワーク接続の失敗に対する、処理の改善

詳細情報については、Microsoft SMB 2.0 プロトコルの仕様書を参照してください。

SMB 2.0 プロトコルの有効化あるいは無効化

cifs.smb2.enable オプションを on あるいは off に設定することで、SMB 2.0 プロトコルをそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは off に設定されています。

このタスクについて

ストレージ・システムで SMB 2.0 プロトコルが無効に設定されている場合、SMB 2.0 クライアントとストレージ・システムの通信はオリジナルの SMB プロトコルにフォールバックします (SMB 2.0 クライアントはネゴシエーション要求にオリジナルの SMB ダイアレクトを含んでいると仮定しています)。

以下を SMB 2.0 プロトコルに実施したい場合、	以下を実行してください。
有効	次のコマンドを入力します。options cifs.smb2.enable on
無効	次のコマンドを入力します。options cifs.smb2.enable off

SMB 2.0 の永続的ハンドルの有効化あるいは無効化

cifs.smb2.durable_handle.enable オプションを on あるいは off に設定することで、SMB 2.0 の永続的ハンドルをそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは on に設定されています。

以下を実施したい場合、	以下を実行してください。
SMB 2.0 永続的ハンドルを有効にする	次のコマンドを入力します。options cifs.smb2.durable_handle.enable on
SMB 2.0 永続的ハンドルを無効にする	次のコマンドを入力します。options cifs.smb2.durable_handle.enable off

SMB 2.0 の永続的ハンドルのタイムアウト値の指定

cifs.smb2.durable_handle.timeout オプションを設定することで、SMB 2.0 の永続的ハンドルのタイムアウト値を指定することができます。デフォルトでは、このオプションは 960 秒 (16 分) です。

コマンド options cifs.smb2.durable_handle.timeout *value* を入力します。ここで、*value* は秒単位でのタイムアウト値で、5 秒から 4,294,967,295 秒の間です。

SMB 署名

Data ONTAP は、クライアントから要求された場合、SMB 署名を (オリジナルの SMB プロトコルおよび SMB 2.0 プロトコルで) サポートします。SMB 署名は、ストレージ・システムとクライアントの間のネットワーク・トラフィックが暗号漏えいしていないことを確実にします。これは、リプレイ・アタック (「中間者攻撃」としても知られています) を防ぐことによって実現されます。

ストレージ・システム上で SMB 署名が有効になっている場合、Microsoft ネットワーク・サーバー・ポリシーの「デジタル署名通信 (if client agrees)」と同等です。クライアントからの SMB 署名通信を要求するようにストレージ・システムを構成することはできません。それは、Microsoft ネットワーク・サーバー・ポリシーの「デジタル署名通信 (always)」と同等です。パフォーマンス上の理由から、SMB 署名はストレージ・システムでデフォルトでは無効に設定されています。

クライアント SMB の署名ポリシーがストレージ・システムとの通信に与える影響

Windows クライアントには、クライアントとストレージ・システム間の通信のデジタル署名をコントロールする 2 つの SMB 署名ポリシー (「always」および「if server agrees」) があります。

クライアント SMB ポリシーは、Microsoft 管理コンソール (MMC) を使用したセキュリティ設定によってコントロールされます。クライアント SMB 署名およびセキュリティ問題に関する詳細は、Microsoft Windows の資料を参照してください。

以下は、Microsoft ネットワーク・クライアントにおける 2 つの SMB 署名ポリシーに関する説明です。

- 「デジタル署名通信 (if server agrees)」: この設定は、クライアントの SMB 署名機能が有効かどうかをコントロールします。デフォルトでは有効になっています。この設定がクライアントで無効になっている場合、クライアントはストレージ・システムの SMB 署名設定に関わらず、SMB 署名なしでストレージ・システムと正常に通信します。この設定がクライアントで有効になっている場合、クライアントとストレージ・システム間の通信は以下のように進みます。

- ストレージ・システムで SMB 署名が有効になっている場合、クライアントとストレージ・システム間のすべての通信は SMB 署名を使用します。
- ストレージ・システムで SMB 署名が有効になっていない場合、通信は SMB 署名なしで正常に進みます。
- 「デジタル署名通信 (always)」: この設定は、サーバーとの通信にクライアントが SMB 署名を要求するかどうかをコントロールします。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB 署名の動作は「デジタル署名通信 (if server agrees)」のポリシー設定およびストレージ・システムの設定に基づきます。この設定がクライアントで有効になっている場合、クライアントとストレージ・システム間の通信は以下のように進みます。
 - ストレージ・システムで SMB 署名が有効になっている場合、クライアントとストレージ・システム間のすべての通信は SMB 署名を使用します。
 - ストレージ・システムで SMB 署名が有効になっていない場合、クライアントはストレージ・システムとの通信を拒否します。

注: ご使用の環境が SMB 署名を要求する Windows クライアント構成を含む場合、ストレージ・システムで SMB 署名を有効にする必要があります。そうしない場合、ストレージ・システムはこれらのシステムにデータを供給できません。

SMB 署名のパフォーマンスへの影響

SMB 署名が有効な場合、Windows クライアントとの CIFS の通信に大きなパフォーマンスの影響があります。これは、クライアントとサーバー (Data ONTAP が稼働しているストレージ・システム) の両方に影響します。

パフォーマンスの低下は、ネットワーク・トラフィック量に変化していないにも関わらず、クライアントとサーバーの両方で CPU 使用率の増加として示されます。

ネットワークおよびストレージ・システムの実装環境に応じて、SMB 署名のパフォーマンスへの影響は大きく異なります。これはご使用のネットワーク環境でテストするだけで検証することが可能です。

ほとんどの Windows クライアントは、サーバー上で有効になっている場合、デフォルトで SMB 署名を交渉します。いくつかの Windows クライアントについて SMB 保護を要求し、SMB 署名がパフォーマンス問題の原因となった場合、リプレイ・アタックからの保護が要求されない Windows クライアントでの SMB 署名を無効にすることができます。Windows クライアント上での SMB 署名の無効化については、Microsoft Windows 資料を参照してください。

オリジナルの SMB プロトコル署名の有効化あるいは無効化

cifs.signing.enable オプションを on あるいは off に設定することで、オリジナルの SMB プロトコル署名をそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは off に設定されています。

以下を実施したい場合、	以下を実行してください。
オリジナルの SMB プロトコル署名を有効にする	次のコマンドを入力します。options cifs.signing.enable on
オリジナルの SMB プロトコル署名を無効にする	次のコマンドを入力します。options cifs.signing.enable off

クライアントが SMB 2.0 メッセージに署名する要件の有効化あるいは無効化

cifs.smb2.signing.required オプションを on あるいは off に設定することで、クライアントが SMB 2.0 メッセージに署名する要件をそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは off に設定されています。

このタスクについて

Data ONTAP は、SMB 2.0 メッセージの署名のためのメッセージ認証コード (MAC) を作成するために、SHA-256 ハッシュ関数を使用します。

cifs.smb2.signing.required オプションを on に設定する場合、Data ONTAP は、有効な署名を持っている場合にのみ SMB 2.0 を承認します。

以下を実施したい場合、	以下を実行してください。
クライアントが SMB 2.0 に署名する要件を有効にする	次のコマンドを入力します。options cifs.smb2.signing.required on
クライアントが SMB 2.0 に署名する要件を無効にする	次のコマンドを入力します。options cifs.signing.enable off

ストレージ・システムの SMB 2.0 プロトコル・クライアント機能の有効化あるいは無効化

cifs.smb2.client.enable オプションを on あるいは off に設定することで、ストレージ・システムの SMB 2.0 プロトコル・クライアント機能をそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは off に設定されています。

このタスクについて

cifs.smb2.client.enable オプションが on に設定されているが、Windows サーバーが SMB 2.0 プロトコルをサポートしない場合、ストレージ・システムは Windows サーバーとの通信にオリジナルの SMB プロトコルを使用します。

cifs.smb2.client.enable オプションを off に設定する場合、ストレージ・システムは Windows サーバーとの新規の通信セッションではオリジナルの SMB プロトコルを使用しますが、既存のセッションでは引き続き SMB 2.0 プロトコルを使用します。

以下を実施したい場合、	以下を実行してください。
ストレージ・システムの SMB 2.0 プロトコル・クライアント機能を有効にする	次のコマンドを入力します。options cifs.smb2.client.enable on
ストレージ・システムの SMB 2.0 プロトコル・クライアント機能を無効にする	次のコマンドを入力します。options cifs.smb2.client.enable off

共有の管理

管理者として、ストレージ・システム上のユーザーとディレクトリーを共有することができます (「共有」の作成)。

共有の作成

Windows クライアント上の Microsoft 管理コンソール (MMC) または Data ONTAP コマンド行から、共有を作成する (フォルダー、qtree、あるいはボリュームを CIFS ユーザーによるアクセスのために指定する) ことができます。

始める前に

共有を作成するときに、以下のすべての情報を提供する必要があります。

- 共有する既存のフォルダー、qtree、あるいはボリュームの完全パス名
- 共有への接続時にユーザーが入力する共有名
- 共有のためのアクセス権

注: 各ユーザーあるいはユーザーのグループについて、アクセス権のリストから選択するか、あるいは特定のアクセス権を指定することができます。

共有を作成するときに、オプションで共有の説明を指定することができます。共有の説明は、ネットワーク上の共有を表示するときにコメント欄に表示されます。

Data ONTAP コマンド行から共有を作成する場合は、以下の共有プロパティを指定することもできます。

- 共有内のファイルのためのグループ・メンバーシップ
- CIFS クライアントが、共有内で同じストレージ・システム上の宛先へのシンボリック・リンクに従うか
- 共有内でのワイド・シンボリック・リンクのサポート
- 共有のための **umask** 値
- 共有が表示可能か
- 共有内のファイルが開かれたときのウィルス・スキャンの無効化
- Windows クライアントによる共有におけるファイル・キャッシングの無効化
- Windows クライアントによる共有内の文書あるいはプログラムの自動キャッシングのサポート
- Windows Access-based Enumeration (ABE) を使用した共有リソースの表示のコントロール

注: 共有作成後に、これらのプロパティをいつでも変更することができます。

次のタスク

共有を作成した後、以下のプロパティを指定します。

- 共有に同時アクセス可能な最大ユーザー数

注: ユーザー数を指定しない場合、ストレージ・システム・メモリーが残っていない場合にのみ追加ユーザーがブロックされます。

- 共有レベル ACL

共有名の規則

Data ONTAP に関する共有名の規則は、Windows と同じです。

例えば、\$ 文字で終了する共有名は非表示共有で、ADMIN\$ および IPC\$ のような特定の共有名が予約されています。

共有名は大/小文字の区別をしません。

Windows クライアントの MMC からの共有の作成

MMC をストレージ・システムに接続し、「共有フォルダ」ウィザードを実行することで、Windows クライアントの MMC から共有を作成することができます。

ストレージ・システムへの MMC の接続:

MMC メニュー・コマンドを使用して、MMC をストレージ・システムに接続することができます。

1. Windows サーバーで、MMC に移動します。例えば、「スタート」メニューで「ファイル名を指定して実行」を選択し、次のコマンドを入力します。`mmc`
2. 左側のペインで、「コンピュータの管理」を選択します。
3. 「操作」メニューから「別のコンピュータへ接続」を選択します。「別のコンピュータ」ボックスが表示されます。
4. ストレージ・システムの名前を入力するか、あるいは「参照」をクリックしてストレージ・システムを参照してください。
5. 「OK」をクリックします。

「共有フォルダ」ウィザードの実行:

MMC を使用して、「共有フォルダ」ウィザードを実行することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」>「共有」>「操作」を選択してください。これらのメニュー項目の単語は、ご使用の Windows のバージョンによって少し異なる場合があります。
4. 「新しいファイルの共有 (New Share)」をダブルクリックします。
5. 「共有フォルダ」ウィザードの指示に従ってください。

Data ONTAP コマンド行からの共有の作成

Data ONTAP コマンド行から `cifs shares` コマンドを使用して、共有を作成することができます。

次のコマンドを入力します。`cifs shares -add shareName path [-comment description] [-userlimit] [-browse | -nobrowse] [-forcegroup groupname] [-widelink] [-nosymlink_strict_security] [-novscan] [-novscanread] [-umask mask] [-no_caching | -auto_document_caching | -auto_program_caching]`
引数がスペースを含んでいる場合は、二重引用符で囲ってください。

パス分離文字として、バックスラッシュまたはスラッシュが使用できますが、Data ONTAP はどちらもスラッシュとして表示します。

詳細情報については、`na_cifs_shares(1)` のマニュアル・ページを参照してください。

タスクの結果

例: 共有 webpages の作成

Web でアクセス可能な共有 (共有 *webpages*) を、最大 100 ユーザーを持ち、CIFS ユーザーが作成したすべてのファイルをすべてのユーザーが所有している /vol/vol1/companyinfo ディレクトリーに作成するには、次のコマンドを入力します。

```
cifs shares -add webpages /vol/vol1/companyinfo -comment "Product Information" -forcegroup webgroup1 -maxusers 100
```

forcegroup オプションについて:

Data ONTAP コマンド行から共有を作成する際に、その共有内で CIFS ユーザーによって作成されたすべてのファイルが同一のグループ (これを「forcegroup」という) に属することを指定するために、forcegroup オプションを使用することができます。このグループは UNIX グループ・データベースで事前定義されたグループでなければなりません。

forcegroup の指定は、共有が UNIX または 混合 qtree にある場合にのみ意味があります。NTFS qtree 内の共有に forcegroup を使用する必要はありません。なぜなら、これらの共有内のファイルへのアクセスは、GID ではなく Windows のアクセス許可によって決定されるからです。

forcegroup が共有に関して指定されている場合は、共有について以下のことが当てはまります。

- この共有にアクセスする forcegroup 内の CIFS ユーザーは、一時的に forcegroup の GID に変更されます。

この GID は、それらのユーザーがプライマリーの GID や UID では通常アクセスすることができないこの共有内のファイルにアクセスすることを可能にします。

- CIFS ユーザーによって作成されたこの共有内のすべてのファイルは、ファイル所有者のプライマリーの GID に関わらず、同一の forcegroup に属します。

CIFS ユーザーが、NFS によって作成されたファイルにアクセスを試みる場合は、CIFS ユーザーのプライマリー GID がアクセス権を決定します。

forcegroup は、NFS ユーザーがこの共有内のファイルにアクセスする方法には影響しません。NFS によって作成されたファイルは、ファイル所有者から GID を獲得します。アクセス許可の決定は、ファイルへのアクセスを試みる NFS ユーザーの UID およびプライマリーの GID に基づきます。

forcegroup を使用することで、様々なグループに属する CIFS ユーザーがファイルに確実にアクセスすることが容易になります。例えば、企業の Web ページを保管する共有を作成し、Engineering および Marketing グループのユーザーに書き込み権限を与えたい場合、共有を作成して「webgroup1」と名付けた forcegroup に書き込み権限を与えることで実現できます。forcegroupのおかげで、この共有内の CIFS ユーザーによって作成されたすべてのファイルは、web グループの所有となります。さらに、ユーザーは共有にアクセスする際に自動的に web グループの GID が

割り当てられます。その結果、Engineering および Marketing グループのアクセス権を管理することなく、すべてのユーザーがこの共有に書き込むことが可能になります。

共有プロパティの表示および変更

MMC から、あるいは Data ONTAP のコマンド行で、共有プロパティを表示あるいは変更することができます。

このタスクについて

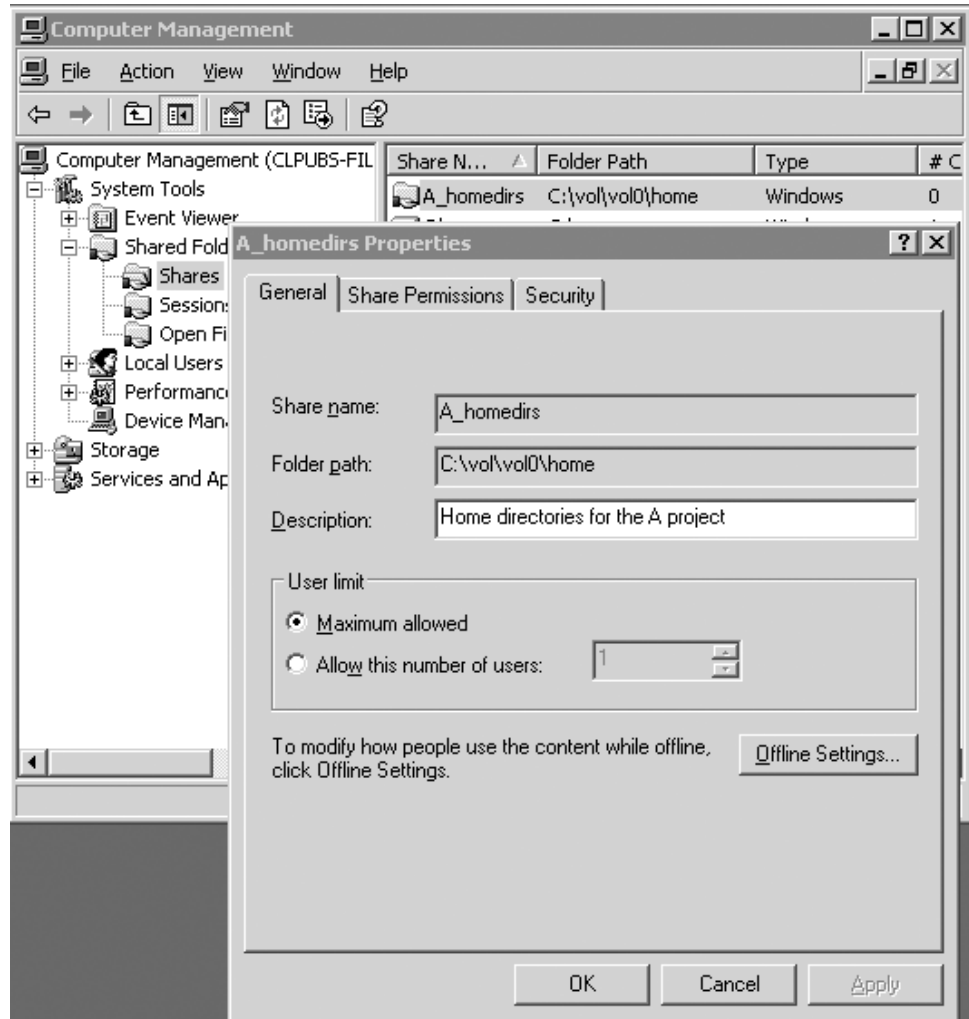
以下の共有プロパティを変更することができます。

- 共有の説明
- 共有に同時アクセス可能な最大ユーザー数
- 共有レベル・アクセス権
- Access-based Enumeration の有効または無効

Windows クライアントの MMC からの共有プロパティの表示および変更

Windows クライアントの MMC から共有プロパティを表示および変更することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」を選択してください。
4. 「共有」をダブルクリックします。
5. 右側のペインで、共有を右クリックします。
6. 「プロパティ」を選択します。選択した共有のプロパティが以下の例に示されているように表示されます。



7. 「共有のアクセス許可」タブを選択します。共有の ACL が表示されます。
8. 共有の ACL を追加グループあるいはユーザーを含むように変更するには、「名前」ボックスからグループあるいはユーザーを選択します。
9. 「アクセス許可」ボックスでアクセス権を変更します。

Data ONTAP コマンド行からの共有プロパティの表示

共有プロパティを、Data ONTAP コマンド行から `cifs shares` コマンドを使用して表示することができます。

このタスクについて

コマンド `cifs shares sharename` を入力します。*sharename* は、単一の共有名です。*sharename* を省略した場合、すべての共有のプロパティが表示されます。

タスクの結果

Data ONTAP は、共有名、共有されているディレクトリーのパス名、共有の説明、および共有レベル ACL を表示します。

Data ONTAP コマンド行からの共有プロパティの変更

共有プロパティを、Data ONTAP コマンド行から `cifs shares` コマンドを使用して変更することができます。

次のコマンドを入力してください。 `cifs shares -change sharename {-browse | -nobrowse} {-comment desc | -nocomment} {-maxusers userlimit | -nomaxusers} {-forcegroup groupname | -noforcegroup} {-widelink | -nowidelink} {-symlink_strict_security | -nosymlink_strict_security} {-vscan | -novscan} {-vscanread | -novscanread} {-umask mask | -noumask} {-no_caching | -manual_caching | -auto_document_caching | -auto_program_caching}`
詳細情報については、`na_cifs_shares(1)` のマニュアル・ページを参照してください。

注: 疑問符 (?) およびアスタリスク文字をワイルドカードを `sharename` で使用して、複数の共有のプロパティを同時に変更することが可能です。例えば、クライアントがいずれかの共有で開いているあらゆるファイルのウィルス・スキャンを無効にするには、次のコマンドを入力します。 `cifs shares -change * -novscan`

`-nocomment`、`-nomaxusers`、`-noforcegroup`、および `-noumask` の指定は、それぞれ、共有の説明、ユーザーの最大数、`forcegroup`、および `umask` 値を消去します。

共有からのシンボリック・リンクの境界チェックの有効化あるいは無効化:

CIFS クライアントが同じストレージ・システム上のあらゆる場所の宛先への、その共有内にあるシンボリック・リンクに従うことを許可するために、共有からのシンボリック・リンクの境界チェックを無効にすることができます。

このタスクについて

デフォルトでは、シンボリック・リンクの境界チェックは、ユーザーが共有の外部にあるファイルにアクセスすることを防ぐために、有効に設定されています。

境界チェックが無効に設定されている場合、ストレージ・システムはシンボリック・リンクを持つ共有の共有許可のみをチェックします。

共有からのシンボリック・リンクの境界チェックを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
共有からのシンボリック・リンクの境界チェックを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -nosymlink_strict_security</code>
共有からのシンボリック・リンクの境界チェックを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -symlink_strict_security</code>

共有からのワイド・シンボリック・リンクの有効化あるいは無効化:

共有あるいはストレージ・システムの外部の宛先への絶対シンボリック・リンクに従うように CIFS クライアントを許可したい場合、共有からのワイド・シンボリック・リンクを有効にすることができます。デフォルトでは、この機能は無効に設定されています。

共有からのワイド・シンボリック・リンクを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
共有からのワイド・シンボリック・リンクを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -widelink</code>
共有からのワイド・シンボリック・リンクを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -nowidelink</code>

タスクの結果

注: 共有の作成時に `widelink` オプションを指定することでも、共有からのワイド・シンボリック・リンクを有効にすることができます。

次のタスク

共有からのワイド・シンボリック・リンクを有効に設定した後、各ワイド・シンボリック・リンクが示す宛先をストレージ・システムがどのように判別するかを指定するために、`/etc/symlink.translations` ファイルに `Widelink` エントリーを作成する必要があります。

共有に新規に作成されたファイルおよびディレクトリーのためのアクセス権の指定:

共有の `umask` オプションを設定することで、混合あるいは UNIX `qtree` セキュリティー・スタイルを持つ共有に新規に作成したファイルおよびディレクトリーのアクセス権を指定することができます。

このタスクについて

共有の `umask` オプションを 8 進数 の値で指定する必要があります。デフォルトの `umask` の値は 0 です。

注: 共有の `umask` オプションの値は NFS には影響しません。

共有に新規に作成されたディレクトリー、ファイル、あるいはその両方のアクセス権を指定します。

以下を実施したい場合、	以下を実行してください。
新規に作成されたファイルおよびディレクトリーのアクセス権を指定する	Data ONTAP コマンド行で、コマンド <code>cifs shares -change sharename -umask mask</code> を入力します。 <code>mask</code> は、新規に作成されたファイルおよびディレクトリーのデフォルトのアクセス権を指定する 8 進数の値です。あるいは、共有の作成時に <code>umask</code> オプションを設定します。

以下を実施したい場合、	以下を実行してください。
新規に作成されたファイル (共有の umask オプションの値をオーバーライド) のアクセス権を指定する	Data ONTAP のコマンド行で、コマンド <code>cifs shares -change sharename -file_umask mask</code> を入力します。 <i>mask</i> は、新規に作成されたファイルのデフォルトのアクセス権を指定する 8 進数の値で、 umask 共有オプションの値をオーバーライドします。あるいは、共有の作成時に <code>file_mask</code> オプションを設定します。
新規に作成されたディレクトリー (共有の umask オプションの値をオーバーライド) のアクセス権を指定する	Data ONTAP のコマンド行で、コマンド <code>cifs shares -change sharename -dir_umask mask</code> を入力します。 <i>mask</i> は、新規に作成されたディレクトリーのデフォルトのアクセス権を指定する 8 進数の値で、 umask 共有オプションの値をオーバーライドします。あるいは、共有の作成時に <code>dir_mask</code> オプションを設定します。

例

共有にファイルを作成するときに、「group」および「other」のアクセス権について書き込み権限をオフにするには、次のコマンドを入力します。

```
dir_umask 022
```

ブラウズの有効化あるいは無効化:

ブラウズを有効あるいは無効にして、ユーザーが特定の共有を見ることを許可あるいは防止することができます。

特定の共有あるいはすべての共有で、ブラウズを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
特定の共有でブラウズを有効にする (<code>cifs.enable_share_browsing</code> オプションがオンの場合は影響はありません)	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -browse</code>
特定の共有でブラウズを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -nobrowse</code>
すべての共有でブラウズを有効にする (ブラウズを有効にしたい各共有で <code>-browse</code> オプションを有効にする必要があります)	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>options cifs.enable_share_browsing on</code>
すべての共有でブラウズを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>options cifs.enable_share_browsing off</code>

次のタスク

詳細情報については、na_options(1) のマニュアル・ページを参照してください。

ウィルス・スキャンの有効化あるいは無効化:

1 つ以上の共有でセキュリティあるいはパフォーマンスを向上させるために、ウィルス・スキャンをそれぞれ有効あるいは無効にすることができます。

このタスクについて

デフォルトでは、Data ONTAP はクライアントが開いたあらゆるファイルをウィルス・スキャンします。

クライアントが開いたすべてのファイルあるいは読み取り専用ファイルのウィルス・スキャンを有効または無効にします。

以下を実施したい場合、	以下を実行してください。
クライアントが開いたすべてのファイルのウィルス・スキャンを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -vscan</code>
クライアントが開いたすべてのファイルのウィルス・スキャンを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -novscan</code>
クライアントが開いた読み取り専用ファイルのウィルス・スキャンを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -vscanread</code>
クライアントが開いた読み取り専用ファイルのウィルス・スキャンを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -vscanread</code>

タスクの結果

注: -novscan あるいは -novscanread オプションを指定して共有を作成した場合、共有に関するウィルス・スキャンも無効にすることができます。

次のタスク

CIFS 共有のウィルス・スキャンの指定に関する詳細情報については、「*Data ONTAP データ保護バックアップとリカバリーのガイド*」を参照してください。

キャッシングの有効化あるいは無効化:

キャッシングを有効あるいは無効にして、クライアントが共有上のファイルをキャッシングすることを許可あるいは防止することができます。

このタスクについて

クライアントがキャッシングするファイルを手動で選択する必要があるかを指定することができます。また、手動で選択しない場合、Data ONTAP がクライアントの設定に従ってプログラム、ユーザー・ファイル、あるいはその両方を自動的にキャッシングするかどうかを指定することができます。デフォルトでは、クライアント

は手動でキャッシングするファイルを指定する必要があります。

キャッシングを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
キャッシングを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -nocaching</code>
手動キャッシングを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -manual_caching</code>
文書の自動キャッシングを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -auto_document_caching</code>
プログラムの自動キャッシングを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。 <code>cifs shares -change sharename -auto_program_caching</code>

タスクの結果

注: 共有を作成するときに、デフォルトのキャッシング・オプション (-manual_caching) を、-nocaching、-auto_document_caching、あるいは -auto_program_caching オプションを指定することでオーバーライドすることができます。

共有のためのクライアント・サイドのキャッシング・プロパティの設定:

Windows 2000、XP、および 2003 クライアントでコンピューター管理アプリケーションを使用している共有のための、クライアント・サイドのキャッシング・プロパティを設定することができます。詳細情報については、Microsoft Windows のオンライン・ヘルプ・システムを参照してください。

Access-based Enumeration の有効化あるいは無効化:

アクセス権を持たない共有リソースをユーザーが見ることを許可あるいは阻止するために、Access-based Enumeration (ABE) を有効あるいは無効に設定することができます。

このタスクについて

デフォルトでは、ABE は無効に設定されています。

ABE を有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
ABE を有効にする	Data ONTAP コマンド行で、次のコマンドを入力してください。 <code>cifs shares -change sharename -accessbasedenum</code>
ABE を無効にする	Data ONTAP コマンド行で、次のコマンドを入力してください。 <code>cifs shares -change sharename -noaccessbasedenum</code>

注: -accessbasedenum オプションを指定して共有を作成した場合も、ABE を有効にすることができます。

***Access-based Enumeration* について:**

Access-based Enumeration (ABE) が CIFS 共有で有効にされている場合は、共有フォルダーあるいは共有フォルダー内のファイルにアクセス権を持たないユーザーは、個人のアクセス権の制限であってもグループのアクセス権の制限であっても、そのユーザーの環境で表示された共有リソースを見ることはできません。

標準的な共有プロパティによって、どのユーザー (個人あるいはグループ) が共有リソースを表示または変更する権限を持つかを指定することが可能です。しかしながら、それらの共有プロパティでは、共有フォルダーあるいは共有ファイルがアクセス権を持たないユーザーに表示されるかをコントロールすることはできません。このことによって、共有フォルダーや共有ファイルの名前が機密情報 (お客様や開発中の製品の名前など) を示している場合に、問題を引き起こす可能性があります。

Access-based Enumeration (ABE) は、共有プロパティを共有リソースの列挙を含むところまで拡張します。そのため、ABE はユーザーのアクセス権に基づいた共有リソースの表示のフィルタリングを可能にします。ワークスペースにおける機密情報の保護に加えて、ABE はコンテンツの全範囲にアクセスする必要が無いユーザーについては、大規模なディレクトリー構造の表示を単純化することができるという利便性があります。

共有の削除

MMC あるいは Data ONTAP コマンド行から共有を削除することができます。

MMC からの共有の削除

MMC から共有を削除することができます。

始める前に

このタスクについて

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」を選択してください。
4. 「共有」をダブルクリックします。
5. 右側のペインで、共有を右クリックし、「共有の停止」を選択します。
6. 確認ボックスで「OK」を選択します。

タスクの結果

MMC は共有を削除します。

Data ONTAP コマンド行からの共有の削除

Data ONTAP コマンド行から、`cifs shares` コマンドを使用して共有を削除することができます。

コマンド `cifs shares -delete [-f] sharename` を入力します。`-f` オプションは、共有上で閉じられているすべてのファイルをプロンプトなしで強制的に削除します。このコマンドは、スクリプトで便利です。

アクセス制御リストの管理

MMC あるいはコマンド行から、共有レベル ACL を表示あるいは変更することができます。ファイル・レベル ACL は、コマンド行からのみ変更することができます。

共有レベル ACL について

CIFS ユーザーが共有にアクセスを試みる場合、Data ONTAP は共有を含む `qtree` のセキュリティー・スタイルに関わらず、常に共有レベル ACL をチェックしてアクセスが許可されるべきかを決定します。

共有レベル ACL (アクセス制御リスト) はアクセス制御エントリ (ACE) のリストで構成されます。それぞれの ACE は、ユーザー名あるいはグループ名と、ユーザーあるいはグループの共有へのアクセスを決定する許可のセットを含んでいます。

共有レベル ACL のみが共有内のファイルへのアクセスを制限し、ファイル・レベル ACL 以上のアクセスを認可することはありません。

共有レベル ACL の表示および変更

ユーザーに、より大きな、あるいはより少ない共有へのアクセス権を提供するために、共有レベル ACL を変更することができます。

このタスクについて

共有を作成した後、デフォルトでは共有レベル ACL は `Everyone` と名付けられた標準的なグループに読み取り権限を与えます。ACL での読み取り権限は、ドメイン内のすべてのユーザーおよびすべての信頼されたドメインが共有への読み取り専用アクセス権を所有していることを意味します。

Windows クライアントの MMC あるいは Data ONTAP コマンド行を使用して、共有レベル ACL を変更することができます。

MMC を使用する場合、以下のガイドラインに注意してください。

- Windows アクセス権のみ指定できます。
- 指定されたユーザー名およびグループ名は Windows 名である必要があります。
- 共有レベル ACL は、UNIX スタイルのアクセス権を持ってはいけません。

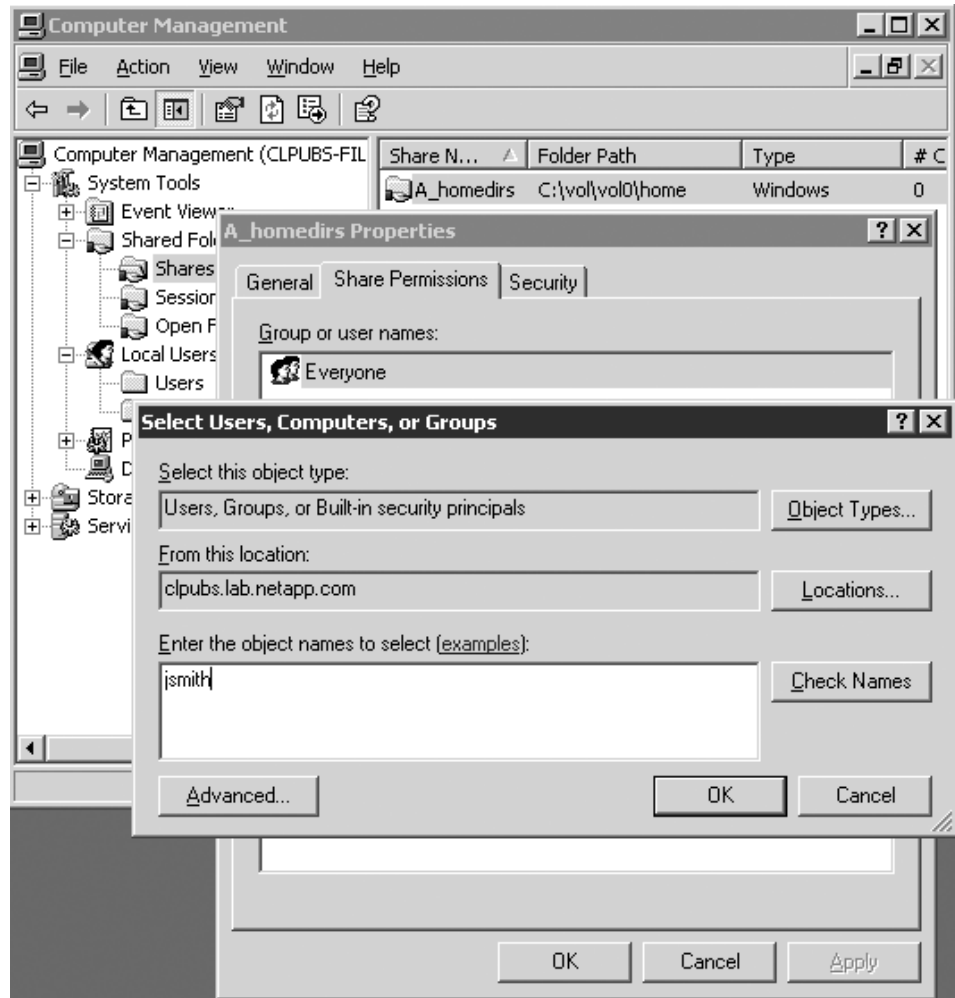
Data ONTAP コマンド行を使用する場合は、以下のガイドラインに注意してください。

- Windows アクセス権あるいは UNIX スタイルのアクセス権のいずれかが指定できます。
- ユーザー名およびグループ名は Windows 名あるいは UNIX 名が可能です。
- ストレージ・システムが `/etc/passwd` ファイルで認証されている場合、ACL のユーザー名あるいはグループ名は UNIX 名であることが仮定されます。ストレージ・システムがドメイン・コントローラーで認証されている場合は、名前はまず Windows 名であることが仮定されますが、ドメイン・コントローラーで名前が検出されなかった場合は、ストレージ・システムは UNIX 名データベースで名前の検索を試行します。

Windows クライアントの MMC から共有レベル ACL へのユーザーあるいはグループの追加

Windows クライアントの MMC から ACL にユーザーあるいはグループを追加することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」を選択してください。
4. 「共有」をダブルクリックします。
5. 右側のペインで、共有を右クリックします。
6. 「プロパティ」を選択します。
7. 「共有のアクセス許可」タブを選択します。共有の ACL が表示されます。
8. 「追加」をクリックします。
9. 「ユーザー または グループの選択 (Select Users, Computers, or Groups)」ウィンドウで、ユーザー名を「選択するオブジェクト名を入力してください (Enter the object names to select)」ボックスに入力します。



10. 「OK」をクリックします。

タスクの結果

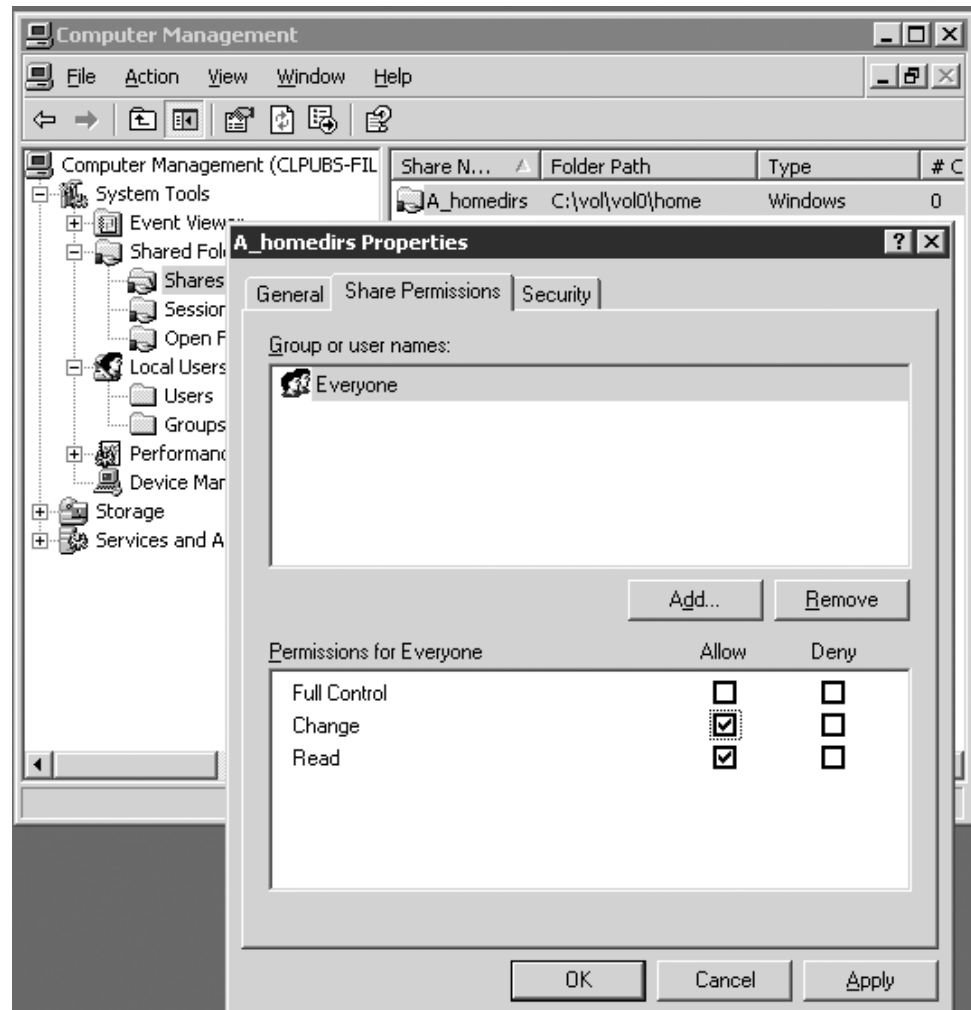
これで ACL は新規ユーザーあるいはグループを含んでいます。

Windows クライアントの MMC からの共有レベル ACL の表示および変更

Windows クライアントの MMC から共有レベル ACL を表示および変更することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」を選択してください。
4. 「共有」をダブルクリックします。
5. 右側のペインで、共有を右クリックします。
6. 「プロパティ」を選択します。
7. 「共有のアクセス許可」タブを選択します。 共有の ACL が表示されます。

8. グループあるいはユーザーの ACL を変更するには、「名前」ボックスからグループあるいはユーザーを選択し、「アクセス許可」ボックスでアクセス権を変更します。



Windows クライアントの MMC を使用した、共有レベル ACL からのユーザーあるいはグループの削除

Windows クライアントの MMC を使用して、共有レベル ACL からユーザーあるいはグループを削除することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「共有フォルダ」を選択してください。
4. 「共有」をダブルクリックします。
5. 右側のペインで、共有を右クリックします。
6. 「プロパティ」を選択します。
7. 「共有のアクセス許可」タブを選択します。共有の ACL が表示されます。
8. ユーザーあるいはグループを選択します。
9. 「削除」をクリックします。

タスクの結果

これで ACL はユーザーあるいはグループを含んでいません。

Data ONTAP コマンド行からの共有レベル ACL の変更

共有レベル ACL を、Data ONTAP コマンド行から `cifs access` コマンドを使用して変更することができます。

次のコマンドを入力します。 `cifs access share [-g] user rights`

`share` は、共有の名前です (* および ? ワイルドカードが使用できます)。

`user` は、ユーザーあるいはグループの名前です (UNIX または Windows)。

`user` がローカル・グループの場合、ドメイン名としてストレージ・システム名を指定します (例えば、`toaster¥writers`)。

`rights` はアクセス権です。 Windows ユーザーについては、アクセス権の以下の選択項目から 1 つを指定します。 No Access (アクセス権なし)、Read (読み取り)、Change (変更)、Full Control (フル・コントロール)。 UNIX ユーザーについては、アクセス権の以下の選択項目から 1 つを指定します。 r (読み取り)、w (書き込み)、x (実行)。

-g オプションを使用して、`user` が UNIX グループの名前であることを指定します。

例

以下の例は、共有 `release` で Windows ユーザー `ENGINEERING¥mary` に Windows 読み取り権限を認可しています。

```
cifs access releases ENGINEERING¥mary Read
```

以下の例は、共有 `accounting` でユーザー `john` に UNIX 読み取りおよび実行アクセス権限を認可しています。

```
cifs access accounting john rx
```

以下の例は、共有 `sysadmins` で UNIX グループ `wheel` にフル・アクセス権限を認可しています。

```
cifs access sysadmins -g wheel Full Control
```

Data ONTAP コマンド行を使用した、共有レベル ACL からのユーザーあるいはグループの削除

Data ONTAP コマンド行を使用して、ACL からユーザーあるいはグループを削除することができます。

次のコマンドを入力します。 `cifs access -delete share [-g] user`

`share` は、共有の名前です (* および ? ワイルドカードが使用できます)。

`user` は、ユーザーあるいはグループの名前です (UNIX または Windows)。

`user` がローカル・グループの場合、ドメイン名としてストレージ・システム名を指定します (例えば `toaster¥writers`)。

-g オプションを使用して、`user` が UNIX グループの名前であることを指定します (つまり、その `user` は、UNIX ユーザーでも、Windows ユーザーでも、Windows グループでもありません)。

**例: 共有 releases からの ENGINEERING¥mary に関する ACL エントリ
の削除**

```
cifs access -delete releases ENGINEERING¥mary
```

**NFSv3 および NFSv4 クライアントが Windows ACL アクセス権
の表示を最小アクセスあるいは最大アクセスのいずれに基づくかの指
定**

NFSv3 および NFSv4 が Windows ACL によって認可された最小アクセスに基づい
て、Windows ACL アクセス権 (UNIX あるいは NFSv4 アクセス権ではない) を表
示するべきであると指定するには、nfs.ntacl_display_permissive_perms オプションを
on に設定します。そうでない場合は、このオプションを off に設定します。デフォ
ルトでは、このオプションは off です。

このタスクについて

Data ONTAP の 7.2.1 より前のバージョンでは、NFSv3 および NFSv4 クライアン
トに表示されるファイルのアクセス権は、Windows ACL に認可された最大アクセ
スに基づいていました。しかし Data ONTAP 7.2.1 からは、NFSv3 および NFSv4
クライアントに表示されるファイルのアクセス権は Windows ACL に認可された最
小アクセスに基づきます。

次のコマンドを入力します。options nfs.ntacl_display_permissive_perms on |
off

ファイル・レベル ACL の表示および変更

ファイル・レベル ACL を変更して、特定のユーザーおよびグループがファイルへ
のアクセス権を所有するかをコントロールすることができます。

このタスクについて

ファイルおよびディレクトリーのアクセス権の設定は、ファイル・レベル ACL に
保管されます。これらの ACL は、Windows 2000 NTFS セキュリティー・モデルに
従います。NTFS スタイルのセキュリティを持つファイルについては、CIFS ユ
ーザーが PC からファイル・レベル ACL を設定および表示することができます。
NTFS スタイルの qtree にあるすべてのファイルおよび混合 qtree にあるいくつか
のファイルは、NTFS スタイルのセキュリティを持つ場合があります。

FAT (ファイル・アロケーション・テーブル) ファイル・システムのファイルには、
ACL がありません。それらのファイルは UNIX アクセス権を使用します。ACL
を持たないファイルが CIFS クライアントから表示された場合、ファイルのプロパ
ティー・ウィンドウでセキュリティ・タブは表示されません。

提供されたリソースのファイル・システム (FAT あるいは NTFS) は、ストレ
ージ・システムの認証方式およびそのリソースの qtree スタイルによって決まりま
す。

qtree スタイルおよび認証方式	ファイル・システム
UNIX スタイルの qtree およびすべての認証方式	FAT

qtree スタイルおよび認証方式	ファイル・システム
混合あるいは NTFS スタイルの qtree および /etc/passwd 認証	FAT
混合あるいは NTFS スタイルの qtree、およびドメインまたはワークグループ認証	NTFS

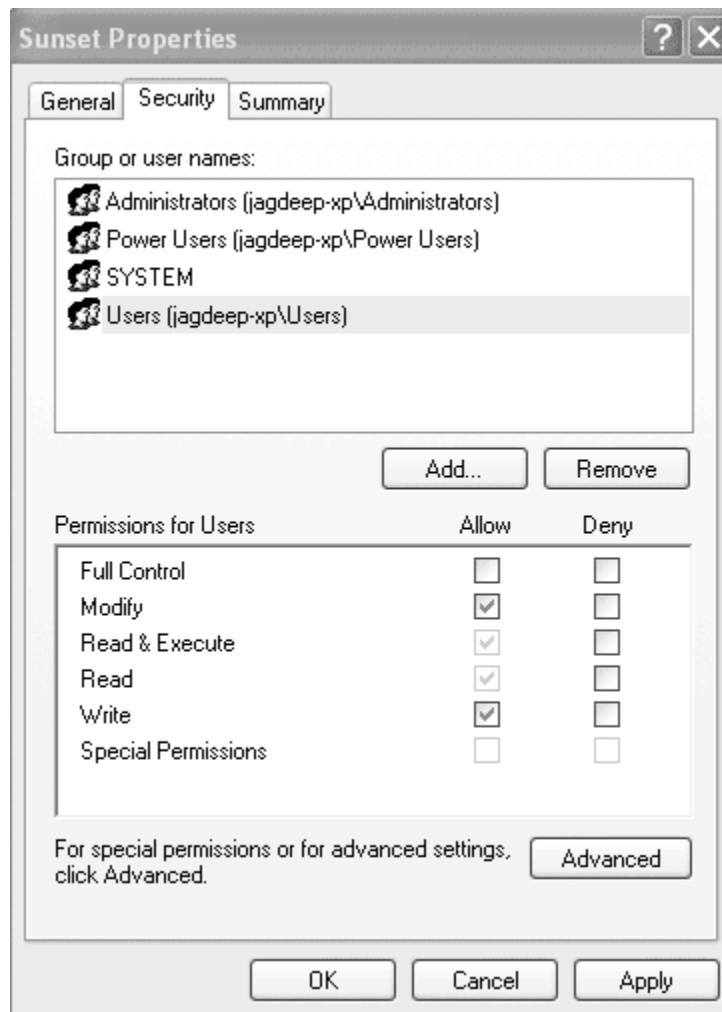
1. Windows のデスクトップからファイルを右クリックし、ポップアップ・メニューから「プロパティ」を選択します。

注: NT4 クライアントで、ワイド・シンボリック・リンクをサポートする共有にあるファイルを右クリックして「プロパティ」を選択した場合、「セキュリティ」タブは表示されません。 `cacls` のようなセキュリティー・ツールを使用して、セキュリティーを設定することができます。あるいは、Windows 2000 クライアントからファイルにアクセスするか、またはワイド・シンボリック・リンクをサポートしない共有を使用してファイルにアクセスすることができます。同一のディレクトリーに 1 つはワイド・シンボリック・リンクをサポートし、1 つはサポートしない 2 つの異なる共有を持つことができ、セキュリティーを設定するときにはワイド・シンボリック・リンクをサポートしない共有を使用します。

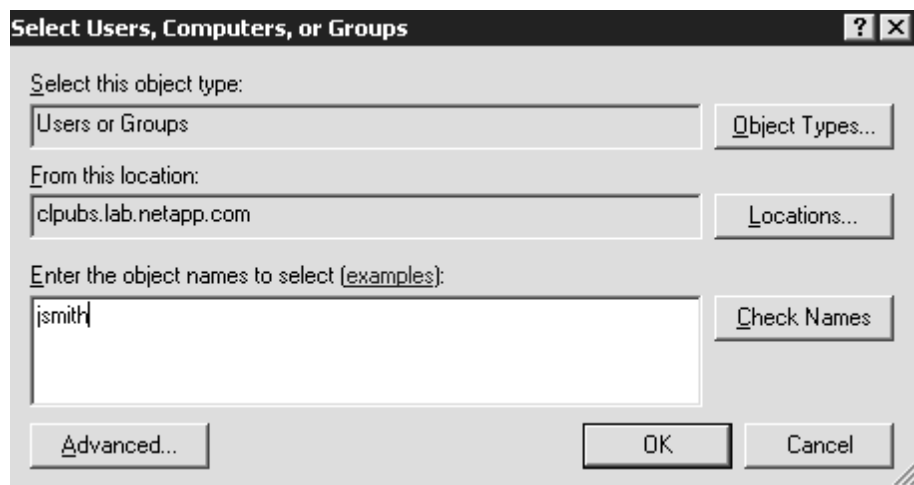
2. 「セキュリティ」タブをクリックします。

注: 認証方式および qtree スタイルによって、「セキュリティ」タブがない場合があります。

3. アクセス権を表示したいユーザーあるいはグループを「名前」ボックスから選択します。 選択したユーザーあるいはグループのアクセス権が「アクセス許可」ボックスに表示されます。



4. ファイルにユーザーあるいはグループを追加するには、「追加」をクリックし、「ユーザー または グループの選択」ウィンドウで「選択するオブジェクト名を入力してください (Enter the object names to select)」ボックスにユーザーあるいはグループの名前を入力します。



ユーザーあるいはグループが ACL に追加されます。

共有レベル ACL と連動したグループ ID の動作方法の指定

共有が UNIX スタイルのセキュリティーを持つファイルを含んでおり、UNIX グループによるアクセスをコントロールするために共有レベル ACL を使用したい場合、Data ONTAP がグループ ID に基づいてファイルへのユーザー・アクセスを認可するかどうかを決定する必要があります。

このタスクについて

共有名 `specs` が UNIX スタイルの `qtree` に存在し、2 つの UNIX グループ `engineering` および `marketing` に共有へのフル・アクセス権限を持たせたい場合、これらのグループに共有レベルで `rwX` アクセス権を与えます。

この共有で `engineering` グループが所有しているファイルが `draft` と命名され、次のアクセス権を持っていると仮定します。

```
draft rwXr-x---
```

`engineering` のメンバーが `draft` ファイルにアクセスを試みると、共有レベル ACL はこのユーザーに共有 `specs` への無制限のアクセス権を与え、`draft` ファイルへのアクセスは `engineering` グループに割り当てられたアクセス権 (この例では `r-x`) によって判別されます。

ただし、`marketing` のメンバーが `draft` ファイルへのアクセスを試みた場合は、UNIX スタイルのファイル・アクセス権は `engineering` の非メンバーにはファイルへのアクセスを認可しないため、アクセスは拒否されます。`draft` ファイルを `marketing` グループに読み取り可能にするには、ファイル・レベルのアクセス権を以下の設定に変更する必要があります。

```
draft rwXr-xr-x
```

これらのアクセス権の欠点は、`marketing` に加えてすべての UNIX ユーザーがファイルを読み取ることができ、それがセキュリティー問題を引き起こします。

この問題を解決するために、Data ONTAP がアクセスを認可するときに `GID` を無視するように構成することができます。

Data ONTAP がアクセスを認可するときにユーザーの `GID` を無視するように構成する場合は、ファイルの所有者ではないすべてのユーザーはそのファイルの所有者である UNIX グループのメンバーであると見なされます。前出の例では、`engineering` グループに適用されたアクセス権が、ファイルにアクセスを試みる `marketing` のメンバーにも適用されます。つまり、`engineering` メンバーおよび `marketing` のメンバーの両方が `draft` ファイルへの `r-x` アクセス権を持ちます。

デフォルトでは、Data ONTAP はアクセス権を認可する前にユーザーの `GID` を考慮します。このデフォルト構成は、以下の記述のいずれかが当てはまる場合には便利です。

- 共有は UNIX スタイルのセキュリティーを持つファイルを含んでいない。
- UNIX グループのアクセスをコントロールするために共有レベル ACL を使用しない。

ユーザー・アクセスを認可するときにユーザーの GID を考慮するか無視するかを指定します。

以下を実施したい場合、	以下を実行してください。
ユーザー・アクセスの認可時にユーザーの GID を無視する	次のコマンドを入力します。options cifs.perm_check_use_gid off
ユーザー・アクセスの認可時にユーザーの GID を考慮する	次のコマンドを入力します。options cifs.perm_check_use_gid on

ホーム・ディレクトリーの管理

ストレージ・システム上にユーザーのホーム・ディレクトリーを作成し、自動的に各ユーザーにホーム・ディレクトリー共有を提供するように Data ONTAP を構成することができます。

このタスクについて

CIFS クライアントから、ホーム・ディレクトリーはユーザーが接続できる他の共有と同じ方法で動作します。

各ユーザーは、自身のホーム・ディレクトリーにのみ接続でき、他のユーザーのホーム・ディレクトリーには接続できません。

ストレージ・システム上のホーム・ディレクトリーについて

Data ONTAP はホーム・ディレクトリー名をユーザー名にマッピングし、指定されたホーム・ディレクトリーを検索し、またホーム・ディレクトリーを通常の共有とは少し異なる方法で扱います。

Data ONTAP はユーザーに対して、マッチング名を使用して共有を提供します。マッチングのためのユーザー名には、Windows ユーザー名、Windows ユーザー名が後に続くドメイン名、あるいは UNIX ユーザー名が使用できます。ホーム・ディレクトリー名は、大/小文字の区別がありません。

Data ONTAP がユーザー名に基づいて命名されたディレクトリーを見つけようとする際には、指定したパスのみを検索します。これらのパスは、ホーム・ディレクトリー・パスと呼ばれます。ホーム・ディレクトリー・パスは、異なるボリュームに存在することができます。

ホーム・ディレクトリーとその他の共有は、以下の点が異なります。

- 共有レベル ACL およびホーム・ディレクトリーに関するコメントを変更することはできません。
- 「cifs shares」コマンドはホーム・ディレクトリーには表示されません。
- 汎用命名規則 (UNC) を使用したホーム・ディレクトリーの指定のフォーマットは、他の共有の指定とは異なる場合があります。

/vol/vol1/enghome および /vol/vol2/mktghome をホーム・ディレクトリー・パスとして指定する場合は、Data ONTAP はこれらのパスをユーザーのホーム・ディレクトリーを見つけるために検索します。jdoe 用のディレクトリーを /vol/vol1/enghome パスに作成し、jsmith 用のディレクトリーを /vol/vol2/mktghome に作成する場合、

両方のユーザーがホーム・ディレクトリーを提供されます。jdoe 用のホーム・ディレクトリーは /vol/vol1/enghome/jdoe ディレクトリーに対応し、jsmith 用のホーム・ディレクトリーは /vol/vol2/mktghome/jsmith ディレクトリーに対応します。

Data ONTAP によるディレクトリーとユーザーのマッチング方法

ホーム・ディレクトリーの命名スタイルを指定し、Data ONTAP がディレクトリーをユーザーとマッチングさせる方法を決定することができます。

以下は、選択可能な命名スタイルおよび各スタイルに関する情報です。

- **Windows 名** — Data ONTAP は、ユーザーの Windows 名に一致するディレクトリーを検索します。
- **非表示名** — 命名スタイルが非表示の場合、ユーザーは Windows ユーザー名にドル記号を追加して (name\$) ホーム・ディレクトリーに接続し、Data ONTAP は Windows ユーザー名 (name) に一致するディレクトリーを検索します。
- **Windows ドメイン名および Windows 名** — 異なるドメインのユーザーのユーザー名が同一である場合、ドメイン名で区別する必要があります。

この命名スタイルでは、Data ONTAP はドメイン名に一致するホーム・ディレクトリー・パス内のディレクトリーを検索します。次に、ドメイン・ディレクトリーでユーザー名に一致するホーム・ディレクトリーを検索します。

例: engineering¥jdoe のディレクトリーおよび marketing¥jdoe のディレクトリーを作成するには、ホーム・ディレクトリー・パスに 2 つのディレクトリーを作成します。ディレクトリーは、ドメイン名 (engineering および marketing) と同じ名前を持ちます。次に、これらのドメイン・ディレクトリーにユーザーのホーム・ディレクトリーを作成します。

- **マッピングされた UNIX 名** — 命名スタイルが UNIX の場合、Data ONTAP はユーザーのマッピングされた UNIX 名と一致するディレクトリーを検索します。

例: John Doe の Windows 名 jdoe が UNIX 名 johndoe にマッピングされている場合、Data ONTAP はホーム・ディレクトリー・パスで johndoe (jdoe ではない) と名付けられたディレクトリーを検索し、それを John Doe にホーム・ディレクトリーとして提供します。

ホーム・ディレクトリーの命名スタイルを指定しない場合、Data ONTAP はディレクトリーのマッチングにユーザーの Windows 名を使用します。これは Data ONTAP のバージョン 6.0 以前で使用されていたものと同じスタイルです。

シンボリック・リンクのホーム・ディレクトリーとの動作の仕方

シンボリック・リンクの動作の仕方は、ホーム・ディレクトリーの命名スタイルによって変わります。

Data ONTAP 6.0 以前の命名スタイル: 命名スタイルを指定しない場合、Data ONTAP はシンボリック・リンクを Data ONTAP 6.0 以前と同じ方法で使用します。この方法は、ホーム・ディレクトリーを位置指定するホーム・ディレクトリー・パスの外部のディレクトリーを指すすべてのシンボリック・リンクに従います。

例: ホーム・ディレクトリー・パスが `/vol/vol0/eng_homes` で、6.0 以前のホーム・ディレクトリーの命名スタイルを使用していると仮定します。 `jdoe` のホーム・ディレクトリーを見つけるために、Data ONTAP は `/vol/vol0/eng_homes/jdoe` を検索します。これは、`/vol/vol1/homes/jdoe` のようなホーム・ディレクトリー・パスの外部のディレクトリーを指すシンボリック・リンクであることも可能です。

他の命名スタイル: ホーム・ディレクトリーの命名スタイルを指定した場合、デフォルトでシンボリック・リンクは、ホーム・ディレクトリー・パス内のディレクトリーをシンボリック・リンクが指している場合のみ動作します。

例: ホーム・ディレクトリー・パスが `/vol/vol0/eng_homes` で、Windows 命名スタイルを使用していると仮定します。 `jdoe` のホーム・ディレクトリーを見つけるために、Data ONTAP は `/vol/vol0/eng_homes/jdoe` を検索します。パスがシンボリック・リンクの場合、ユーザーは、シンボリック・リンクのターゲットがホーム・ディレクトリー・パス内にある場合にのみ、ホーム・ディレクトリーにアクセスできます。例えば、シンボリック・リンクが `/vol/vol0/eng_homes/john` ディレクトリーを指す場合は動作しますが、`/vol/vol1/homes/john` ディレクトリーを指す場合は動作しません。

注: CIFS クライアントが、ホーム・ディレクトリー・パスの外部の宛先へのシンボリック・リンクに従うことを許可するように、デフォルトのストレージ・システム設定を変更することが可能です。

Data ONTAP 6.0 以前のリリースでは、ホーム・ディレクトリーを別のボリュームに置きたい場合、シンボリック・リンクをホーム・ディレクトリー・パス内のホーム・ディレクトリーとして指定する必要がありました。現在は、Data ONTAP が異なるボリュームのホーム・ディレクトリーをサポートしているため、シンボリック・リンクをホーム・ディレクトリー名として使用する必要はありません。ただし、Data ONTAP は後方互換性のためにホーム・ディレクトリー名としてのシンボリック・リンクを引き続きサポートしています。

ホーム・ディレクトリー・パスの指定

Data ONTAP は、ユーザー名と一致するディレクトリーについて、指定した順番でホーム・ディレクトリー・パスを検索します。

始める前に

`cifs_homedir.cfg` ファイルのエントリーを変更することで、いつでもホーム・ディレクトリー・パスを変更することができます。ただし、リストから削除したホーム・ディレクトリー・パスにあるファイルをユーザーが開くと、Data ONTAP は警告メッセージを表示して変更の確認を要求します。オープン・ファイルを含むディレクトリー・パスを変更すると、ホーム・ディレクトリーへの接続は終了します。

このタスクについて

複数のホーム・ディレクトリー・パスを指定することができます。Data ONTAP はマッチング・ディレクトリーを検出すると、検索を停止します。

ホーム・ディレクトリーの最上位にユーザーをアクセスさせたくない場合は、ホーム・ディレクトリー・パスに拡張子を追加することができます。拡張子は、ユーザーがホーム・ディレクトリーにアクセスしたときに自動的に開かれるサブディレクトリーを指定します。

/etc/cifs_homedir.cfg ファイルを編集することで、ホーム・ディレクトリー・パスを指定することができます。 /etc/cifs_homedir.cfg ファイルに、最大で 1,000 個までのパス名を指定することができます。

Data ONTAP は CIFS が始動したときに既存のファイルがない場合、/etc ディレクトリーにデフォルトの cifs_homedir.cfg ファイルを作成します。このファイルへの変更は、CIFS が始動するときには必ず自動的に処理されます。 cifs homedir load コマンドを使用して、このファイルへの変更を処理することもできます。

1. ホーム・ディレクトリー・パスとして使用するためのディレクトリーを作成します。例えば、/vol/vol0 ボリュームに enghome と命名したディレクトリーを作成します。
2. 編集のために /etc/cifs_homedir.cfg ファイルを開きます。
3. ステップ 1 で作成したホーム・ディレクトリー・パス名を、/etc/cifs_homedir.cfg ファイルに 1 行につき 1 エントリーずつ入力し、Data ONTAP がユーザー・ホーム・ディレクトリーを検索するパスとして指定します。

注: 最大 1,000 個までパス名を入力することができます。

4. エントリーを処理するには、コマンド cifs homedir load [-f] を入力します。-f オプションは、新規のパスの使用を強制します。

ホーム・ディレクトリー・パスのリストの表示

cifs homedir コマンドを使用して、現在のディレクトリー・パスのリストを表示することができます。

次のコマンドを入力します。cifs homedir

注: ホーム・ディレクトリーに非表示の命名スタイルを使用している場合、ホーム・ディレクトリー・パスのリストを表示する際は Data ONTAP が自動的にホーム・ディレクトリー名に \$ 記号を追加します (例、name\$)。

タスクの結果

ホーム・ディレクトリーに非表示の命名スタイルを使用している場合、以下のような場合にはホーム・ディレクトリーは表示されません。

- DOS で net view ¥¥filer コマンドを使用する
- Windows で、エクスプローラー・アプリケーションを使用してストレージ・システムにアクセスし、ホーム・ディレクトリー・フォルダーを表示する

ホーム・ディレクトリーの命名スタイルの指定

cifs.home_dir_namestyle オプションを設定することで、ホーム・ディレクトリーの命名スタイルを指定することができます。

次のコマンドを入力します。options cifs.home_dir_namestyle {ntname | hidden | domain | mapped | ""}

ホーム・ディレクトリーが Windows ユーザー名と同じ名前を持つ場合は、ntname を使用します。

Windows ユーザー名と同じ名前のホーム・ディレクトリーの検索を開始するために、ドル記号 (\$) が追加された Windows ユーザー名を使用したい場合は、hidden を使用します。

ホーム・ディレクトリーを検索するために、Windows ユーザー名に加えてドメイン名を使用したい場合は、domain を使用します。

ホーム・ディレクトリーが usermap.cfg ファイルで指定されたとおりの UNIX ユーザー名を持つ場合は、mapped を使用します。

命名スタイルを指定せず、Data ONTAP 6.0 より前で行われていた方法と同じ方法でホーム・ディレクトリーをユーザー名にマッチングさせたい場合は、"" を使用します。この方法では、ホーム・ディレクトリーを位置指定するためのホーム・ディレクトリー・パスの外部にあるディレクトリーをポイントするシンボリック・リンクに従います。

デフォルトでは、cifs.home_dir_namestyle オプションは "" です。

ホーム・ディレクトリー・パスでのディレクトリー作成 (ドメイン名スタイル)

cifs.home_dir_namestyle オプションが domain の場合、/etc/cifs_homedir.cfg の編集、ディレクトリーの作成、およびディレクトリーのアクセス権の設定によってホーム・ディレクトリーを作成することができます。

1. /etc/cifs_homedir.cfg ファイルを開き、ホーム・ディレクトリーをどこに存在させるかを示すパスを追加します。ホーム・ディレクトリーは、それぞれのユーザーが属している NetBIOS ドメインのために命名されたフォルダー内に存在します。例えば、パス /vol/vol1/homedir を /etc/cifs_homedir.cfg ファイルに追加します。
2. /etc/cifs_homedir.cfg ファイルに追加したディレクトリーに、各ドメインのディレクトリーを作成します。例えば、2 つのドメイン、HQ と UK がある場合、/vol/vol1/homedir/hq/ ディレクトリーおよび /vol/vol1/homedir/uk/ ディレクトリーを作成します。
3. ステップ 2 で作成された各ドメイン・ディレクトリーで、そのドメインのユーザー用にホーム・ディレクトリーを作成します。例えば、2 人のユーザーが jsmith をいう名前で、HQ ドメインと UK ドメインにいる場合、/vol/vol1/homedir/HQ/jsmith ホーム・ディレクトリーおよび /vol/vol1/homedir/UK/jsmith ホーム・ディレクトリーを作成します。
4. 各ユーザーをそれぞれのホーム・ディレクトリーの所有者にします。例えば、HQ\jsmith を /vol/vol1/homedir/HQ/jsmith ホーム・ディレクトリーの所有者にし、UK\jsmith を /vol/vol1/homedir/UK/jsmith ホーム・ディレクトリーの所有者にします。

HQ\jsmith という名前のユーザーは、/vol/vol1/homedir/HQ/jsmith ホーム・ディレクトリーに対応している jsmith 共有に接続することができます。UK\jsmith という名前のユーザーは、/vol/vol1/homedir/UK/jsmith ホーム・ディレクトリーに対応している jsmith 共有に接続することができます。

5. 新規の CIFS homedir 構成をストレージ・システムにロードします。例えば、次のコマンドを入力します。`cifs homedir load -f`
6. CIFS homedir ドメイン名スタイルが動作しているかを、コマンド `cifs homedir showuser user_name` を入力して確認します。例えば、次のコマンドの 1 つを入力します。`cifs homedir showuser hq/jsmith` または `cifs homedir showuser uk/jsmith`

ホーム・ディレクトリー・パスでのディレクトリー作成 (非ドメイン名スタイル)

`cifs.home_dir_namestyle` オプションが `domain` ではない場合、ディレクトリーを作成し、ユーザーをそのディレクトリーの所有者にすることでホーム・ディレクトリーを作成することができます。

1. ホーム・ディレクトリー・パスの指定で、ホーム・ディレクトリーを作成します。例えば、2 人のユーザー `jsmith` と `jdoe` がいる場合に、`/vol/vol0/enghome/jsmith` および `/vol/vol1/mktghome/jdoe` ホーム・ディレクトリーを作成します。

ユーザーは、ユーザー名と同じ名前の共有に接続し、ホーム・ディレクトリーとして共有の使用を開始することができます。

2. 各ユーザーをそれぞれのホーム・ディレクトリーの所有者にします。例えば、`jsmith` を `/vol/vol0/enghome/jsmith` ホーム・ディレクトリーの所有者にし、`jdoe` を `/vol/vol1/mktghome/jdoe` ホーム・ディレクトリーの所有者にします。

`engineering¥jsmith` という名前のユーザーは、共有名 `jsmith` に接続できます。この共有は `/vol/vol0/enghome/engineering/jsmith` ホーム・ディレクトリーに対応しています。

`marketing¥jdoe` という名前のユーザーは、共有名 `jdoe` に接続できます。この共有は `/vol/vol1/mktghome/marketing/jdoe` ホーム・ディレクトリーに対応しています。

タスクの結果

注: 命名スタイルが非表示の場合、ユーザーはホーム・ディレクトリーに接続するために、ユーザー名にドル記号 (\$) を追加して (例えば、`name$`) 入力する必要があります。

ホーム・ディレクトリー・パス拡張が使用されている場合の、ホーム・ディレクトリーでのサブディレクトリー作成

ホーム・ディレクトリー・パス拡張を使用している場合に、ユーザーがホーム・ディレクトリー内でアクセス可能なサブディレクトリーを作成することができます。

拡張機能を持つホーム・ディレクトリー・パスにある各ホーム・ディレクトリーについて、ユーザーにアクセスさせたいサブディレクトリーを作成します。例えば、`/etc/cifs_homedir.cfg` ファイルが `/vol/vol0/enghome/%u%/data` パスを含む場合、各ホーム・ディレクトリーに `data` という名前のサブディレクトリーを作成します。ユーザーは、ユーザー名と同じ名前の共有に接続することができます。ユーザーが共有に読み取りあるいは書き込みを行う場合、ユーザーは実際には `data` サブディレクトリーにアクセスします。

UNC 名を使用したホーム・ディレクトリー指定の構文

UNC を使用してホーム・ディレクトリーを指定するための規則は、`cifs.home_dir_namestyle` オプションによって指定されたホーム・ディレクトリーの命名スタイルによって決まります。

以下の表は命名スタイルの各値に関する UNC 名を、例と一緒にリストしています。

<code>cifs.home_dir_namestyle</code> の値	UNC 名
<code>ntname</code> または <code>""</code>	<code>¥¥filer¥¥Windows_NT_name</code> 例: <code>¥¥toaster¥¥jdoe</code>
<code>hidden</code>	<code>¥¥filer¥¥Windows_NT_name\$</code> 例: <code>¥¥toaster¥¥jdoe\$</code>
<code>domain</code>	<code>¥¥filer¥~domain~Windows_NT_name</code> 例: <code>¥¥toaster¥~engineering~jdoe</code>
<code>mapped</code>	<code>¥¥filer¥~mapped_name</code> 例: <code>¥¥toaster¥~jdoe</code>

`cifs.home_dir_namestyle` が `domain` にも関わらず、アクセス要求の UNC 名 がドメイン名を指定していない場合、Data ONTAP はドメインを、要求が送信されたドメインであると仮定します。アクセス要求でドメイン名を省略する場合、ユーザー名の前のチルド (~) も省略することができます。

例: ユーザー名 `jdoe` が、`engineering` ドメインにある PC から `engineering¥jdoe` としてログインしています。このユーザーが `marketing` ドメインでのユーザー名を使用して自分の ホーム・ディレクトリー にアクセスしようとする場合、アクセスを要求するために次のいずれかのコマンドを入力することができます。

```
net use * ¥¥toaster¥~jdoe /user:marketing¥jdoe
```

```
net use * ¥¥toaster¥jdoe /user:marketing¥jdoe
```

他のユーザーのホーム・ディレクトリーへのアクセスの有効化

ユーザーは自分のホーム・ディレクトリーにのみ接続できますが、他のユーザーのホーム・ディレクトリーにアクセスすることを許可することができます。

1. 以下のいずれか 1 つのパス名に一致する共有を作成します。

- `cifs.home_dir_name_style` が `domain` ではない場合は、ホーム・ディレクトリー・パス
- `cifs.home_dir_name_style` が `domain` の場合は、ホーム・ディレクトリー・パス内の・ディレクトリー

例: `/vol/vol0/enghome` がホーム・ディレクトリー・パスの場合、次のコマンドを使用します。


```
cifs shares -add eng_dirs /vol/vol0/enghome -comment "readable  
engineering home directories"
```

2. 各ユーザーに他のユーザーのホーム・ディレクトリーへの適切なアクセス許可を割り当てます。 例: 次のように、eng_dirs 共有について engineering グループに読み取り専用アクセス権を割り当てます。cifs access eng_dirs engineering full これにより、engineering グループのメンバーは読み取り専用アクセス権を eng_dirs 共有内のすべてのホーム・ディレクトリーに対して所有します。

共有エイリアスを使用した CIFS ホーム・ディレクトリーへのアクセス

あらゆる CIFS ホーム・ディレクトリーの命名スタイルについて、cifs.homedir あるいはチルド (~) 共有エイリアスのいずれかを使用して、所有する CIFS ホーム・ディレクトリーに接続することが可能です。

このタスクについて

所有する CIFS ホーム・ディレクトリーへの接続は、スクリプトを書いているときに便利です。

例

```
net use * ¥¥toaster¥cifs.homedir
```

```
net use * ¥¥toaster¥~
```

共有からのワイド・シンボリック・リンクの有効化あるいは無効化

共有あるいはストレージ・システムの外部の宛先への絶対シンボリック・リンクに従うように CIFS クライアントを許可したい場合、共有からのワイド・シンボリック・リンクを有効にすることができます。デフォルトでは、この機能は無効に設定されています。

共有からのワイド・シンボリック・リンクを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
共有からのワイド・シンボリック・リンクを有効にする	Data ONTAP コマンド行で、次のコマンドを入力します。cifs shares -change sharename -widelink
共有からのワイド・シンボリック・リンクを無効にする	Data ONTAP コマンド行で、次のコマンドを入力します。cifs shares -change sharename -nowidelink

タスクの結果

注: 共有の作成時に widelink オプションを指定することでも、共有からのワイド・シンボリック・リンクを有効にすることができます。

次のタスク

共有からのワイド・シンボリック・リンクを有効に設定した後、各ワイド・シンボリック・リンクが示す宛先をストレージ・システムがどのように判別するかを指定するために、`/etc/symlink.translations` ファイルに `Widelink` エントリーを作成する必要があります。

ホーム・ディレクトリーの無効設定

`/etc/cifs_homedir.cfg` ファイルを削除することで、ホーム・ディレクトリーの提供を停止することができます。ホーム・ディレクトリーを削除するために、`cifs shares -delete` コマンドは使用できません。

ストレージ・システム上の `/etc/cifs_homedir.cfg` ファイルを削除します。

ローカル・ユーザーおよびグループの管理

このセクションでは、ストレージ・システム上でのローカル・ユーザーおよびグループの作成および管理について説明しています。

ローカル・ユーザーの管理

ローカル・ユーザーは、ユーザーおよびグループのリストで指定することができます。例えば、ファイル・レベル ACL および共有レベル ACL でローカル・ユーザーを指定することができます。また、ローカル・ユーザーをローカル・グループに追加することもできます。

ローカル・ユーザー・アカウントをいつ作成するべきか

ストレージ・システム上にローカル・ユーザー・アカウントを作成するのには、いくつかの理由があります。

- セットアップ中にストレージ・システムを Windows ワークグループのメンバーとして構成した場合、ローカル・ユーザー・アカウントを作成する必要があります。この場合、ストレージ・システムはユーザーを認証するためにローカル・ユーザー・アカウントの情報を使用しなければなりません。
- ストレージ・システムがドメインのメンバーの場合。
 - ローカル・ユーザー・アカウントによって、ストレージ・システムは信頼されていないドメインからストレージ・システムに接続しようとしているユーザーを認証することが可能になります。
 - ドメイン・コントローラーが停止している、あるいはネットワークの問題によってストレージ・システムがドメイン・コントローラーにコンタクトできない場合に、ローカル・ユーザーはストレージ・システムにアクセスすることができます。例えば、ストレージ・システムがドメイン・コントローラーへのコンタクトに失敗するときでも、ストレージ・システムにアクセスするのに使用できる `BUILTIN\Administrators` アカウントを定義することができます。

注:

セットアップ中に、ユーザーの認証に UNIX モードを使用するようにストレージ・システムを構成した場合は、ローカル・ユーザー・アカウントを作成する必要はあ

りません。UNIX モードでは、ストレージ・システムは常に UNIX パスワード・データベースを使用してユーザーの認証を行います。

ストレージ・システムの認証方式の表示

`cifs sessions` コマンドを入力することで、ストレージ・システムの認証方式を表示し、ローカル・ユーザーおよびグループを作成するべきかを判別することができます。

コマンド `cifs sessions` を入力します。詳細情報については、`na_cifs_sessions(1)` のマニュアル・ページを参照してください。

ローカル・ユーザー・アカウントの制限

ローカル・ユーザー・アカウントにはいくつかの制限があります。

- ご使用のストレージ・システム上でローカル・ユーザー・アカウントを管理するのにユーザー・マネージャー (User Manager) を使用することはできません。
- Windows NT 4.0 のユーザー・マネージャーは、ローカル・ユーザー・アカウントの表示にのみ使用できます。ただし、Windows 2000 のユーザー・マネージャーを使用した場合、ローカル・ユーザーを表示するのにユーザー・メニューは使用できません。ローカル・ユーザーを表示するには、グループ・メニューを使用します。
- 最大で 96 のローカル・ユーザー・アカウントを作成することができます。

ローカル・ユーザー・アカウントの追加、表示、および削除

`useradmin` コマンドを使用して、ローカル・ユーザー・アカウントを追加、表示、および削除することができます。

このタスクについて

`useradmin` コマンドを使用して、ストレージ・システムの管理ユーザーを作成、表示、および削除することができます。(domainuser サブコマンドから非ローカル・ユーザーを管理するためにも、このコマンドを使用できます。) `useradmin` コマンドの使用方法に関する情報については、「System Administration Guide」のストレージ・システムの管理の概要にあるローカル・ユーザー・アカウントの管理に関するセクションを参照してください。

注: Data ONTAP は、`useradmin` コマンドによって作成されたユーザー・アカウントの単一のリストを保持します。同じタイプの情報が、ローカル・ユーザー・アカウントおよび管理ユーザー・アカウントについても存在します。適切な管理者役割があるローカル・ユーザー・アカウントを持つ CIFS ユーザーは、ストレージ・システムにログインするために Windows RPC コールを使用することができます。詳細情報については、「Data ONTAP System Administration Guide」の管理者権限の管理の章を参照してください。

ローカル・グループの管理

ローカル・グループを管理して、どのユーザーがどのリソースにアクセス権を持つかをコントロールすることができます。

このタスクについて

ローカル・グループは、ユーザーおよび信頼されたドメインからのグローバル・グループで構成することができます。ローカル・グループのメンバーは、ファイルおよびリソースへのアクセス権が与えられます。

特定の既知のローカル・グループのメンバーシップは、ストレージ・システム上で特別な特権を授与します。例えば、BUILTIN¥Power ユーザーのメンバーは、共有を取り扱うことができますが、他の管理機能は所有していません。

CIFS クライアントは、以下のいずれかのフォーマットでローカル・グループの名前を表示します。

- *FILENAME¥localgroup*
- *BUILTIN¥localgroup*

Data ONTAP コマンド行からの、ローカル・グループの追加、表示、および削除

Data ONTAP コマンド行から *useradmin* コマンドを使用して、ローカル・グループを追加、表示、および削除することができます。

このタスクについて

詳細情報については、「*Data ONTAP System Administration Guide*」を参照してください。

Windows クライアントの MMC からのローカル・グループの追加

Windows クライアントの MMC からローカル・グループを追加することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「ローカル ユーザーとグループ」を選択してください。
4. 「グループ」を右クリックします。
5. 「新しいグループ」を選択します。
6. 「新しいグループ」ボックスで、グループの名前および説明を入力します。
7. 「作成」をクリックします。

タスクの結果

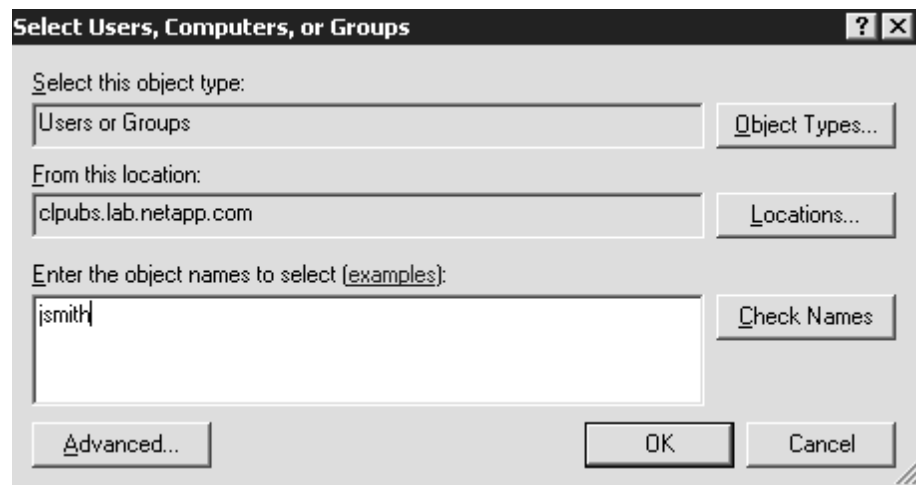
ストレージ・システムに新しいグループが作成されます。

Windows クライアントの MMC からローカル・グループへのユーザーの追加

Windows クライアントの MMC からローカル・グループにユーザーを追加することができます。

1. MMC をストレージ・システムに接続します。

2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「ローカル ユーザーとグループ」を選択してください。
4. 「グループ」をダブルクリックします。
5. 右側のパネルで、ユーザーを追加したいグループを右クリックします。
6. 「グループに追加」を選択します。MMC が「プロパティ」ボックスを表示します。
7. 「プロパティ」ボックスで、「追加」をクリックします。
8. 「ユーザー または グループの選択 (Select Users, Computers, or Groups)」ウィンドウで、ユーザー名を「選択するオブジェクト名を入力してください (Enter the object names to select)」ボックスに入力します。



9. 「OK」をクリックします。

タスクの結果

MMC はユーザーをグループに追加します。

Windows クライアントの MMC を使用したローカル・グループの削除

Windows クライアントの MMC を使用して、ローカル・グループを削除することができます。

1. MMC をストレージ・システムに接続します。
2. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
3. 「システム ツール」>「ローカル ユーザーとグループ」>「グループ」を選択してください。
4. 右側のパネルで、ユーザーを追加したいグループを右クリックします。
5. 「グループに追加」を選択します。MMC が「プロパティ」ボックスを表示します。
6. 「プロパティ」ボックスで、「追加」をクリックします。

7. 「ユーザー または グループの選択 (Select Users, Computers, or Groups)」ウィンドウで、ユーザー名を「選択するオブジェクト名を入力してください (Enter the object names to select)」ボックスに入力します。
8. 「OK」をクリックします。

タスクの結果

MMC はユーザーをグループに追加します。

SnapMirror のローカル・グループとの動作の仕方

ミラーは読み取り専用ボリュームで、ACL あるいは アクセス権を変更することができないため、SnapMirror によって複製されるファイルの ACL でローカル・グループを使用することはできません。

ボリュームを他のストレージ・システムにコピーするために SnapMirror 機能を使用し、ボリュームがローカル・グループに関する ACL を持っている場合、ACL はミラー上では適用されません。これは、グループがソースのストレージ・システムに対してローカルであるためです。

SnapMirror によって複製するファイルに関して ACL でローカル・グループを使用したい場合は、MultiStore 製品を使用することで可能になります。MultiStore 製品に関する詳細については、「MultiStore Management Guide」を参照してください。

グループ・ポリシー・オブジェクトの適用

ストレージ・システムは、Active Directory 環境のコンピューターに適用される規則のセット (グループ・ポリシー属性として知られます) である、グループ・ポリシー・オブジェクト (GPO) をサポートします。

このタスクについて

ストレージ・システムで CIFS および GPO が有効になっている場合、Data ONTAP は GPO 情報を要求している Active Directory サーバーに LDAP 照会を送信します。ご使用のストレージ・システムに適用可能な GPO 定義がある場合、Active Directory サーバーは以下を含む GPO 情報を返します。

- GPO 名
- 現行の GPO バージョン
- GPO 定義の場所
- GPO ポリシー・セットに関する UUID (汎用一意識別子) のリスト

注: Windows GPO に関する詳細情報については、www.microsoft.com で Microsoft Web サイトを参照してください。

一部の GPO がご使用のストレージ・システムに適用可能な場合は、ストレージ・システムは適切な GPO のセットを認識および処理することが可能です。

以下の GPO は、現在ご使用のストレージ・システムでサポートされています。

- 開始および終了スクリプト

- コンピューターのグループ・ポリシーのリフレッシュ・インターバル (ランダム・オフセットを含む)
- ファイル・システム・セキュリティー・ポリシー
- 制限付きグループ・セキュリティー・ポリシー
- イベント・ログ
- 監査
- 所有者ユーザー権限の取得

注: イベント・ログおよび監査ポリシーの設定のストレージ・システムへの適用は、Windows システムとは異なります。また、Windows 組み込み管理者アカウントを含まない所有ユーザーあるいはグループのリストの取得を定義した場合、これらの管理者は所有権取得の特権を失います。

ストレージ・システムで GPO を使用するための要件

ストレージ・システムで GPO を使用するには、いくつかの要件を満たしている必要があります。

要件は以下のとおりです。

- ストレージ・システム上で CIFS がライセンス交付を受け、有効になっていること。
- `cifs setup` コマンドを使用して CIFS が構成されており、セットアップ処理が Windows ドメイン・バージョン 2000 以降へのストレージ・システムの参加を含んでいること。
- ストレージ・システムと組織単位 (OU) を関連付けることによって、GPO が Windows Active Directory サーバー上で構成されていること。
- GPO サポートが、ストレージ・システム上で有効になっていること。

ストレージ・システムと OU の関連付け

`cifs setup` プロセスは、デフォルトではストレージ・システムを OU と関連付けしません。明示的に関連を構成する必要があります。

1. Windows サーバーで、「Active Directory ユーザーおよびコンピュータ (Active Directory Users and Computers)」のツリーを開きます。
2. ストレージ・システムの Active Directory オブジェクトを見つけます。
3. オブジェクトを右クリックし、「移動」を選択します。
4. ストレージ・システムと関連付けたい OU を選択します。

タスクの結果

ストレージ・システム・オブジェクトは、選択した OU に置かれています。

ストレージ・システム上での GPO サポートの有効化あるいは無効化

`cifs.gpo.enable` オプションを設定することで、ストレージ・システム上での GPO サポートを有効あるいは無効にすることができます。

以下を実施したい場合、	以下を実行してください。
GPO を有効にする	次のコマンドを入力します。options cifs.gpo.enable on
GPO を無効にする	次のコマンドを入力します。options cifs.gpo.enable off

ストレージ・システム上の GPO の管理

ストレージ・システム上のグループ・ポリシー・オブジェクト (GPO) の作成、表示、構成、更新、およびトラブルシューティングを行うことができます。

ファイル・システム・セキュリティー GPO の作成

GPO ファイル・システム・セキュリティーの設定を、Data ONTAP ファイル・システム・オブジェクト (ディレクトリーまたはファイル) に直接に指定することができます。

このタスクについて

GPO ファイル・システム・セキュリティーの設定は、ディレクトリー階層まで伝搬して下りていきます。つまり、GPO セキュリティー設定をあるディレクトリーにセットした場合、その設定はそのディレクトリー内にあるオブジェクトに適用されます。

注:

これらのファイル・システム・セキュリティーの設定は、混合あるいは NTFS のボリュームまたは qtree でのみ適用されます。UNIX のボリュームまたは qtree のファイルおよびディレクトリーには適用されません。

ファイル・システム・セキュリティー ACL の伝搬は、およそ 280 レベルのディレクトリー階層に制限されます。

1. Windows サーバーで、「Active Directory ユーザーおよびコンピュータ (Active Directory Users and Computers)」のツリーを開きます。
2. ストレージ・システムを含む「組織単位 (Organization Unit) (OU)」を右クリックします。
3. 「グループ ポリシー (Group Policy)」タブを選択し、「新規 (New)」を選択します。
4. 新規の GPO の名前を入力します。
5. 新規の GPO をハイライトし、「編集 (Edit)」を選択します。「グループ ポリシー オブジェクト エディター (Group Policy Object Editor)」が表示されます。
6. 「コンピュータの構成 (Computer Configuration)」>「Windows 設定 (Windows Settings)」>「セキュリティー設定 (Security Settings)」をダブルクリックします。
7. 「ファイル システム (File System)」を右クリックし、「ファイルの追加 (Add File)」を選択します。「ファイルまたはフォルダの追加 (Add a file or folder)」ボックスが表示されます。

注: ローカル・サーバーのドライブを表示するためのオプションは選択しないでください。

8. 「フォルダ (Folder)」フィールドで、GPO を適用するストレージ・システム・パスを入力し、「OK」をクリックします。「データベース セキュリティ (Database Security)」ウィンドウが開きます。
9. 「データベース セキュリティ (Database Security)」ウィンドウで、必要なアクセス権を設定し、「OK」をクリックします。「オブジェクトの追加 (Add Object)」ウィンドウが開きます。
10. 「オブジェクトの追加 (Add Object)」ウィンドウで、必要な ACL 継承を選択し、「OK」をクリックします。「グループ ポリシー エディタ (Group Policy Editor)」が、新規のオブジェクト名を表示します。
11. 「グループ ポリシー エディタ (Group Policy Editor)」および「OU プロパティ」ダイアログ・ボックスを閉じます。
12. ストレージ・システムでコマンド `cifs gpupdate` を入力し、新規の GPO の取得および適用を行います。`cifs gpupdate` コマンドを使用して明示的に新規の GPO を適用しない場合は、ストレージ・システムは次に Active Directory サーバーを照会するとき (90 分以内) に新規の GPO を適用します。

現行の GPO およびその効果の表示

ストレージ・システムで現在有効な GPO およびそれらの GPO の結果を `cifs gpresult` コマンドを使用して表示することができます。

このタスクについて

`cifs gpresult` コマンドは、Windows 2000/XP の `gpresult.exe /force` コマンドの出力をシミュレートします。

注: `cifs gpresult` コマンドは、ストレージ・システムおよび現行の Data ONTAP のリリースに関連するグループ・ポリシー設定のみを表示します。

次のコマンドを入力します。`cifs gpresult [-r] [-d] [-v]`

オプション	出力
none	現在ストレージ・システムに適用されている GPO に関する名前、バージョン、および位置を含めた情報を表示します。
-r	現在の GPO をストレージ・システムに適用した結果を表示します。
-v	適用された GPO およびそれらを適用した結果に関する情報を含む、詳細表示を生成します。
-d	<code>cifs gpresult -v</code> からの出力を <code>/etc/ad/gpresult_timestamp</code> ファイルにダンプします。

GPO 設定の更新

Data ONTAP は、90 分ごとに GPO の変更を取得および適用し、16 時間ごとにセキュリティ設定をリフレッシュしますが、`cifs gpupdate` コマンドを入力することで更新を強制的に実行することができます。

このタスクについて

ストレージ・システム上のグループ・ポリシー設定は、以下の方法で更新することができます。

- すべての GPO が 90 分ごとに検証されます。デフォルトでは、Data ONTAP は GPO への変更について Active Directory に照会します。Active Directory に記録されている GPO のバージョン番号がストレージ・システム上の GPO のバージョン番号よりも大きい場合、Data ONTAP は新しい GPO を取得して適用します。バージョン番号が同じ場合は、ストレージ・システム上の GPO は更新されません。
- セキュリティ設定 GPO は、16 時間ごとにリフレッシュされます。Data ONTAP は、これらの GPO に対する変更の有無に関わらず、16 時間ごとにセキュリティ設定 GPO を取得して適用します。

注: 現在の Data ONTAP のバージョンでは、16 時間というデフォルト値を変更することはできません。これは、Windows クライアントのデフォルト設定です。

- Data ONTAP コマンドを使用して、すべての GPO を要求に応じて更新することができます。このコマンドは、Windows 2000/XP の `gpupdate.exe /force` コマンドをシミュレートします。

グループ・ポリシー設定を手動で更新するには、次のコマンドを入力します。`cifs gpupdate`。

GPO 更新問題のトラブルシューティング

例えば `cifs gpupdate` コマンドを発行した後に、Data ONTAP が GPO 設定の適用に成功したことを示すメッセージをコンソールに表示しない場合、`cifs.gpo.trace.enable` オプションを使用してストレージ・システムの GPO 接続に関する診断情報をチェックする必要があります。

このタスクについて

更新されたポリシー設定がストレージ・システム GPO に適用されると、以下と同様なメッセージのうち 1 つあるいは両方がストレージ・システムのコンソールに表示されます。

CIFS GPO System: GPO processing is successfully completed.

CIFS GPO System: GPO Security processing is completed.

1. 次のコマンドを入力して、GPO トレースを有効にします。`options cifs.gpo.trace.enable on`
2. 次のコマンドを入力して、GPO 設定を更新します。`cifs gpupdate`

GPO に関する Active Directory 情報を含んだ以下と同様のメッセージが表示されます。

```
CIFS GPO Trace: Site DN: cn=Default-First-Site-Name,  
cn=sites,CN=Configuration,DC=cifs,DC=lab,DC=company, DC=com.
```

```
CIFS GPO Trace: Domain DN: dc=CIFS,dc=LAB,dc=COMPANY, dc=COM.
```

```
CIFS GPO Trace: Filer DN: cn=user1,ou=gpo_ou,dc=cifs, dc=lab,dc=company,dc=com.
```

```
CIFS GPO Trace: Processing GPO[0]: T_sub.
```

```
CIFS: Warning for server \\LAB-A0: Connection terminated.
```

GPO トレース・メッセージは、GPO トレースがオフにされるまでコンソールおよびメッセージ・ログに書き込まれます。

3. 次のコマンドを入力して、GPO トレースを無効にします。options
cifs.gpo.trace.enable off

ストレージ・システム上の始動およびシャットダウン・スクリプトについて

ストレージ・システム上で GPO が有効になっており、Active Directory ドメインで指定されている場合、Data ONTAP は CIFS を始動またはシャットダウンする際には必ず、始動およびシャットダウン・スクリプトを自動的に実行します。

ストレージ・システムは、ドメイン・コントローラーの sysvol ディレクトリーからスクリプトにアクセスし、これらのファイルを /etc/ad ディレクトリーにローカルに保存します。

注: ストレージ・システムは、開始およびシャットダウン・スクリプトに対して定期的に更新を取得しますが、開始スクリプトは次に CIFS が再始動するまでは適用されません。

/etc/ad ディレクトリーについて

GPO サポートがストレージ・システム上で初めて cifs.gpo.enable オプションによって有効に設定される際に、/etc/ad ディレクトリーが作成されます。

このディレクトリーは、以下のファイルのリポジトリーとして使用されます。

- ドメイン・コントローラーから取得される GPO 開始およびシャットダウン・スクリプト。
- cifs gpresult -d コマンドの出力。

Data ONTAP のパス名に関する構成要件

ターゲットのファイル名あるいはディレクトリー名の書式は、Data ONTAP に認識される必要があり、また絶対形式あるいは相対形式でなければなりません。

以下は、パス名の書式に関する詳細情報です。

- 絶対パス名 — 例えば、/vol/vol0/home

絶対パス名が提供された場合、Data ONTAP は指定したターゲット・ファイルまたはターゲット・ディレクトリー内のファイルに、ファイル・システム・セキュリティ設定を適用します。この例では、設定はストレージ・システムのルート・ボリューム内の /home ディレクトリーに適用されます。

- 相対パス名 — 例えば、/home

相対パス名 (/vol から始まらないあらゆるパス名) が提供された場合、Data ONTAP は指定した要素を含むすべてのターゲット・ファイルまたはターゲット・ディレクトリーに、ファイル・システム・セキュリティ設定を適用します。これは単一のストレージ・システム内の複数の並列ターゲットに対して設定を適用する便利な方法です。この例では、設定は /home ディレクトリーを持つすべての vFiler ユニットに適用されます。

oplock を使用したクライアント・パフォーマンスの改善

oplock (便宜的ロック) によって、特定のファイル共有シナリオにある CIFS クライアントは、先読み、後書き、およびロックの情報のクライアント・サイド・キャッシングを実行することが可能になります。そしてクライアントは、疑わしいファイルへのアクセス権が必要であることを正式にサーバーに指摘することなく、ファイルの読み取りあるいはファイルへの書き込みを行うことができます。これによって、ネットワーク・トラフィックを削減することでパフォーマンスが改善されます。

oplock 使用時の書き込みキャッシュのデータ損失に関する考慮事項

ある環境下で、1 つのプロセスがファイルの排他的 oplock を持っており、2 つめのプロセスがそのファイルのオープンを試行した場合、最初のプロセスはキャッシュ・データを無効にして書き込みおよびロックをフラッシュしなければなりません。クライアントは次に、oplock を解放してからファイルにアクセスする必要があります。このフラッシュの間にネットワーク障害が発生した場合、キャッシュ書き込みデータは失われる可能性があります。

データ損失の可能性: 書き込みキャッシュ・データを持つアプリケーションがある場合、以下の環境が重なるとそのデータが失われる可能性があります。

- ファイルに排他的 oplock を持っている環境。
- oplock の中断またはファイルのクローズのいずれかが求められる環境。
- 書き込みキャッシュのフラッシュ処理中に、ネットワークあるいはターゲット・システムがエラーを生成する環境。

エラー処理および書き込み完了: キャッシュ自体にはエラー処理がなく、アプリケーションが実施します。アプリケーションがキャッシュへの書き込みを行う場合、書き込みは常に完了しています。キャッシュが次々にネットワーク上でターゲット・システムに書き込みを行う場合、書き込みは完了していると仮定されなければなりません。なぜなら、もしそうでない場合はデータ損失が起こるからです。

ストレージ・システム上での oplock の有効化あるいは無効化

ストレージ・システムで oplock を有効にしている場合、個々の qtree で oplock を有効あるいは無効にすることができます。

このタスクについて

ご使用のストレージ・システムでの CIFS oplock は、デフォルトでオンです。

以下のいずれかの環境下で、CIFS oplock をオフにする場合があります。

- 資料が oplock をオフにすることを推奨しているデータベース・アプリケーションを使用している。
- CIFS クライアントが信頼できないネットワーク上にある。
- 重大なデータを取り扱っており、どんなに小さなデータ損失も起こすことができない。

そうでない場合は、CIFS oplock をオンのままにしておくことができます。

ストレージ・システムで CIFS oplock をオンにすることは、どのクライアント固有の設定もオーバーライドしません。ストレージ・システムで CIFS oplock をオフにすることで、ストレージ・システムへの、あるいはストレージ・システムからのすべての oplock を無効にします。Windows のレジストリー設定を使用して、個々のクライアントで CIFS oplock を有効あるいは無効にすることができます。

oplock を有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
ストレージ・システムで oplock を有効にする	次のコマンドを入力します。options cifs.oplocks.enable on
ストレージ・システムで oplock を無効にする	次のコマンドを入力します。options cifs.oplocks.enable off

タスクの結果

cifs.oplocks.enable オプションが on に設定されている場合、qtree ごとの oplock 設定が有効になります。そうでない場合は、qtree ごとの oplock 設定に関わらず、すべての qtree の oplock は無効になります。

qtree での oplock の有効化あるいは無効化

ストレージ・システム・レベルで oplock が有効に設定されている場合、個々の qtree で oplock を有効あるいは無効にすることができます。

以下を実施したい場合、	以下を実行してください。
qtree で oplock を有効にする	次のコマンドを入力します。qtree oplocks qtree_name enable
qtree で oplock を無効にする	次のコマンドを入力します。qtree oplocks qtree_name disable

タスクの結果

cifs.oplocks.enable オプションが on に設定されている場合、qtree の qtree oplocks コマンドは直ちに発効されます。cifs.oplocks.enable オプションが off に設定されている場合、qtree oplocks コマンドはオプションを on に変更するまで発効されません。

oplock 中断の送信に関する遅延時間の変更

ファイル oplock を所有しているクライアントがファイル・オープン要求を送信すると、ストレージ・システムが oplock の中断を要求した場合に発生する可能性がある「競合状態」に対して一時的にぜい弱になります。この状態を避けるために、ストレージ・システムは cifs.oplocks.opendelta オプションによって指定された遅延時間の値 (ミリ秒) によって、oplock 中断の送信を遅らせます。

このタスクについて

デフォルトの遅延時間は 0 ミリ秒です。ご使用のストレージ・システムが、最新の Service Pack なしの Microsoft Windows NT 4.0 および Microsoft Windows NT 3.5.1 を含む古い Windows クライアントをサポートする必要がある場合、Microsoft のサポート技術情報の項目 163525 に記載されているパフォーマンス上の問題を避けるために、このデフォルト値を保持する必要があります。

古いバージョンの Windows が稼働しているクライアントを使用していない場合は、他の値 (例えば 8) を遅延時間に設定することができます。これは、ストレージ・システムがファイル・オープン要求を受信あるいは要求に応答した後、ストレージ・システムはクライアントに oplock 中断を送信する前に 8 ミリ秒が経過していることを確認することを意味します。

cifs stat コマンドを発行して、出力の OpLkBkNoBreakAck フィールドがゼロ以外の値を示した場合、遅延時間を増やす必要があります。

また、以下と同様な syslog メッセージを見た場合も、oplock 中断の送信に関する遅延時間を増やす必要があります。

```
Mon Jan 21 15:18:38 PST [CIFSAdmin:warning]: oplock break timed out to station JOHN-PC
for file ¥¥FILER¥share¥subdir¥file.txt
```

コマンド options cifs.oplocks.opendelta *time* を入力してください。ここで、*time* はミリ秒単位での遅延時間を意味します。cifs.oplocks.opendelta オプションの設定は、開かれたファイルを持っているクライアントへの oplock 中断要求の送信を延期します。この値を 35 より大きく設定することを考慮する場合は、技術サポートに相談する必要があります。

認証およびネットワーク・サービスの管理

このセクションでは、古い NetBIOS プロトコルの管理手順と同様に、ストレージ・システムの認証について説明しています。

認証発行の理解

ストレージ・システムは、UNIX 認証、Windows ワークグループ認証、および Kerberos 認証の 3 つのタイプの認証をサポートします。

UNIX 認証について

UNIX モードを使用すると、認証は `/etc/passwd` ファイル内のエントリーまたは NIS/LDAP ベースの認証、あるいはその両方を使用して実行されます。

UNIX 認証の使用

- パスワードは平文 (暗号化されていない) で送信されます。
- 認証されたユーザーは、固有ではないセキュア・ユーザー ID (SID) を持つ資格情報が与えられます。
- ストレージ・システムは受信したパスワードを、ユーザー・パスワードの hash (アルゴリズム的バリエーション) に対して検証します。パスワードは、ストレージ・システム上には保管されません。

UNIX クライアント認証を提供するために、以下の項目を構成する必要があります。

- クライアント情報が、ストレージ・システムの `/etc/passwd` ファイルにある必要があります。
- クライアント情報が、NIS および LDAP またはそのいずれかに入力されている必要があります。
- Windows クライアントのレジストリーが、非暗号化テキストのパスワードを許可するように変更されている必要があります。

UNIX 認証が非暗号化パスワードを送信するため、Windows クライアントは暗号化なしでパスワードを送信するために、レジストリーの編集が必要です。ストレージ・システムに平文のパスワードを送信するために適切に構成されていないクライアントは、アクセスが拒否されて以下のようなエラー・メッセージが表示される可能性があります。

System error 1240 has occurred.

The account is not authorized to login from this station.

クライアントが UNIX 認証を使用するために、非暗号化テキストのパスワードを有効にするための情報については、Microsoft サポートを参照してください。

Windows ワークグループ認証について

ワークグループ認証はローカルの Windows クライアント・アクセスを許可します。

以下の事実はワークグループ認証に適用されます。

- ドメイン・コントローラーに依存しない
- ストレージ・システム・アクセスを 96 台のローカル・クライアントまでに制限する
- ストレージ・システムの `useradmin` コマンドによって管理される

Kerberos 認証について

Kerberos 認証を使用すると、ご使用のストレージ・システムへの接続時に、クライアントは最高位の可能なセキュリティ・レベルを交渉します。

以下の 2 つのプライマリーのセキュリティ・レベルが選択可能です。

- NT LAN マネージャー (NTLM)、lanman、および netlogon のようなネットワーク・サービスに基づく基本的な (Windows NT-4) セキュリティ
- Windows 2000 Kerberos 実装環境を使用した拡張セキュリティ

注: 拡張セキュリティ機能は、Windows Active Directory ドメインのメンバーになっているクライアントにのみ使用可能です。

ストレージ・システムの最小セキュリティ・レベルの設定

ストレージ・システムの最小セキュリティ・レベル (ストレージ・システムがクライアントから受け入れるセキュリティ・トークンの最小レベル) を設定するには、cifs.LMCompatibilityLevel オプションを設定します。デフォルトでは、このオプションは 1 に設定されています。

次のコマンドを入力します。options cifs.LMCompatibilityLevel *minimum_level*
ここで、*minimum_level* は、以下の表で定義されているように、ストレージ・システムがクライアントから受け入れるセキュリティ・トークンの最小レベルです。

値	説明
1 (デフォルト)	ストレージ・システムは、LM、NTLM、および NTLMv2 セッション・セキュリティを受け入れます。NTLMv2 および Kerberos 認証も受け入れます。
2	ストレージ・システムは、NTLM および NTLMv2 セッション・セキュリティを受け入れます。NTLMv2 および Kerberos 認証も受け入れます。ストレージ・システムは LM 認証を拒否します。
3	ストレージ・システムは、NTLMv2 セッション・セキュリティを受け入れます。NTLMv2 および Kerberos 認証も受け入れます。ストレージ・システムは LM および NTLM 認証を拒否します。
4	ストレージ・システムは NTLMv2 および Kerberos 認証を受け入れます。ストレージ・システムは、LM、NTLM、および NTLMv2 セッション・セキュリティを拒否します。
5	ストレージ・システムは Kerberos 認証のみを受け入れます。

Kerberos パッシブ・リプレイ・アタックの防止

Kerberos リプレイ・キャッシュは、ストレージ・システム上のユーザー認証を短時間保管することで、および認証子が次の Kerberos チケットで再利用されないことを保証することで、パッシブ・リプレイ・アタックを防止します。

以下を実施したい場合、	以下を実行してください。
Kerberos リプレイ・キャッシュを有効にする	次のコマンドを入力します。option kerberos.replay_cache.enable on
Kerberos リプレイ・キャッシュを無効にする	次のコマンドを入力します。option kerberos.replay_cache.enable off

タスクの結果

注: Kerberos 認証子の保管および比較によって、特定のストレージ・システム・ワークロードに関する重大なパフォーマンスのペナルティーを引き起こす可能性があります。この理由から、`kerberos.replay_cache.enable` オプションは、デフォルトでは `off` に設定されています。

ドメイン・コントローラーおよび LDAP サーバーの選択

始動時および以下にリストされているときに、ストレージ・システムは Windows ドメイン・コントローラーを検索します。このセクションでは、いつ、どのようにストレージ・システムがドメイン・コントローラーを検出して選択するかを説明しています。

このタスクについて

ストレージ・システムは、以下のいずれかが当てはまる場合に、ドメイン・コントローラーを検索します。

- ストレージ・システムが始動あるいはリブートされた場合。
- `cifs resetdc` コマンドが発行された場合。
- 最後の検索から 4 時間が経過した場合。

注: Active Directory LDAP サーバーが、同じ条件で検索されます。

ドメイン・コントローラーのディスカバリー・プロセスの理解

ドメイン環境で CIFS を稼働している場合、ストレージ・システムは Internet Control Message Protocol (ICMP) パケットを 4 時間ごとに送信してすべてのドメイン・コントローラーの再ディスカバリーを試行します。そうすることで、現在のドメイン・コントローラーがまだアクセス可能であることを確認し、パケットの往復時間を使用した使用可能なドメイン・コントローラーの優先順位付けをすることを可能にします。

ストレージ・システムが、接続速度が非常に優良なドメイン・コントローラーへのアクセスを失い、接続速度が遅いバックアップ・ドメイン・コントローラーと接続する必要がある場合、より優れた接続を検出するまで、2 分ごとにドメイン・コントローラーの再ディスカバリーを試行します。いったんその接続を検出すると、新規のドメイン・コントローラーに接続し、ディスカバリー・パケットの送信を 4 時間ごとに戻します。

以下の表は、ドメイン・コントローラーのディスカバリー・プロセスおよび優先グループについて記載しています。ストレージ・システムは、優先順位が高いグループにあるすべてのドメイン・コントローラーへの接続が失敗した場合のみ、優先順位が低いグループに進みます。

注: Active Directory 環境では、サイト・メンバーシップは (使用可能な優先ドメイン・コントローラーがない場合に) ストレージ・システムがドメイン・コントローラーを選択する 1 つの基準です。そのため、(ストレージ・システムと同じサイトに含まれるストレージ・システムのサブネット情報を持つ) 適切に構成されたサイ

トおよびサービスを持つことが重要です。

ドメイン・コントローラー・カテゴリー	優先グループ: ドメイン・コントローラーが 選択される順番
Preferred: prefdc リストにあるコントローラー	グループ 1: 優先ドメイン・コントローラーは、prefdc リストに出現するコントローラーの順番で選択されます。
Favored: ストレージ・システムと同じ Active Directory のサイト・メンバーシップを共有するコントローラー (このカテゴリーは Windows NT 環境でのストレージ・システムでは空です。)	グループ 2: 応答の受信が ping されてから 1 秒以内であったドメイン・コントローラーで、応答時間の早い順番に選択されます。 グループ 3: 1 秒以内に応答はなかったが、ストレージ・システムと同じサブネットを共有するドメイン・コントローラー。 グループ 4: ping されてから 1 秒以内に応答がない、すべての非ローカルのドメイン・コントローラー。
Other: サイト・メンバーシップを共有しないコントローラー	グループ 5: 応答の受信が ping されてから 1 秒以内であったドメイン・コントローラーで、応答時間の早い順番に選択されます。 グループ 6: 1 秒以内に応答はなかったが、ストレージ・システムと同じサブネットを共有するドメイン・コントローラー。 グループ 7: ping されてから 1 秒以内に応答がない、すべての非ローカルのドメイン・コントローラー。

注: サイト・メンバーシップは Active Directory に固有のため、Windows NT4 ドメインおよびストレージ・システムが NT4 サーバーとして構成されている混合モードのドメインには「favored」カテゴリーはありません。これらの環境では、ディスクカバリーを通して検出されたすべてのドメイン・コントローラーは「other」カテゴリーに割り当てられます。

優先ドメイン・コントローラーおよび LDAP サーバーのリストの指定

cifs prefdc add コマンドを使用して、優先ドメイン・コントローラーおよび LDAP サーバーのリストを指定することができます。

次のコマンドを入力します。cifs prefdc add *domain address* [*address ...*]

変数	説明
<i>domain</i>	ドメイン・コントローラーあるいは LDAP サーバーを指定したいドメイン。
<i>address</i>	ドメイン・コントローラーあるいは LDAP サーバーの IP アドレス。

lab ドメインのための 2 つの優先ドメイン・コントローラーの指定

lab ドメインのために 2 つの優先ドメイン・コントローラーを指定するには、次のコマンドを入力します。

```
cifs prefdc add lab 10.10.10.10 10.10.10.11
```

注: ストレージ・システムが優先ドメイン・コントローラーあるいは LDAP サーバーの修正されたリストを使用することを強制するには、`cifs resetdc` コマンドを使用します。

prefdc リストからのサーバーの削除

`cifs prefdc delete` コマンドを使用して、サーバーを `prefdc` リストから削除することができます。

このタスクについて

`prefdc` リストからドメインを削除した後、以下の手順のステップ 2 で示しているように、ストレージ・システムの使用可能なドメイン・コントローラー情報を更新するために必ず `cifs resetdc` コマンドを実行する必要があります。 `prefdc` リストが更新されたときには、ストレージ・システムはネットワーク・サービスからのドメイン・コントローラー・ディスカバリー情報を更新しません。ドメイン・コントローラー情報のリセットの失敗は、ストレージ・システムが無効なドメイン・コントローラー (あるいは LDAP サーバー) との接続の確立を試行した場合に、接続が失敗する原因になる可能性があります。

注: ストレージ・システムは再始動時にドメイン・コントローラー・ディスカバリー操作を自動的に実行しません。ストレージ・システムの再始動は、使用可能なドメイン・コントローラーおよび LDAP サーバーのリストを更新しません。

1. コマンド `cifs prefdc delete domain` を入力します。*domain* は、優先ドメイン・コントローラーあるいは LDAP サーバーがあるドメインです。
2. コマンド `cifs resetdc [domain]` を入力します。*domain* は、ステップ 1 で指定したドメインです。

タスクの結果

ストレージ・システムは、逆 `prefdc` リストで指定された順番でドメイン・コントローラーの切断および検索を行います。

prefdc リストからの lab の削除

`prefdc` リストから `lab` を削除するには、次のコマンドを入力します。`cifs prefdc delete lab`

ドメイン・コントローラー接続のトラブルシューティング

潜在的なセキュリティの懸案事項が原因で、ICTM Echo Request (ping) トラフィックにおけるあらゆる増加がドメイン・コントローラー接続状況の変更に関連していることを確認する必要があります。

1. 目撃したあらゆる ICMP パケットが、ストレージ・システムと既知のドメイン・コントローラーの間を往来していることを確認します。既知のドメイン・コントローラーのリストを表示するには、次のコマンドを入力します。`cifs domaininfo`
2. ストレージ・システムがこれらのデバイスに 4 時間ごとに 1 回だけ ping することを確認してください。
3. ping トラフィックがそれよりも頻繁に発生している場合は、ドメイン・コントローラーとの接続のロスを示すメッセージがないか、ログを検索してください。
4. また、一時的に `cifs.trace_dc_connection` オプションを有効にすることで、ストレージ・システム上のすべてのドメイン・コントローラー・アドレス・ディスカバリーおよび接続アクティビティをログに記録することができます。これにより、目撃したパケットとドメイン・コントローラーを再ディスカバリーしたときにストレージ・システムが報告した時間を、相互に関連付けることができます。このオプションに関する使用方法の情報については、`options(1)` のマニュアル・ページを参照してください。

優先ドメイン・コントローラーおよび LDAP サーバーのリストの表示

`cifs prefcdc print` コマンドを使用して、優先ドメイン・コントローラーおよび LDAP サーバーのリストを表示することができます。

コマンド `cifs prefcdc print [domain]` を入力します。*domain* は、ドメイン・コントローラーを表示したいドメインです。ドメインが指定されなかった場合、このコマンドはすべてのドメインに関する優先ドメイン・コントローラーを表示します。

lab ドメインの優先コントローラーおよび LDAP サーバーの表示

lab ドメインの優先コントローラーおよび LDAP サーバーを表示するには、次のコマンドを入力します。`cifs prefcdc print lab`

ドメインとのストレージ・システム接続の復旧

`cifs resetdc` コマンドを使用して、ドメインとのストレージ・システム接続を復旧することができます。

このタスクについて

以下の手順は、ストレージ・システムを現在のドメイン・コントローラーから切断し、ストレージ・システムと優先ドメイン・コントローラーの間の接続を確立します。この手順は、ドメイン・コントローラー・ディスカバリー、使用可能なドメイン・コントローラーのリストの更新を強制的に行います。

注: この手順はまた、LDAP 接続を復旧し、LDAP サーバー・ディスカバリーを実行します。

コマンド `cifs resetdc domain` を入力します。*domain* は、ストレージ・システムを切断するドメインです。これが省略された場合、ストレージ・システムはストレージ・システムがインストールされているドメインから切断します。

lab ドメインのドメイン・コントローラーからのストレージ・システムの切断

lab ドメインのドメイン・コントローラーからストレージ・システムを切断するには、次のコマンドを入力します。cifs resetdc lab

非 Kerberos 環境のストレージにアクセスするための NULL セッションの使用

NULL セッション・アクセスは、ストレージ・システム・データのようなネットワーク・リソースのためのアクセス権を、ローカル・システムで稼働しているクライアント・ベースのサービスに対して提供します。クライアント・プロセスがネットワーク・リソースにアクセスするために「system」アカウントを使用するときに、NULL セッションが発生します。NULL セッション構成は、非 Kerberos 認証に固有です。

ストレージ・システムによる NULL セッション・アクセスの提供方法

NULL セッション共有は認証を要求しないため、NULL セッション・アクセスを要求したクライアントにはストレージ・システムにマッピングされた IP アドレス が必要です。

デフォルトでは、マッピングされていない NULL セッション・クライアントは、共有列挙のような一部の Data ONTAP システム・サービスにはアクセスできますが、あらゆるストレージ・システム・データへのアクセスについては制限されています。

注: Data ONTAP は、cifs.restrict_anonymous オプションによる Windows RestrictAnonymous レジストリー設定値をサポートしています。これにより、マッピングされていない NULL ユーザーが表示あるいはアクセスできるシステム・リソースの範囲をコントロールすることができます。例えば、IPC\$ 共有 (非表示の名前付きパイプ共有) への共有列挙およびアクセスを無効にすることができます。詳細については、options(1) のマニュアル・ページを参照してください。

特に構成がない場合は、NULL セッションを通してストレージ・システム・アクセスを要求するローカル・プロセスを実行しているクライアントは、「everyone」のような非制限のグループのみのメンバーです。選択されたストレージ・システム・リソースへの NULL セッション・アクセスを制限するには、NULL セッション・クライアントが属するグループを作成する方法があります。このグループの作成によって、ストレージ・システム・アクセスの制限を可能にし、明確に NULL セッション・クライアントに適用するストレージ・システム・リソースへのアクセス権を設定することが可能になります。

ファイル・システム共有への NULL ユーザー・アクセスの認可

NULL セッション・クライアントが使用するグループの割り当て、および NULL セッションを使用してデータにアクセスすることを許可されたクライアントがリストされたストレージ・システムのリストに追加するための NULL セッション・クライアントの IP アドレスを記録することで、NULL セッション・クライアントによるストレージ・システム・リソースへのアクセスを許可することができます。

1. `/etc/usermap.cfg` ファイルを開きます。
2. 次のフォーマットを使用して、各 NULL ユーザーのためのエントリーを追加します。IPqual:"" => *unixacct* ここで IPqual は、IP アドレス (ホスト名あるいはドット・フォーマットの数値) あるいはサブネット (IP アドレス + ネットワーク・マスク) のいずれかを指定します。"" は、NULL ユーザーを示します。=> は、マッピングの方向を示します。そして、*unixacct* はマッピングされた NULL ユーザーが所有する、(`/etc/passwd` あるいは NIS からの) UNIX アカウントです。
3. `cifs.mapped_null_user_extra_group` オプションを、NULL セッション・クライアントに使用するグループ名に設定します。
4. NULL セッション・クライアントに適切なアクセス権を許可するために、アクセス権を設定します。

例

```
10.10.20.19:"" => exchuser 192.168.78.0/255.255.255.0:"" => iisuser
```

IP アドレス 10.10.20.19 のクライアントは、ストレージ・システムへの NULL セッション・アクセスが許可されます。NULL ユーザー・アカウントは *exchuser* と呼ばれる UNIX アカウントにマッピングされ、そのアカウントは `/etc/passwd` あるいは NIS データベースに存在している必要があります。

また、192.168.78.0 クラス C サブネットから接続を確立しているすべてのクライアントは、NULL セッション・アクセスを許可されており、UNIX アカウント *iisuser* にマッピングされています。ストレージ・システムへの他の NULL ユーザー接続は許可されていません。

次のタスク

Data ONTAP は、NULL ユーザー・セッションを使用してストレージ・システム・リソースにアクセスすることを許可されたクライアントの IP アドレスを指定するために、`/etc/usermap.cfg` ファイルのマッピング構文を提供します。いったん NULL ユーザーのためのグループを作成すると、ストレージ・システム・リソースに関するアクセス制限、および NULL セッションにのみ適用するリソース・アクセス権を指定することができます。

マッピングされた IP アドレスからストレージ・システムにアクセスしているいずれの NULL ユーザーも、マッピングされたユーザーのアクセス権を認可されます。NULL ユーザーを使用してマッピングされたストレージ・システムへの無許可アクセスを防止するために、適切な予防措置を検討してください。最大の保護のために、ストレージ・システムと NULL ユーザーのストレージ・システム・アクセスを要求するすべてのクライアントを分離したネットワークに置き、IP アドレスの「なりすまし」の可能性を排除します。

Kerberos 環境のストレージにアクセスするためのマシン・アカウントの使用

マシン・アカウントはユーザー・アカウントと同じ Kerberos 認証に従うため、ストレージ・システム上でマッピングされる必要はありません。

このタスクについて

Kerberos を使用して認証されると、「system」アカウントを使用したローカル・プロセスを実行するクライアントは、それらのプロセスをリモート・リソースにアクセスするときにマシン・アカウントに割り当てます。マシン・アカウントはドメイン・コントローラーに登録されたコンピューター名の後にドル記号 (\$) が付いた名前を割り当てられます。

マシン・アカウントによるデータへのアクセスの防止:

デフォルトでは、(他の認証されたユーザーのような) マシン・アカウントは常にデータ共有へのアクセス権を所有しています。ただし、セキュリティ上の理由から、Kerberos が有効にされたクライアント上で稼働しているサービスが CIFS を使用してデータにアクセスすることを防止することをお勧めします。

このタスクについて

注: マシン・アカウントによるデータ共有へのアクセスを無効にすることは、多くのサービス (例えば、オフライン・フォルダーおよびローミング・プロファイル) が失敗する原因になる可能性があります。マシン・アカウント・アクセスを無効にする前に、ストレージ・システム・サービスが必要とする評価を確認してください。

次のコマンドを入力します。 `cifs access -delete share_name -m`

注: IPC\$ 共有 (非表示の名前付きパイプ共有) へのアクセスは、変更することはできず、また常に許可されています。

詳細情報については、`cifs_access(1)` のマニュアル・ページを参照してください。

ストレージ・システムの NetBIOS エイリアスの作成

`cifs.netbios_aliases` オプションの設定、あるいは `/etc/cifs_nbalias.cfg` ファイルの編集によって、NetBIOS エイリアスを作成することができます。

このタスクについて

NetBIOS エイリアスは、ストレージ・システムの代替名です。リストにあるどの名前を使用しても、ストレージ・システムに接続することができます。

`cifs.netbios_aliases` オプションを使用して、コンマ区切りリストとして NetBIOS エイリアスを作成することができます。このリストは、コンマを含めて 255 文字まで許可します。 `/etc/cifs_nbalias.cfg` ファイルは、200 エントリーまで許可します。

コマンド行からの NetBIOS エイリアスの作成

コマンド行から `cifs.netbios_aliases` オプションを設定することで、NetBIOS エイリアスを作成することができます。

1. 次のコマンドを入力します。 `options cifs.netbios_aliases name,...` コンマを含めて 255 文字まで入力できます。

例 `options cifs.netbios_aliases alias1,alias2,alias3`

2. エントリーを処理するには、次のコマンドを入力します。 `cifs nbalias load`

/etc/cifs_nbalias.cfg ファイルでの NetBIOS エイリアスの作成

/etc/cifs_nbalias.cfg ファイルに NetBIOS エイリアスを作成することができます。

このタスクについて

Data ONTAP は、CIFS の始動時に /etc ディレクトリーにデフォルトの cifs_nbalias.cfg ファイルを作成します (ファイルが既に存在していない場合)。このファイルへの変更は、CIFS が始動するときには必ず自動的に処理されます。cifs nbalias load コマンドを使用しても、このファイルへの変更を処理することができます。

1. 編集のために /etc/cifs_nbalias.cfg ファイルを開きます。
2. 1 行に 1 エントリーずつ、/etc/cifs_nbalias.cfg ファイルに NetBIOS エイリアスを入力します。

注: ASCII あるいは Unicode 文字のいずれかを使用して、ファイルに最大 200 までの NetBIOS エイリアスを入力することができます。

3. エントリーを処理するには、次のコマンドを入力します。cifs nbalias load

NetBIOS エイリアスのリストの表示

cifs nbalias コマンドを入力して、NetBIOS エイリアスのリストを表示することができます。

次のコマンドを入力します。cifs nbalias

NetBIOS over TCPの無効化

ご使用の Windows 2000 ネットワークで既に NetBIOS over TCP が無効にされている場合は、cifs.netbios_over_tcp.enable オプションを使用して、ストレージ・システムの NetBIOS over TCP を無効にします。

このタスクについて

NetBIOS over TCP は、Windows 2000 より前の CIFS に使用される標準的なプロトコルです。このプロトコルを使用するためのオプション cifs.netbios_over_tcp.enable は、ストレージ・システム上でデフォルトで有効に設定されています。これは、Windows 2000 の「高度な TCP/IP 設定」タブの「NetBIOS over TCP を有効にする」設定に対応します。

ご使用のストレージ・システム上の NetBIOS over TCP の状況を確認するには、nbtstat(1) のマニュアル・ページに記載されているように、nbtstat コマンドを使用します。

NetBIOS over TCP を無効にするためには、すべてのストレージ・システムは Windows 2000 以降で稼働している必要があります。いったん NetBIOS over TCP を無効にすると、Windows 2000 ドメイン・コントローラーおよびウィルス・スキャナーのみが使用可能です。

注: いったん NetBIOS over TCP を無効にすると、クライアントはシャットダウン・メッセージあるいは vscan (ウィルス・スキャン) 警告のような Data ONTAP の通知メッセージを受信しません。

次のコマンドを入力します。options cifs.netbios_over_tcp.enable off

CIFS 活動の監視

このセクションでは、CIFS セッション活動の監視およびストレージ・システム統計の収集について説明します。

このタスクについて

以下のタイプのセッション情報を表示することができます。

- ストレージ・システム情報、およびオープン共有と各接続ユーザーによって開かれたファイルの数を含むセッション情報の要約。
- 1 つの接続ユーザーあるいはすべての接続ユーザーに関する共有およびファイルの情報 (以下が含まれます)。
 - 指定された接続ユーザーあるいはすべての接続ユーザーによって開かれた共有名
 - 開かれたファイルのアクセス・レベル
 - 指定された接続ユーザーあるいはすべての接続ユーザーに関するセキュリティ情報 (UNIX UID およびそのユーザーが属する UNIX グループおよび Windows グループのリストを含む)

注: セッション情報に表示されるオープン共有の数は、非表示の IPC\$ 共有を含みます。

ユーザーを指定する別の方法

接続されているユーザーのセッション情報を表示する場合、ユーザー名あるいはワークステーションの IP アドレスによってユーザーを指定することができます。さらに、ユーザーが Windows 2000 以前のクライアントからストレージ・システムに接続している場合は、ワークステーション名で指定することもできます。

クライアントは、非認証の NULL セッションで接続する場合があります。このようなセッションは、クライアントが共有を列挙するために使用される場合があります。クライアントがストレージ・システムに接続している NULL セッションのみを所有している場合は、次の状況メッセージが表示されます。

User (or PC) not logged in

セッション情報の要約の表示

cifs sessions コマンドを使用して、セッション情報の要約を表示することができます。

次のコマンドを入力します。cifs sessions

アイドル・セッションのタイムアウト

Data ONTAP がアイドル・セッションを切断する前に経過する時間 (秒単位) を指定することができます。

このタスクについて

ユーザーがストレージ・システム上にオープンなファイルを持っていない場合、セッションはアイドルであると見なされます。デフォルトでは、Data ONTAP はアイドル状態が 30 分経過するとセッションを切断します。

アイドル・セッションが切断されると、次にクライアントがストレージ・システムにアクセスするときに自動的に再接続します。

コマンド `options cifs.idle_timeout time` を入力します。*time* は、秒数です。このオプションの新しい値は直ちに有効になります。

統計のトラッキング

`stats` コマンドを使用して、パフォーマンスをトラッキングするためにシステム統計を表示することができます。

このタスクについて

`stats` コマンドは、CIFS 関連の統計に固有ではありません。統計データを出力する 2 つの `stats` コマンドは、`stats show` (リアルタイムの統計データ) および `stats stop` (時間の範囲を超えて統計をトラッキングする場合) です。(cifs stats コマンドはまだ使用可能であることを注意してください。)

`stats` コマンドによって表示される統計は、カウンターで集計されています。階層名を使用した特定のカウンターに、`object_name:instance_name:counter_name` のようにコンポーネントを使って参照をつけます。例えば、カウンターは `system:system:cifs_ops` と命名されるかもしれません。 `stats list` コマンドを使用して、ストレージ・システム上で使用可能な `object_names`、`instance_names` および `counter_names` を判別します。

`stats show` コマンドの出力は、コマンドを発行した瞬間のストレージ・システムを説明するデータを提供します。時間を超えて統計をトラッキングするには、`stats start` コマンドを使用してトラッキングしたい時間の開始にマークを付け、`stats stop` コマンドを使用して統計データを収集したい時間の最後にマークを付けます。Data ONTAP は `stats stop` コマンドを入力するとすぐに、収集したデータを出力します。

Data ONTAP では、異なる統計を同時にトラッキングするために、`stats start` および `stats stop` コマンドを使用することができます。これを行うためには、`stats start` および `stats stop` コマンドにインスタンス (-i) 引数を付けて入力します。

使用方法および構文に関する詳細情報については、`stats(1)` のマニュアル・ページを参照してください。

1. `stats` コマンドによってトラッキングされているオブジェクトのリストを表示するには、コマンド `stats list objects` を入力します。Data ONTAP は、`stats show object_name` を使用して表示可能なオブジェクトのリストを返します。
2. 統計インスタンスのリストを表示するには、コマンド `stats list instances` を入力します。Data ONTAP は、`stats show` コマンドを使用して表示可能なインスタンスのリストを返します。`stats show` コマンドの出力にフォーカスするためにこれらのインスタンスを使用することができます。

3. 統計カウンターのリストを表示するには、コマンド `stats list counters` を入力します。Data ONTAP は、`stats show` コマンドを使用して表示可能なカウンターのリストを返します。
4. すべてのカウンター、インスタンス、あるいはオブジェクトの説明を受信するには、コマンド `stats explain counters` を入力します。Data ONTAP は、`stats show` コマンドの出力にフォーカスするために使用可能な、すべてのカウンター、インスタンス、およびオブジェクトの説明を返します。

特定の統計の表示

個々の統計をトラッキングするために監視することができるオブジェクト、インスタンス、およびカウンターが一度わかると、それらをコマンド行の引数として使用し、`cifs show` コマンドの出力にフォーカスすることができます。

このタスクについて

詳細情報については、`stats(1)` のマニュアル・ページを参照してください。

コマンド `stats show [[object_name][:instance_name][:counter_name]]` を入力します。Data ONTAP は、要求した特定の統計を返します。

統計照会の保存および再利用

通常に実行する「事前設定された」統計照会を、保管して再利用することができます。事前設定された照会は、次の場所および命名フォーマットで、XML ファイルに保管されます。`/etc/stats/preset/preset_name.xml` 照会の保管および再利用の方法に関する情報については、`stats_preset(5)` のマニュアル・ページを参照してください。

CIFS リソースの制限

いくつかの CIFS リソースへのアクセスは、ご使用のストレージ・システムのメモリーおよび CIFS サービスに使用可能な最大メモリーによって制限されています。

これらのリソースには以下が含まれます。

- 接続
- 共有
- 共有接続
- オープン・ファイル
- ロック・ファイル
- ロック

注: ご使用のストレージ・システムがこれらのカテゴリで十分なリソースを得ることができない場合は、技術サポートにお問い合わせください。

CIFS サービスの管理

このセクションでは、ストレージ・システム上での CIFS サービスの管理について説明しています。

MMC を使用した、選択されたクライアントの切断

MMC を使用して、選択されたクライアントを切断することができます。

始める前に

MMC をストレージ・システムに接続します。

1. 左側のペインで「コンピュータの管理」が選択されていない場合は、選択してください。
2. 「システム ツール」>「共有フォルダ」>「セッション」をダブルクリックしてください。
3. 切断したい各クライアントについて、クライアント名を右クリックし、「セッションを閉じる」を選択し、「OK」をクリックします。あるいは、すべてのクライアントを切断する場合は、「セッション」で右クリックし、「セッションをすべて切断」を選択して「OK」をクリックします。

コマンド行からの選択されたユーザーの切断

コマンド行から選択されたユーザーを切断するには、`cifs terminate` コマンドを使用します。

1. 次のコマンドを入力し、接続されているクライアントのリストを表示します。
`cifs sessions *`
2. 次のコマンドを入力してクライアントを切断します。`cifs terminate`
`client_name_or_IP_address [[-t] time]`

パラメーター	説明
<code>client_name_or_IP_address</code>	ストレージ・システムから切断したいワークステーションの名前あるいは IP アドレス
<code>time</code>	クライアントがストレージ・システムから切断されるまでの分数。 0 を入力するとクライアントは直ちに切断されます。

注: 時間を指定せず、Data ONTAP がクライアントに開かれたファイルを検出した場合は、Data ONTAP はクライアントから切断するまでに待つべき分数をプロンプトに出します。

例: `cifs terminate jsmith-pc -t 5`

タスクの結果

Data ONTAP は、jsmith-pc という名前のワークステーションに対し、ユーザーに切断が差し迫っていることを通知するメッセージを送信します。コマンドを入力した 5 分後に、jsmith-pc はストレージ・システムから切断されます。

ストレージ・システム全体の CIFS の無効化

CIFS サービスの無効化は、リブートを越えて持続しません。CIFS サービスを無効にした後でストレージ・システムをリブートすると、Data ONTAP は自動的に CIFS を再始動します。

1. CIFS サービスを無効にするには、コマンド `cifs terminate [-t time]` を入力します。*time* は、ストレージ・システムがすべてのクライアントを切断し、CIFS サービスを終了するまでの分数です。0 を入力するとコマンドは直ちに実施されます。

注: 引数なしで `cifs terminate` コマンドを入力し、Data ONTAP がいずれかのクライアントに開かれたファイルを検出した場合、Data ONTAP はクライアントから切断するまでに待つべき分数をプロンプトに出します。

例 `cifs terminate -t 5`

2. CIFS がストレージ・システムのリブート後に自動的に開始するのを防ぐために、`/etc/cifsconfig.cfg` ファイルの名前を変更します。

タスクの結果

Data ONTAP は、接続しているすべてのクライアントに対し、ユーザーに切断が差し迫っていることを通知するメッセージを送信します。コマンドを入力した 5 分後に、すべてのクライアントは切断され、ストレージ・システムは CIFS サービスの提供を停止します。

次のタスク

ストレージ・システム全体の CIFS を無効にした後、ほとんどの `cifs` コマンドは無効になります。CIFS を無効にした状態で使用できる `cifs` コマンドは以下のとおりです。

- `cifs prefdc`
- `cifs restart`
- `cifs setup`
- `cifs testdc`

CIFS シャットダウン・メッセージを受信するユーザーの指定

`cifs terminate` コマンドを発行すると、デフォルトで Data ONTAP はすべてのオープン・クライアント接続に対して、いつ CIFS サービスが切断されるかをユーザーに通知するためのメッセージを送信します。デフォルト設定を変更して、Data ONTAP がこれらのメッセージを送信しない、あるいはオープン・ファイルを持つ接続クライアントにのみ送信することができます。

次のコマンドを入力します。 `options cifs.shutdown_msg_level 0 | 1 | 2`

0 を使用すると、CIFS シャットダウン・メッセージは送信されません。

1 を使用すると、オープン・ファイルを持つ接続クライアントにのみメッセージを送信します。

2 を使用すると、すべてのオープン接続にメッセージを送信します。これはデフォルト設定です。

CIFS サービスの再始動

`cifs restart` コマンドを入力することで、CIFS サービスを再始動することができます。

次のコマンドを入力します。 `cifs restart`

タスクの結果

ストレージ・システムはドメイン・コントローラーに接続し、CIFS サービスを再始動します。

ストレージ・システム上のすべてのユーザーへのメッセージ送信

重要なイベントを通知するために、ストレージ・システム上のすべてのユーザーにメッセージを送信することができます。メッセージはユーザーのコンピューター上でアラート・ボックスに表示されます。

このタスクについて

Data ONTAP は、`cifs terminate` コマンドを入力すると接続されているユーザーに自動的にメッセージを送信します。ただし、例えば CIFS サービスを停止せずにメッセージを送信したい場合は、ユーザーにすべてのファイルを閉じるように通知するために、サーバー・マネージャーあるいは Data ONTAP コマンド行を使用してメッセージを送信することができます。

ブロードキャスト・メッセージを受信しないクライアントがある場合があります。以下の制限および前提条件が、この機能に適用されます。

- Windows 95 および Windows for Workgroups のクライアントでは、WinPopup プログラムが構成されている必要があります。
- Windows 2003 および Windows XP Service Pack 2 のクライアントでは、メッセージング・サービスが有効に設定されている必要があります。(デフォルトでは、無効です。)
- ユーザーへのメッセージは、NetBIOS over TCP を使用して接続されている Windows クライアントによってのみ確認することができます。

注: ネットワーク構成も、どのクライアントがブロードキャスト・メッセージを受信するかに影響します。

以下を実施したい場合、	以下を実行してください。
ストレージ・システムに接続しているすべての CIFS ユーザーにメッセージを送信する	次のコマンドを入力します。 <code>cifs broadcast * "message"</code>
ストレージ・システムに接続している特定の CIFS ユーザーにメッセージを送信する	次のコマンドを入力します。 <code>cifs broadcast client_name "message"</code>
特定のボリュームに接続しているすべての CIFS ユーザーにメッセージを送信する	次のコマンドを入力します。 <code>cifs broadcast -v volume "message"</code>

ストレージ・システムの説明の表示および変更

参考になる説明を追加することで、ストレージ・システムをネットワーク上の他のコンピューターを区別することができます。

このタスクについて

ストレージ・システムの説明は、ネットワーク表示を行うときに、コメント欄に表示されます。最初は、ストレージ・システムの説明はありません。説明は最大 48 文字まで可能です。

1. 現在の説明を表示するには、次のコマンドを入力します。 `cifs comment`
2. 説明を変更するには、次のコマンドを入力します。 `cifs comment "description"`

ストレージ・システムのコンピューター・アカウント・パスワードの変更

`cifs changefilerpwd` コマンドは、(Active Directory ドメインあるいは NT4 ドメインのいずれの場合も) ストレージ・システムにドメイン・アカウント・パスワードをすぐに変更することを指示します。 `cifs.weekly_W2K_password_change` オプションが `on` に設定されている場合、Windows Active Directory ドメインに属しているストレージ・システムは週に 1 回、ドメイン・パスワードを変更する必要があります。

このタスクについて

詳細については、`cifs_changepassword(1)` および `options(1)` のマニュアル・ページを参照してください。

1. コマンド `cifs changefilerpwd` を入力します。 ストレージ・システムは、以下のメッセージで応答します。

password change scheduled.

パスワード変更がスケジュールされたので、1 分以内に実行されます。

2. オプションで、コマンド `options cifs.weekly_W2K_password_change on | off` を入力します。 ストレージ・システムが Windows Active Directory ドメインに属している場合、ドメイン・パスワードを週に 1 回変更します。パスワード変更は日曜日の 1:00 a.m 前後に行われます。デフォルトは `off` です。

Windows 管理ツールを使用したファイル管理について

CIFS ファイル・アクセス管理タスクには、Windows 管理ツールを使用することで遂行できるものがあります。

以下の Windows 管理ツールは、Data ONTAP と互換性があります。

- Microsoft 管理コンソール (MMC) が管理する Computer Management スナップ・イン
- およびグループ
- Microsoft Active Directory ユーザーの MMC スナップ・イン
- Microsoft イベント・ビューアー
- Microsoft パフォーマンス・モニター

上に示した Microsoft 管理ツールを使用したストレージ・システムの管理手順は、Windows サーバーの管理手順と同様です。この章の手順は、Windows サーバーの管理と手順が異なる Data ONTAP 管理タスクに関する情報を記載しています。

Windows サーバーの管理ツールで入力したテキストと異なり、Data ONTAP のコマンド行は大/小文字の区別があります。例えば、Windows でボリューム名を指定する場合は、小文字と大文字のいずれでタイプすることも可能です。しかし、Windows ツールでは区別ができないため、TEST と命名された `qtree` と同一のレベルに `Test`

と命名された `qtree` を作成するために、Windows ツールを使用することはできません。Data ONTAP コマンド行からは、これらの 2 つの `qtree` を作成して区別することが可能です。

ご使用のストレージ・システムに NT ユーザー・マネージャーを使用する場合は、以下の制限が NT ユーザー・マネージャーに適用されます。

- ストレージ・システムがローカル・ユーザーをサポートしている場合でも、ローカル・ユーザー・アカウントの作成または削除に User メニュー上で「New Users」コマンドを使用することはできません。
- Policies メニューが無効に設定されている場合でも、いくつかのポリシーはオプションあるいはグループ・メンバーシップからコントロールできます。

以下の NT サーバー・マネージャーの機能は、Data ONTAP では適用されないため、サポートされません。

- サービスの停止および開始
- アラートの宛先の指定

アクセス制御問題のトラブルシューティング

アクセス制御問題をトラブルシューティングする (クライアントあるいはユーザーがストレージ・システム上のファイルへのアクセスを期待に反して許可あるいは拒否された場合に、その理由を判別する) には、`sectrace` コマンドを使用します。

このタスクについて

アクセス権トレース・フィルターの追加

クライアントあるいはユーザーが操作を実行することを、ストレージ・システムがなぜ許可あるいは拒否したのかについて、Data ONTAP がシステム・ログの情報をログに記録するように指示するために、アクセス権トレース・フィルターを追加することができます。

このタスクについて

アクセス権トレース・フィルターの追加は、ストレージ・システムのパフォーマンスにわずかに影響します。そのため、アクセス権トレース・フィルターは、デバッグ目的でのみ追加してください。デバッグが終了したときには、すべてのアクセス権トレース・フィルターを削除する必要があります。さらに、指定したフィルタリングの基準は、Data ONTAP がコンソールに多くの EMS メッセージを送信しないように、可能な限り具体的にする必要があります。

以下の制限に注意する必要があります。

- vFiler ごとに最大 10 個のアクセス権トレース・フィルターを追加できます。
- CIFS 要求についてのみ、アクセス権トレース・フィルターを追加できます。

次のコマンドを入力します。`sectrace add [-ip ip_address] [-ntuser nt_username] [-unixuser unix_username] [-path path_prefix] [-a]`

パラメーター	説明
<i>ip_address</i>	アクセスを試行しているクライアントの IP アドレス。
<i>nt_username</i>	アクセスを試行しているユーザーの Windows NT ユーザー名。
<i>unix_username</i>	アクセスを試行しているユーザーの UNIX ユーザー名。 NT ユーザー名を指定している場合、UNIX ユーザー名を指定することはできません。
<i>path_prefix</i>	アクセスをトレースする対象ファイルのパス名の接頭部。例えば、/vol/vol0/home/ ディレクトリー内の「file」で始まる名前を持つすべてのファイル、例えば /vol/vol0/home/file100 および /vol/vol0/home/file200 など、へのアクセスをトレースするため に、/vol/vol0/home/file を指定します。
<i>-a</i>	ストレージ・システムが、拒否した要求だけではなく許可した要求もトレースする必要があることを示します。

例

以下のコマンドは、Data ONTAP が拒否した IP アドレス 192.168.10.23 のクライアントからのすべてのアクセス要求をトレースするためのアクセス権トレース・フィルターを追加します。

```
sectrace add -ip 192.168.10.23
```

以下のコマンドは、Data ONTAP が許可あるいは拒否した UNIX ユーザー **foo** からパス /vol/vol0/home4 へのすべてのアクセス要求をトレースするためのアクセス権トレース・フィルターを追加します。

```
sectrace add -unixuser foo -path /vol/vol0/home4 -a
```

アクセス権トレース・フィルターの削除

アクセス権トレース・フィルターはストレージ・システムのパフォーマンスに小さい影響があるため、アクセス・エラーのデバッグが終了したときに削除することをお勧めします。

1 つあるいはすべてのアクセス権トレース・フィルターを削除します。

以下を実施したい場合、	以下を実行してください。
すべてのアクセス権トレース・フィルターを削除する	次のコマンドを入力します。sectrace delete all

以下を実施したい場合、	以下を実行してください。
1 つのアクセス権トレース・フィルタを削除する	次のコマンドを入力します。sectrace delete <i>index</i> ここで、<i>index</i> は削除するアクセス権トレース・フィルタのインデックスです。(アクセス権トレース・フィルタを追加するときに、Data ONTAP が 1 から 10 の間でインデックスを割り当てます。)

例: インデックス 1 のアクセス権トレース・フィルタの削除

次のコマンドを入力して、インデックス 1 のアクセス権トレース・フィルタを削除します。sectrace delete 1

アクセス権トレース・フィルタの表示

ストレージ・システムあるいは vFiler 上のアクセス権トレース・フィルタを表示するには、sectrace show コマンドを使用します。

このタスクについて

次のコマンドを入力します。sectrace show [*index*] ここで、*index* は表示するアクセス権トレース・フィルタのインデックスです。(アクセス権トレース・フィルタを追加するときに、Data ONTAP が 1 から 10 の間でインデックスを割り当てます。) インデックスを指定しない場合、Data ONTAP はすべてのアクセス権トレース・フィルタを表示します。

例: すべてのアクセス権トレース・フィルタの表示

ストレージ・システム上のすべてのアクセス権トレース・フィルタを表示するには、次のコマンドを入力します。sectrace show

Data ONTAP は、次のような出力ですべてのアクセス権トレース・フィルタを表示します。

```
Sectrace filter: 1
Hits: 5
Path: /vol/vol1/unix1/file1.txt
NT User: CIFS-DOM\harry
Trace DENY and ALLOW events
Sectrace filter: 2
Hits: 7
IP Addr: 10.30.43.42
Path: /vol/vol1/mixed1/dir1/file1.txt
NT User: CIFS-DOM\chris
Trace DENY and ALLOW events
Sectrace filter: 3
Hits: 1
Path: /vol/vol1/mixed1/file2.txt
NT User: CIFS-DOM\chris
Trace DENY events
```

Data ONTAP がアクセスを許可あるいは拒否した理由の解明

Data ONTAP は、アクセス権トレース・フィルターの基準に触れたときには必ず、コンソールへの EMS メッセージをログに記録します。なぜ Data ONTAP が特定のクライアントあるいはユーザーのアクセスを許可あるいは拒否したかについての詳細情報を取得するには、`sectrace print-status` コマンドを使用します。

このタスクについて

次のコマンドを入力します。`sectrace print-status status_code` ここで、`status_code` は、ストレージ・システムが許可あるいは拒否した要求に関するストレージ・システム・ログの「Status:」タグの値に対応しています。

例: Data ONTAP が特定のユーザーが特定のファイルにアクセスすることを許可あるいは拒否した理由についての詳細情報の取得

Data ONTAP が以下のコンソールへの EMS メッセージをログに記録する原因となった、アクセス権トレース・フィルターを追加したと仮定します。

```
Thu Dec 20 13:06:58 GMT [sectrace.filter.allowed:info]: [sectrace index: 1] Access allowed
because 'Read Control, Read Attributes, Read EA, Read' permission (0x20089) is granted on file or
directory (Access allowed by unix permissions for group) - Status: 1:6047397839364:0:0 - 10.73.9.89
- NT user name: CIFS-DOM\harry - UNIX user name: harry(4096) - Qtree security style is MIXED and
unix permissions are set on file/directory - Path: /vol/vol1/mixed1/file1.txt
```

Data ONTAP が、この特定のユーザーがこの特定のファイルにアクセスすることを許可した理由に関する詳細情報を取得するには、次のコマンドを入力してください。`sectrace print-status 1:6047397839364:0:0`

注: `sectrace print-status` コマンドを呼び出す場合、対応するエラー・メッセージの「Status:」行から状況コードを指定する必要があります。

応答で、Data ONTAP は以下のような詳細情報を提供します。

```
secAccess allowed because 'Traverse' permission is granted on requested path.
- Access allowed by unix permissions for others.
- Access allowed because requested permission is granted on file or directory.
- Access allowed by share-level ACL.
- Access allowed by unix permissions for group.
trace print-status 1:6047397839364:0:0
```

FPolicy の使用

FPolicy を使用して、ストレージ・システムに接続しているパートナー・アプリケーションが、ファイル・アクセス許可を監視および設定することを許可します。

FPolicy の概要

FPolicy の概要には、システム体系、動作の仕方に関する情報、FPolicy の一般的なユース・ケース、様々な FPolicy アプリケーション、および FPolicy の制限についてが含まれます。

FPolicyとは

FPolicy は、パートナー・アプリケーションがファイル・アクセス権を監視あるいは設定するためにご使用のストレージ・システムに接続することを可能にする、Data ONTAP のインフラストラクチャー・コンポーネントです。

FPolicy の構成に基づいてストレージ・システムからクライアントがファイルにアクセスする場合は必ず、パートナー・アプリケーションはファイル・アクセスについて通知されます。これにより、ストレージ・システム 上で作成またはアクセスされたファイルの制限を、パートナーが設定できるようになります。

FPolicy は、ファイル・タイプによるファイル操作の権限を指定するファイル・ポリシーを作成することを許可します。例えば、JPEG および .mp3 のような特定のファイル・タイプが、ストレージ・システム上に保管されることを制限することができます。

FPolicy が Data ONTAP 6.4 で初めて導入されたときは、CIFS プロトコルのみがサポートされていました。NFS プロトコル は、Data ONTAP 7.0 で追加されました。ただし、FPolicy は NFS 固有のイベントであっても、CIFS のライセンスがあることを要求します。

FPolicy は、作成、オープン、名前変更、および削除というような個々のクライアント・システムからの操作要求を、ストレージ・システムがどのように処理するかを決定します。ストレージ・システムは、ポリシー名およびそのポリシーがアクティブかどうかを含めて、FPolicy のプロパティを設定を維持します。これらの FPolicy のプロパティは、ストレージ・システムのコンソール・コマンドを使用して設定できます。

FPolicy インターフェースは、Data ONTAP API (ONTAPI と呼ばれます) であり、分散コンピューティング環境 (DCE) で実行され、リモート・プロシージャー・コール (RPC) を使用します。これらのツールを使用して、外部アプリケーションは FPolicy サーバーとして登録することができます。

FPolicy インターフェースは、プログラマーが個別のプラットフォーム上で稼働している外部アプリケーションから、高度化されたファイル選別機能をストレージ・システムや NearStore システムに実装することを許可します。

FPolicy インターフェースを使用するアプリケーションによって、以下のアクションを実行することができます。

- 1 つ以上の Fpolicy サーバーを 1 つ以上のストレージ・システムに登録する
- ファイルのオープン、作成、あるいは名前変更のようなファイル操作に関する通知を受信する
- 通知を受信したファイルへのアクセスをブロックする

以下のプロトコルは FPolicy によってサポートされます。

- CIFS
- NFS (バージョン 2、バージョン 3、バージョン 4)

以下のフィルターは、FPolicy サーバーによって使用可能です。

- プロトコル

- ボリューム名
- ファイル拡張子
- オフライン・ビット
- 操作

Data ONTAP におけるファイル選別は、次の 2 つの方法で有効にできます。

- 外部のファイル選別ソフトウェアの使用

ファイル選別ソフトウェアは、ファイル選別サーバーとして機能するクライアント上で稼働します。ファイル選別ソフトウェアは、ファイル内容の柔軟なコントロールとフィルタリングを提供します。

注: 最適なパフォーマンスのために、FPolicy サーバーがストレージ・システムと同一のサブネットに存在するように構成することをお勧めします。

- ネイティブ・ファイル・ブロッキングの使用

ストレージ・システム上では、固有のファイル選別ソフトウェアが稼働しています。ネイティブ・ファイル・ブロッキングによって、制限されたファイル・タイプを単純に拒否することができます。

FPolicy の動作

FPolicy サーバーは、NFS および CIFS を使用したクライアントからのアクセスに関する通知を送信するように構成する前に、ストレージ・システムに登録されている必要があります。

FPolicy サーバーをストレージ・システムに登録した後、クライアントがファイルへのアクセスを要求すると、ストレージ・システムは通知に登録しているイベントに関して FPolicy サーバーに通知します。ストレージ・システムは、クライアントの要求時に送信される通知の一部として、クライアント・アクセスに関する情報を FPolicy サーバーに送信します。 FPolicy サーバーに送信された情報は、ファイル名、パス名、クライアント情報、プロトコル情報、およびクライアントに要求された操作を含みます。受信した情報と、FPolicy サーバーの構成に基づいて、FPolicy サーバーはクライアントの要求に応答します。 FPolicy サーバーは、クライアントからの要求を許可するか拒否するかをストレージ・システムに伝達します。

ファイルあるいはディレクトリーの操作を指定し、それらの制限を設置するために、ファイル・ポリシーを使用することができます。ファイルまたはディレクトリーの操作要求 (オープン、書き込み、作成、あるいは名前変更など) を受信すると、Data ONTAP は、操作を許可する前にファイル・ポリシーをチェックします。

ポリシーが、ファイルの拡張子に基づくファイル選別を指定した場合は、ファイル選別サーバーまたはストレージ・システム上でファイル選別が行われます。以下のリストは、ファイル選別に関するこれらの方式を記載しています。

- (外部の選別ソフトウェアを使用している) ファイル選別サーバー: 選別の対象となるファイル選別サーバー、および要求されたファイル操作をストレージ・システムが許可すべきかを決定するためのルールを適用するファイル選別サーバーに、通知が送信されます。次に、ファイル選別サーバーは、要求されたファイル操作を許可するかブロックするかの応答をストレージ・システムに送信します。

- (ネイティブ・ファイル・ブロッキングを使用する) ストレージ・システム: 要求は拒否され、ファイル操作はブロックされます。

関連概念

137 ページの『ネイティブ・ファイル・ブロッキングとは』

ネイティブ・ファイル・ブロッキングを使用すると、監視リストに記載されたすべてのファイルまたはディレクトリーの操作を拒否することが可能です。

FPolicy 処理のフローチャート

フローチャートは、FPolicy の使用モデルの概要を記述しています。

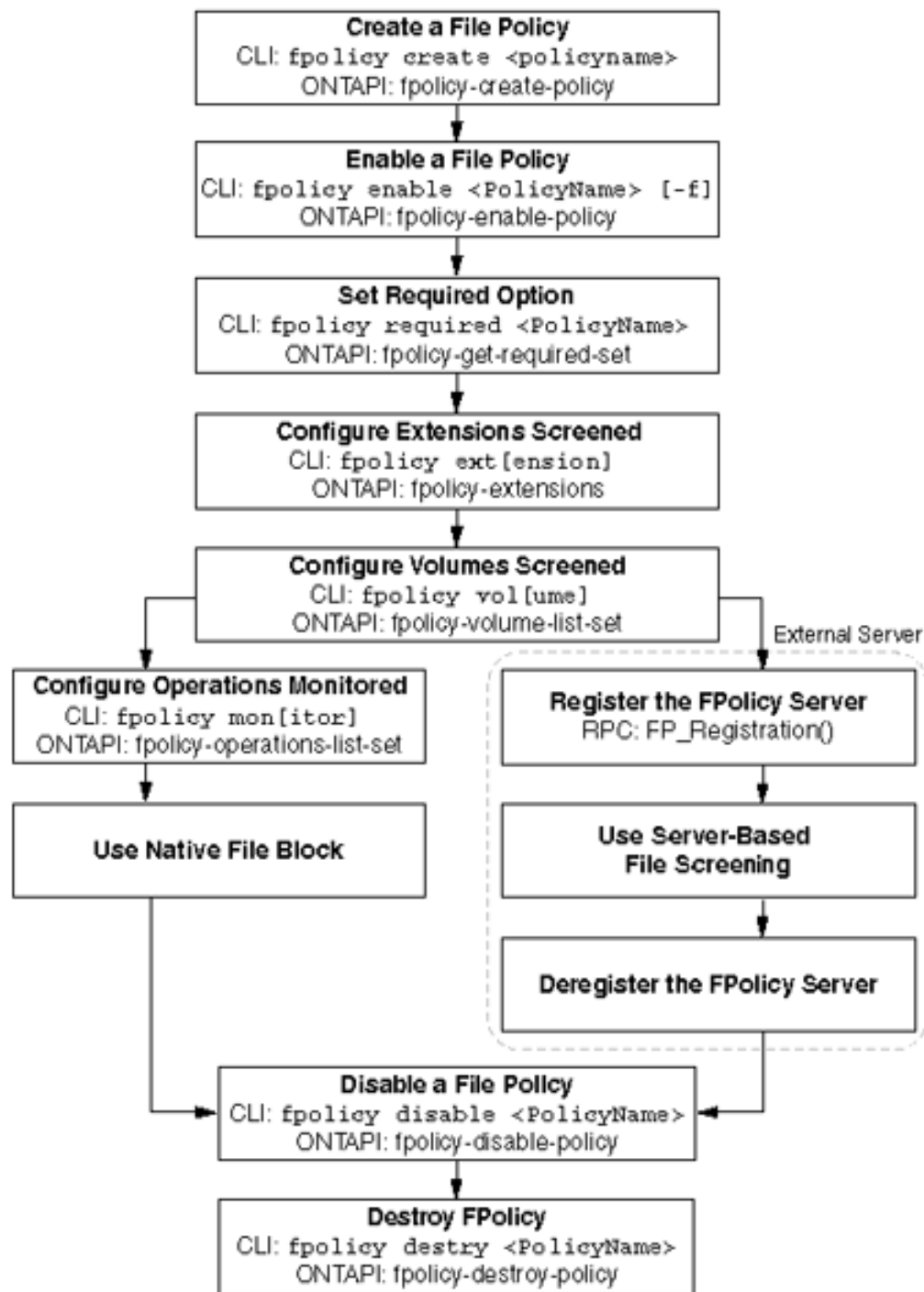


図 1. FPolicy フローチャート

ストレージ環境における FPolicy

クライアントがファイルを要求する場合、要求は Protocol Stack (プロトコル・スタック) に送信されます。 FPolicy 機能が有効になっている場合、プロトコル・スタックは CIFS および NFS 要求を確認し、それらを FPolicy 選別のためにマーク付けします。

その後、要求は WAFL モジュールに送信されます。WAFL モジュールはストレージ・システムからの要求を FPolicy サーバーに転送します。WAFL モジュールは、ファイル要求を FPolicy エンジンに送信します。

FPolicy エンジンは、FPolicy インフラストラクチャー、ONTAPI、および RPC から構成されています。FPolicy エンジンは、要求を RPC コールとして FPolicy サーバーに送信します。FPolicy サーバーが応答を返すと、FPolicy エンジンはクライアント要求に応答します。この応答は、WAFL モジュールに転送され、さらにプロトコル・スタック、クライアントへと順々に転送されます。

ファイル・アクセスが許可されると、クライアントにファイルが提供されます。ファイル・アクセスが拒否された場合は、クライアントに適切な応答が送信されます。CIFS クライアントでは、ファイル・アクセスが拒否された場合、STATUS_ACCESS_DENIED エラー・メッセージが表示されます。

システム体系ダイアグラムは、システム体系全体の概要を規定し、Data ONTAP の様々なレイヤーにおける FPolicy インフラストラクチャーを示します。

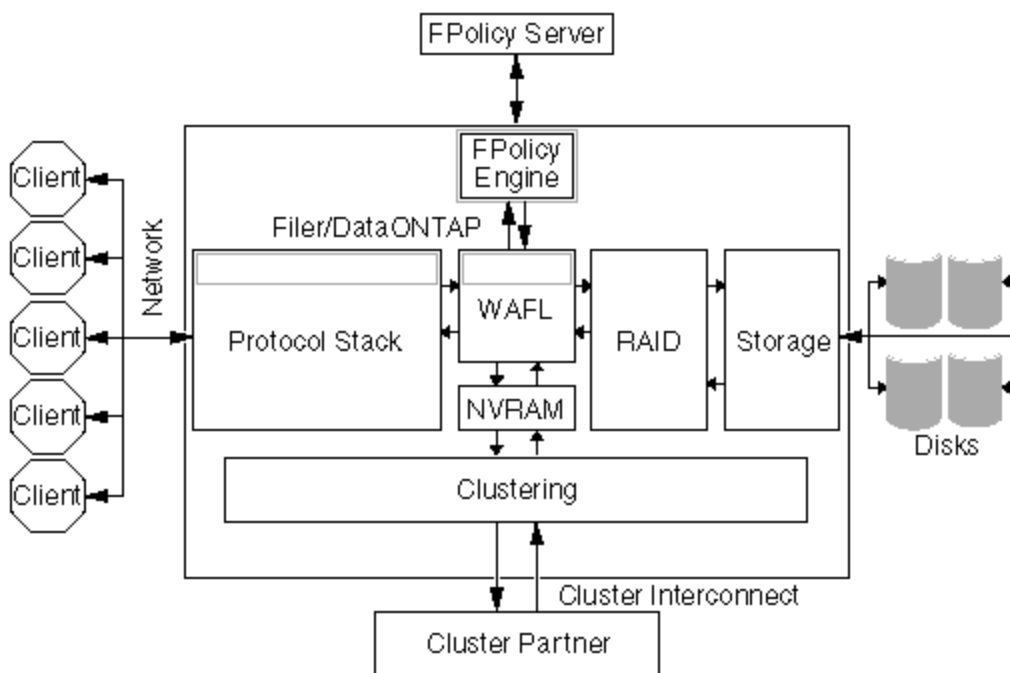


図 2. ストレージ環境における FPolicy

複数サーバーの構成機能

FPolicy は、1 つのポリシーに登録された異なるサーバー間での負荷共有をサポートします。FPolicy は、複数のサーバーを 1 つのポリシーに登録することを許可します。これらのサーバーは、プライマリーまたはセカンダリー・サーバーとして登録可能です。

複数の FPolicy サーバーがプライマリー・サーバーとしてストレージ・システムに登録されている場合、すべての FPolicy 通知は、登録された FPolicy サーバー間で同等に共有されます。通知は、接続されたすべての FPolicy サーバーの負荷共有に応じて送信されます。

使用可能なプライマリー・サーバーがない場合、通知はセカンダリー・サーバー間で共有されます。いったんプライマリー・サーバーが使用可能になると、要求はプライマリー・サーバーに送信され、セカンダリー・サーバーには送信されません。

FPolicy サーバーのいずれか 1 つが、最大未解決要求の制限 (現行では 50) に達した場合は、通知は他のアクティブなサーバーに転送されます。登録されたすべてのサーバーが最大未解決要求のこの制限に達した場合、すべての通知はスロットル・キューで待機させられます。

サーバーは機能タイプに基づいて構成されます。例えば、パススルー読み取り、ファイル・サイズ、および所有者はサーバー・ベースの機能です。これらの機能は、特定のサーバーで有効にされている必要があります。ただし、許可変更の通知、ファイル・パスへの inode、およびオフライン・ビットのような機能は、ポリシー・ワイドな機能です。これは、これらの機能が 1 つのポリシーで有効になっている場合に、機能がポリシーを使用してすべての FPolicy サーバーに更新されることを意味します。

複数サーバーの構成機能の制限は、応答が遅いサーバーと早いサーバーを区別することができないことです。応答が遅いサーバーは、システム全体のパフォーマンスを低下させる可能性があります。

FPolicy サーバーが接続されている場合、この機能は有効です。

FPolicy の制限

FPolicy の制限はプロトコル、選別、および一般の制限に分類できます。

以下は FPolicy のプロトコル制限です。

- FPolicy は、CIFS および NFS プロトコルのみをサポートします。FTP、HTTP、WebDAV、FileIO、などその他のプロトコルはサポートしません。
- CIFS および NFS プロトコルのいくつかの操作は、FPolicy を使用して監視することができません。
- CIFS と NFS の操作は、同一のポリシー上で個別に構成することができません。

以下は、FPolicy の選別の制限です。:

- ファイル選別は、ボリューム全体でセットアップする必要があります。個々の qtree およびディレクトリーは選別することができません。
- FPolicy では ADS を選別できません。
- 複数のサーバーが登録されている場合、接続されているすべてのサーバーのポリシーは、最後に登録したサーバーの設定に基づいて変更します。
- IP アドレスからの FPolicy サーバーは、ストレージ・システムに一度だけ登録できます。1 つのサーバーに関しては、1 つのポリシーのみが構成できます。

- 単一の FPolicy サーバーは、一度に 1 つのポリシーにのみ登録できます。
FPolicy は、同一の IP アドレス から他のポリシーを登録するためのあらゆる要求を拒否します。1 台のクライアントには 1 つの FPolicy サーバーのみが稼働可能です。

Data ONTAP 内での FPolicy の使用

FPolicy は、ストレージ・システム上でのネイティブ・ファイル・ブロッキングに使用できます。

ネイティブ・ファイル・ブロッキングとは

ネイティブ・ファイル・ブロッキングを使用すると、監視リストに記載されたすべてのファイルまたはディレクトリーの操作を拒否することが可能です。

サーバー・ベースのファイル選別によってサポートされるものと同一のフィルターおよびプロトコル設定が、ネイティブ・ファイル・ブロッキングによってもサポートされます。ネイティブ・ファイル・ブロッキング・ポリシー と FPolicy サーバー・ベース・ファイル選別の異なるポリシーを、同時に構成することが可能です。

以下の図は、ネイティブ・ファイル・ブロッキングが有効になっている場合の、クライアント要求の処理を示しています。数値は要求フローの順序を示しています。

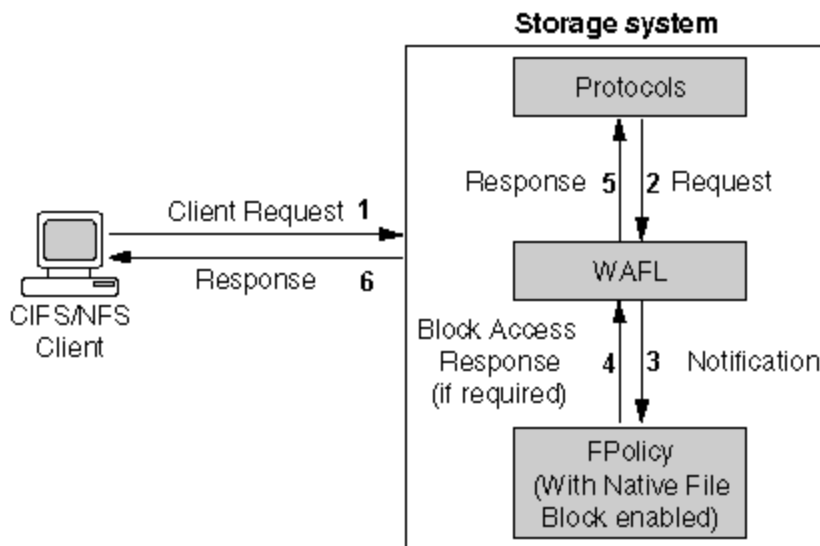


図 3. ネイティブ・ファイル・ブロッキング

CIFS あるいは NFS が要求を発行した場合、ネイティブ・ファイル・ブロッキングが有効になっていると、ファイルはストレージ・システムで選別されます。要求が選別要件と一致した場合、要求は拒否されます。

ネイティブ・ファイル・ブロッキングは、以下の操作上で実行可能です。

- ファイル・オープン
- ファイル作成
- ファイル名変更

- ファイル・クローズ
- ファイル削除
- ファイル読み取り
- ファイル書き込み
- ディレクトリー削除
- ディレクトリー名変更
- ディレクトリー作成
- getattr (NFS のみ)
- Setattr
- ハード・リンクの作成 (NFS のみ)
- シンボリック・リンクの作成 (NFS のみ)
- 検索 (NFS のみ)
- アクセス権変更の通知 (CIFS のみ)
 - 所有者の変更
 - グループの変更
 - システム ACL (SACL) の変更
 - 任意 ACL (DACL) の変更

関連概念

『ネイティブ・ファイル・ブロッキングの使用方法』

ネイティブ・ファイル・ブロッキングを使用するには、まず FPolicy を作成し、次に指定の操作に関する通知を提供するように FPolicy を構成します。ネイティブ・ファイル・ブロッキングの機能は、Data ONTAP によってデフォルトで有効です。

関連資料

140 ページの『CIFS を通して監視されるイベント』

FPolicy は多くの CIFS イベントを監視することができます。

140 ページの『NFS を通して監視されるイベント』

FPolicy は多くの NFS イベントを監視することができます。

ネイティブ・ファイル・ブロッキングの使用方法

ネイティブ・ファイル・ブロッキングを使用するには、まず FPolicy を作成し、次に指定の操作に関する通知を提供するように FPolicy を構成します。ネイティブ・ファイル・ブロッキングの機能は、Data ONTAP によってデフォルトで有効です。

ネイティブ・ファイル・ブロッキングによって、ファイル選別セクションに記載されているあらゆるファイル操作を拒否することが可能です。特定の拡張子を持つファイルへのアクセスをブロックすることが可能です。

例えば、.mp3 拡張子を含むファイルをブロックするには、拡張子が .mp3 のターゲット・ファイルへの指定の操作に関する通知を提供するためのポリシーを構成します。ポリシーは、.mp3 ファイル要求を拒否するように構成します。クライアントが .mp3 拡張子を持つファイルを要求した場合、ストレージ・システムはネイティブ・ファイル・ブロッキング構成に基づいて、ファイルへのアクセスを拒否します。

ネイティブ・ファイル・ブロッキングおよびサーバー・ベースのファイル選別アプリケーションを同時に構成することが可能です。

注: ネイティブ・ファイル・ブロッキングの機能は拡張子に基づくファイル選別のみに、ファイルの内容に基づくファイル選別は行いません。

ネイティブ・ファイル・ブロッキングの構成

ネイティブ・ファイル・ブロッキングを構成するには、ポリシーを作成し、次にブロックするためのファイル拡張子のリストで構成します。

始める前に

CIFS プロトコルが、ライセンス交付を受けて構成されている必要があります。

1. 次の CLI コマンドを使用して、ファイル・ポリシーを作成します。fpolicy create *PolicyName Policytype*

.mp3blocker という名前の選別ポリシーを作成するには、コマンド fpolicy create .mp3blocker screen を入力します。指定したポリシー名を持つ FPolicy が、screen ポリシー・タイプを使用して作成されます。

2. 次のコマンドを使用して、ポリシーに監視される操作およびプロトコルを設定します。fpolicy monitor {add|remove|set} *PolicyName* [-p *protocols*] [-f] *op-spec*

PolicyName は、操作を追加したいポリシーの名前です。

protocols は、監視を有効にしたいプロトコルのセットです。cifs を使用して CIFS 要求を監視し、nfs を使用して NFS 要求を監視し、あるいは cifs,nfs を使用して両方を監視します。

-f オプションは、ポリシーを実行するために使用可能なサーバーがない場合でも、ポリシーを強制的に有効にします。

op-spec は、追加したい操作のリストです。

CIFS および NFS 操作についてのポリシー .mp3blocker の監視操作のリストを置き換えるには、次のコマンドを入力します。fpolicy monitor set .mp3blocker -p cifs,nfs create,rename

create オプションを指定して、.mp3 ファイルの作成を防止します。さらに、.mp3 ファイルが異なる拡張子や名前変更によって絶対にストレージ・システム上にコピーされないようにするために、rename オプションも指定します。この CLI コマンドは、監視する特定の操作を設定します。

3. 次のコマンド構文を使用して、required オプションを on に設定します。
fpolicy options *PolicyType* required on この CLI コマンドは、ファイルがアクセスされる前にファイル選別を必須にします。
4. CLI コマンド fpolicy enable *PolicyType* [-f] を使用して、FPolicy 機能を有効にします。screen は、FPolicy で使用可能な唯一の *PolicyType* です。

FPolicy .mp3blocker を有効にするには、コマンド fpolicy enable .mp3blocker を入力します。この CLI コマンドはファイル・ポリシーを有効にします。

タスクの結果

先の手順の完了時に、クライアントがブロックされたファイルを使用した操作を実行しようとする、操作は失敗し、STATUS_ACCESS_DENIED エラー・コードが送信されます。

関連概念

180 ページの『FPolicy を使用した操作の監視方法』

fpolicy monitor CLI コマンドによって、監視する操作のリストの追加、削除、あるいは設定が可能です。

関連タスク

142 ページの『ファイル・ポリシーの作成』

ファイル・ポリシーをセットアップするためには、最初にファイル・ポリシーを作成する必要があります。ファイル・ポリシーを作成するには、create コマンドを使用します。

143 ページの『必須ファイル選別の指定』

required オプションによって、ファイル選別を必須にするかを決定します。

141 ページの『FPolicy 機能の有効化』

CIFS プロトコルがライセンス交付を受けて構成されている場合、FPolicy はデフォルトで有効です。

CIFS を通して監視されるイベント:

FPolicy は多くの CIFS イベントを監視することができます。

以下の表は、FPolicy が監視することができる CIFS 操作およびそれぞれの操作を FPolicy がどのように処理するかについての要旨を記載しています。

イベント	説明
ファイル・オープン	ファイルが開かれたときに送信される通知
ファイル作成	ファイルが作成されたときに送信される通知
ファイル名変更	ファイル名が変更されたときに送信される通知
ファイル・クローズ	ファイルが閉じられたときに送信される通知
ファイル削除	ファイルが削除されたときに送信される通知
ファイル読み取り	ファイルが読み取られたときに送信される通知
ファイル書き込み	ファイルが変更されたときに送信される通知
ディレクトリー削除	ディレクトリーが削除されたときに送信される通知
ディレクトリー名変更	ディレクトリー名が変更されたときに送信される通知
ディレクトリー作成	ディレクトリーが作成されたときに送信される通知
Setattr	属性情報が設定されたときに送信される通知

NFS を通して監視されるイベント:

FPolicy は多くの NFS イベントを監視することができます。

以下の表は、FPolicy が監視することができる NFS 操作およびそれぞれの操作の要旨を記載しています。

イベント	説明
ファイル・オープン	ファイルが開かれたときに送信される通知
ファイル作成	ファイルが作成されたときに送信される通知
ファイル名変更	ファイル名が変更されたときに送信される通知
ファイル・クローズ	ファイルが閉じられたときに送信される通知
ファイル削除	ファイルが削除されたときに送信される通知
ファイル読み取り	ファイルが読み取られたときに送信される通知
ファイル書き込み	ファイルが変更されたときに送信される通知
ディレクトリー削除	ディレクトリーが削除されたときに送信される通知
ディレクトリー名変更	ディレクトリー名が変更されたときに送信される通知
ディレクトリー作成	ディレクトリーが作成されたときに送信される通知
setattr	属性情報が設定されたときに送信される通知
getattr	属性情報が要求されたときに送信される通知
リンク	ハード・リンクが作成されたときに送信される通知
symlink	シンボリック・リンクが作成されたときに送信される通知
検索	NFS 検索が発生したときに送信される通知

FPolicy の処理方法

CLI コマンドを使用して、FPolicy の作成、FPolicy の有効化、FPolicy の構成、監視操作、およびボリュームと拡張子に基づくファイルの選別が可能です。

FPolicy のセットアップ方法

FPolicy は、単純な CLI コマンドを使用してセットアップすることができます。

FPolicy 機能の有効化:

CIFS プロトコルがライセンス交付を受けて構成されている場合、FPolicy はデフォルトで有効です。

FPolicy 機能を有効にするには、次のコマンドを入力します。options
fpolicy.enable on

タスクの結果

このコマンドを入力すると、FPolicy 機能は有効になります。

FPolicy 機能の無効化:

FPolicy 機能の無効化は、個々のポリシーの有効あるいは無効の設定をオーバーライドし、すべてのポリシーを無効にします。

FPolicy 機能を無効にするには、次のコマンドを入力します。options
fpolicy.enable off

タスクの結果

このコマンドを入力すると、FPolicy 機能は無効になります。

ファイル・ポリシーの作成:

ファイル・ポリシーをセットアップするためには、最初にファイル・ポリシーを作成する必要があります。ファイル・ポリシーを作成するには、`create` コマンドを使用します。

このタスクについて

通知のためのポリシーを構成するには、ファイル・ポリシーを作成します。次に、ファイル・ポリシーは、特定のファイル操作要求あるいはネイティブ・ファイル・ブロッキングについて、FPolicy サーバーに通知を送信するように構成することができます。

`create` コマンドは固有のポリシー名で新規のファイル・ポリシーを作成します。

新規のファイル・ポリシーが作成された後、オプションを設定し、特定の拡張子について選別が必要な要求を決定することができます。

ファイル・ポリシーを作成するには、次のコマンドを入力します。 `fpolicy create PolicyName policytype`

PolicyName は、作成したいポリシーの名前です。ポリシー名は、固有で 80 文字を超えない長さである必要があります。ファイル・ポリシー名は Unicode 英数字で構成することができます。ポリシー名で FPolicy がサポートする特殊文字は、アンダースコア (`_`) のみです。

policytype は、ファイル・ポリシーが属するポリシー・グループです。現在は、FPolicy がサポートするポリシー・タイプは、`screen` のみです。

```
fpolicy create policy1 screen
```

タスクの結果

`screen` ポリシー・タイプを使用して指定されたポリシー名 *policy1* を使用して、ファイル・ポリシーが作成されます。

注: 各 VFiler に最大 20 個まで、同時にファイル・ポリシーを作成することができます。

次のタスク

ファイル・ポリシーが動作して発効するために、作成したファイル・ポリシーを有効に設定します。

関連タスク

141 ページの『FPolicy 機能の有効化』

CIFS プロトコルがライセンス交付を受けて構成されている場合、FPolicy はデフォルトで有効です。

ファイル・ポリシーの有効化:

いったん作成されると、ファイル・ポリシーは通知ポリシーを構成する前に有効にする必要があります。ファイル・ポリシーを有効にするには、`enable` コマンドを使用します。

ファイル・ポリシーを有効にするには、次のコマンドを入力します。 `fpolicy enable PolicyName`

`PolicyName` は、有効にしたいポリシーの名前です。

```
fpolicy enable policy1
```

タスクの結果

指定されたファイル・ポリシーが有効になります。

注: ファイル・ポリシーをアクティブにするするために、`options fpolicy.enable` がオンになっていることを確認してください。

必須ファイル選別の指定:

`required` オプションによって、ファイル選別を必須にするかを決定します。

このタスクについて

`required` オプションが `on` に設定されると、ファイル選別は必須になります。FPolicy サーバーが使用可能でない場合、選別が実行されないため、クライアント要求は拒否されます。このオプションを使用して、ネイティブ・ファイル・ブロッキングも同様に有効にします。

`required` オプションが `off` に設定されていると、ファイル選別は必須ではありません。FPolicy サーバーが接続されていない場合は、操作は選別なしで許可されます。

ファイル選別を必須にするには、コマンド `fpolicy options PolicyName required on` を入力します。 `PolicyName` は、必要なオプションを設定したいポリシーの名前です。

タスクの結果

このオプションは、デフォルトで `off` に設定されています。使用可能なファイル選別サーバーがないときに、ポリシーの `required` オプションをオンにすると、ネイティブ・ファイル・ブロッキング機能が、そのポリシーで指定されているファイルへのアクセスをブロックします。

注: ファイル選別を必須にはしたくない場合は、同じコマンドを `off` に設定します。

関連概念

137 ページの『ネイティブ・ファイル・ブロッキングとは』

ネイティブ・ファイル・ブロッキングを使用すると、監視リストに記載されたすべてのファイルまたはディレクトリーの操作を拒否することが可能です。

ファイル・ポリシーの情報の表示:

特定のファイル・ポリシーの重要情報は、`fpolicy show` コマンドで表示することができます。

次のコマンドを入力します。`fpolicy show PolicyName`
`PolicyName` は、情報を表示したいファイル・ポリシーの名前です。

タスクの結果

`show` コマンドは、特定のファイル・ポリシーに関する以下の情報を表示します。

- ファイル・ポリシーの状況
- 監視されている操作のリスト
- 選別されているボリュームのリスト
- 選別されている拡張子のリスト
- サーバーが接続されている合計時間
- 選別された要求の数
- 拒否された要求の数
- ローカルでブロックされた要求の数

すべてのファイル・ポリシーの情報の表示:

すべてのファイル・ポリシーの重要方法は、`fpolicy` コマンドで表示することができます。

次のコマンドを入力します。`fpolicy`

タスクの結果

`fpolicy show` コマンドは、すべての既存のファイル・ポリシーに関する以下の情報を表示します。

- 登録されている FPolicy サーバーのリスト
- すべてのファイル・ポリシーの状況
- 各ファイル・ポリシーで監視されている操作のリスト
- 各ファイル・ポリシーで選別されているボリュームのリスト
- 各ファイル・ポリシーによって選別されている拡張子のリスト
- サーバーが接続されている合計時間
- 各ファイル・ポリシーで選別された要求の数
- 各ファイル・ポリシーで拒否された要求の数
- ローカルでブロックされた要求の数

ファイル・ポリシーの無効化:

ファイル・ポリシーが無効にされると、その特定のファイル・ポリシーに指定された操作は監視されなくなります。特定のファイル・ポリシーが無効にされた場合、FPolicy サーバーがストレージ・システムに登録されている場合でも、ファイル要求通知は FPolicy サーバーに送信されません。

ファイル・ポリシーを無効にするには、次のコマンドを入力します。 `fpolicy disable PolicyName` `fpolicy disable policy1`

ファイル・ポリシーの破棄:

ファイル・ポリシーの破棄は、既存のファイル・ポリシーを接続されたストレージ・システムから直ちに削除します。

このタスクについて

特定のファイル・ポリシーを破棄あるいは削除するには、`destroy` コマンドを使用します。FPolicy サーバーがファイル・ポリシーに接続されている場合、FPolicy サーバーは登録を取り消されます。

ファイル・ポリシーを破棄し、ファイル・ポリシーのリストから削除するには、次のコマンドを入力します。 `fpolicy destroy PolicyName` `fpolicy destroy policy1` `PolicyName` は、削除したいファイル・ポリシーの名前です。

タスクの結果

このコマンドを入力すると、指定したファイル・ポリシーはポリシーのリストから破棄あるいは削除されます。

注: 破棄されているポリシーが未解決の要求をもっている場合、ポリシーはその未解決の要求が完了するまで破棄されません。

切断された CIFS 要求のサーバー選別の停止:

`cifs_disconnect_check` オプションを有効にすることでセッションが切断された CIFS 要求の選別を、サーバーが停止することを選択することができます。

このタスクについて

重複する要求を除去し、FPolicy サーバーの負荷を削減することができます。

個々のファイル・ポリシーでこの機能を有効にするには、次のコマンドを入力します。 `fpolicy options PolicyName cifs_disconnect_check on` `PolicyName` は、チェックを有効にしたいファイル・ポリシーの名前です。

タスクの結果

注: デフォルトでは、このオプションは `off` に設定されています。

例

ファイル・ポリシー `p1` について `cifs_disconnect_check` を有効にするには、次のコマンドを使用します。

```
filer> fpolicy options p1 cifs_disconnect_check
fpolicy options p1 cifs_disconnect_check: off
filer> fpolicy options p1 cifs_disconnect_check on
```

CIFS 要求の同時選別の制限の設定:

FPolicy サーバーによって同時に選別可能な CIFS 要求の数を制限することができます。このオプションにより、CIFS 要求は絶対に `pBlk` を使い果たさなくなります。

このタスクについて

特定の制限が設定されている場合、制限を超える要求が選別のために FPolicy サーバーに送信されることはありません。

この制限はフラグ `fp_maxcifsreqs_pblkpercent` から設定できます。このフラグは、ストレージ・システム上で使用可能な pBlk の最大数のパーセンテージとして制限を設定します。これを `setflag` および `printflag` コマンドを使用して設定することができます。

注: `setflag` および `printflag` は、診断特権レベルでのみ使用可能です。

選別の制限を設定するには、コマンド `setflag fp_maxcifsreqs_pblkpercent limit_value` を使用します。 `limit_value` は、許可したい同時要求の最大数です。この値は、1 から 100 の範囲で設定する必要があります。

注: 1 から 100 の範囲外の値を設定した場合、この機能は無効になります。

例

制限を設定するには、次のコマンドを入力します。

```
filer> priv set diag
filer*> printflag fp_maxcifsreqs_pblkpercent
fp_maxcifsreqs_pblkpercent = 0
filer*> setflag fp_maxcifsreqs_pblkpercent 30
```

次のタスク

ストレージ・システム上の pBlk の最大数を測定するには、コマンド `cifs stat` を実行します。出力の「Max pBlks」フィールドは、ストレージ・システム上の pBlk の最大数を表示します。

```
filer> cifs stat
...
...
Max pBlks = 256 Current pBlks = 256 Num Logons = 0
```

サーバー・タイムアウトの設定:

要求に対する FPolicy サーバーの応答をシステムがどれぐらいの期間待つかについて、制限を設定することができます。この制限は、各ファイル・ポリシーについて個別に設定することができます。このオプションにより、FPolicy サーバーが進行中であることを確認することができます。

個々のファイル・ポリシーについてのタイムアウト値を設定するには、次のコマンドを入力します。 `fpolicy options PolicyName serverprogress_timeout timeout-in-secs`
`PolicyName` は、FPolicy サーバーのタイムアウトを設定したいファイル・ポリシーの名前です。
`timeout-in-secs` は、タイムアウト値の秒数です。

注: デフォルトでは、このオプションは無効に設定されており、タイムアウト値は設定されていません。

タスクの結果

タイムアウト値が設定された後は、設定されたタイムアウト値までに FPolicy サーバーが応答しない場合、切断されます。

例

ファイル・ポリシー `p1` についてのタイムアウト値を設定するには、次のコマンドを使用します。

```
filer> fpolicy options p1 serverprogress_timeout
fpolicy options p1 serverprogress_timeout: 0 secs (disabled)
filer> fpolicy options p1 serverprogress_timeout 600
```

要求選別のタイムアウトの設定:

要求に対する FPolicy サーバーの選別をシステムがどれぐらいの期間待つかについて、制限を設定することができます。この制限は、各ポリシーについて個別に設定することができます。このオプションは、FPolicy サーバーのパフォーマンスを向上させます。

個々のファイル・ポリシーについてのタイムアウト値を設定するには、次のコマンドを入力します。 `fpolicy options PolicyName reqcancel_timeout timeout-in-secs`

`PolicyName` は、選別のタイムアウトを設定したいファイル・ポリシーの名前です。
`timeout-in-secs` は、タイムアウト値の秒数です。

タスクの結果

タイムアウト値が設定された後は、設定されたタイムアウト値以内に選別要求が完了しない場合は、選別要求は取り消されます。

例

ファイル・ポリシー `p1` についてのタイムアウト値を設定するには、次のコマンドを使用します。

```
filer> fpolicy options p1 reqcancel_timeout
fpolicy options p1 reqcancel_timeout: 0 secs (disabled)
filer> fpolicy options p1 reqcancel_timeout 60
```

NFS および CIFS クライアントに対して選別されたイベント

FPolicy サーバーは、NFS および CIFS クライアントから受信したファイル要求に関する多くの操作あるいはイベントを選別することができます。

以下の表は、ネイティブ・ファイル・ブロッキングおよびサーバー・ベースの選別の両方に関して、NFS および CIFS で選別されるイベントを記載しています。

イベント	プロトコル	説明
ファイル・オープン	CIFS および NFS(v4)	ファイルが開かれたときに送信される通知
ファイル作成	CIFS および NFS	ファイルが作成されたときに送信される通知

イベント	プロトコル	説明
ファイル名変更	CIFS および NFS	ファイル名が変更されたときに送信される通知
ファイル・クローズ	CIFS および NFS(v4)	ファイルが閉じられたときに送信される通知
ファイル削除	CIFS および NFS	ファイルが削除されたときに送信される通知
ファイル読み取り	CIFS および NFS	ファイルが読み取られたときに送信される通知
ファイル書き込み	CIFS および NFS	ファイルが変更されたときに送信される通知
ディレクトリー削除	CIFS および NFS	ディレクトリーが削除されたときに送信される通知
ディレクトリー名変更	CIFS および NFS	ディレクトリー名が変更されたときに送信される通知
ディレクトリー作成	CIFS および NFS	ディレクトリーが作成されたときに送信される通知
getattr	NFS	属性情報の要求に対して送信される通知
setattr	CIFS および NFS	属性情報の設定に対して送信される通知
ハード・リンク作成	NFS	ハード・リンクが作成されたときに送信される通知
シンボリック・リンクの作成	NFS	シンボリック・リンクが作成されたときに送信される通知
検索	NFS	NFS 検索が発生したときに送信される通知

注: CIFS の setattr イベントは様々な機能を実行しますが、セキュリティー記述子情報を変更する setattr 操作のみが FPolicy によって監視されます。セキュリティー記述子情報は、所有者、グループ、任意アクセス制御リスト (**DACL**)、およびシステム・アクセス制御リスト (**SACL**) の情報を含みます。

FPolicy は、NFS および CIFS 操作に関連するほとんどのファイル・システムのイベントをカバーするのに使用できます。FPolicy が監視することができないいくつかの操作を、以下に記載しています。

- NFS (v2、v3、v4) : ACCESS、COMMIT、FSINFO、FSTAT、PATHCONF、ROOT、READLINK、REaddir、REaddirPLUS、STATFS、MKNOD
- FSv4 : ロックおよび委任に関連する操作
- CIFS:
- SMB_COM_TREE_CONNECT および SMB_COM_TREE_DISCONNECT のようなツリー操作
- SMB_COM_SESSION_SETUP_ANDX のような、セッションに関連する操作
- ロックに関連する操作
- プリント関連の操作のような、ファイル・システムのアクティビティーに関連しない操作

ファイルまたはディレクトリーのイベント

様々なファイルおよびディレクトリー操作が選別されます。ポリシーの構成に基づいて、操作要求に関する通知が FPolicy サーバーに送信されます。

ファイル・オープン要求の監視:

FPolicy は、ストレージ・システムからファイル・オープン操作の通知を受信します。

ファイル・オープン要求が CIFS クライアントあるいは NFSv4 クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。この関連するチェックには、アクセス権のチェック、ファイルの可用性のチェック、およびファイルが他のクライアントからアクセスされているかのチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子がファイル・ポリシーの拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。 FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル・オープン要求を許可あるいはブロックします。

ストレージ・システムがリブートすると、NFSv4 クライアントはシャットダウンの前に開かれたファイルのファイル・ハンドルを再要求することができます。ストレージ・システムが機能を取り戻した後、FPolicy サーバーが NFS クライアントの前にストレージ・システムに接続すると、ストレージ・システムはレクラメーション処理ファイルをオープン要求として FPolicy サーバーに転送します。

FPolicy サーバーが NFS クライアントの後にストレージ・システムに接続すると、ストレージ・システムはオープン・レクラメーション処理要求をオープン要求として FPolicy サーバーに転送しません。この場合、NFS クライアントは NFSv4 のレクラメーション処理操作を使用してファイル・ハンドルを手に入れます。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションをオフに設定します。これにより、ボリューム上の inode からパスへのファイル名の変換が可能になります。

注: FPolicy は、NFSv4 プロトコルおよびボリュームでの `i2p` オプションを、Data ONTAP 7.3 リリースからサポートします。それ以前の FPolicy のリリースでは、NFSv4 プロトコルおよび `i2p` オプションはサポートしません。

Data ONTAP ベースのアプリケーションのために NFSv4 環境で FPolicy を稼働させている場合、FPolicy アプリケーションを NFSv4 をサポートするレベルにアップグレードする必要があります。

NFSv4 は、ファイル・オープン (OPEN) およびファイル・クローズ (CLOSE) のイベントのサポートを追加します。そのため、以前のリリースの FPolicy に基づくアプリケーションでは、これらのファイル操作は UNKNOWN イベント・エラーとして FPolicy アプリケーションに現れる可能性があります。

ストレージ・システムからの通知を受信するためには、ファイル・オープン操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル・オープン操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイル・オープン操作を監視するための CLI からの FPolicy の構成:

ファイル・オープン操作を監視するためにファイル・ポリシーを構成するには、`fpolicy monitor add` コマンドを使用します。

ファイル・オープン操作を監視するには、次の CLI コマンドを使用します。
`fpolicy monitor add PolicyName open`

タスクの結果

この CLI コマンドは、ファイル・オープン操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル・オープン操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI 呼び出しを使用して、ファイル・オープン操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・オープン操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。`fpolicy-operations-list-set`

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **file-open** 操作を含む必要があります。**monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル・オープン操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル・オープン要求を監視するための FPolicy の登録:

ファイル・オープン操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル・オープン操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_OPEN 0x0001`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル・オープン要求を監視します。

ファイル作成要求の監視:

FPolicy サーバーは、ストレージ・システムからファイル作成操作の通知を受信します。

ファイル作成要求が CIFS クライアントあるいは NFS クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル作成要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル作成操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル作成操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイル作成操作を監視するための CLI からの FPolicy の構成:

ファイル作成操作を監視するためにファイル・ポリシーを構成するには、`fpolicy monitor add` コマンドを使用します。

ファイル作成操作を監視するには、次の CLI コマンドを使用します。`fpolicy monitor add PolicyName create`

タスクの結果

この CLI コマンドは、ファイル作成操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル作成操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI 呼び出しを使用して、ファイル作成操作を監視するためにファイル・ポリシーを構成することができます。

ファイル作成操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。`fpolicy-operations-list-set`

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **file-create** 操作を含む必要があります。**monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル作成操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル作成要求を監視するための FPolicy の登録:

ファイル作成操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル作成操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_CREATE 0x0002`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル作成要求を監視します。

ファイル・クローズ要求の監視:

FPolicy サーバーは、ストレージ・システムからファイル・クローズ操作の通知を受信します。

ファイル・クローズ要求が CIFS クライアントあるいは NFSv4 クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにある

すべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、要求は FPolicy サーバーに転送されます。ファイルが閉じられた後、ストレージ・システムは FPolicy サーバーにファイルが閉じた通知を送信します。

FPolicy サーバーは、ファイル・クローズ操作をブロックすることはできません。

ストレージ・システムからの通知を受信するためには、ファイル・クローズ操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル・クローズ操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

NFSv4 でのオープン・ダウングレード操作は、クローズ操作とも考えられており、通知はこのような操作について送信されます。

ファイルの拡張子ベースの選別を可能にするには、NFSv4 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

注: Data ONTAP 7.3 リリースから、FPolicy は NFSv4 プロトコルをサポートします。

ファイル・クローズ操作を監視するための CLI からの FPolicy の構成:

`fpolicy monitor add` CLI コマンドを使用して、ファイル・クローズ操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・クローズ操作を監視するには、次の CLI コマンドを使用します。

```
fpolicy monitor add PolicyName close
```

タスクの結果

この CLI コマンドは、ファイル・クローズ操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル・クローズ操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ファイル・クローズ操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・クローズ操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。 `fpolicy-operations-list-set`

タスクの結果

`monitored-operations` の名前入力フィールドで、`monitored-operation-info[]` は `file-close` 操作を含む必要があります。 `monitored-protocols` は、監視したい特定のプロトコルを含む必要があります。ファイル・クローズ操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル・クローズ要求を監視するための FPolicy の登録:

ファイル・クローズ操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル・クローズ操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_CLOSE 0x0008`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル・クローズ要求を監視します。

ファイル名変更要求の監視:

FPolicy サーバーは、ストレージ・システムからファイル名変更操作の通知を受信します。

ファイル名変更要求が CIFS クライアントあるいは NFS クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。

名前変更要求は、新旧いずれかの拡張子が拡張子組み込みリストに記載されている場合のみ、FPolicy サーバーに送信されます。つまり、ファイル名が `test.txt` から `test.mp3` に変更された場合、どちらかあるいは両方の拡張子 (`txt` または `.mp3`) が拡張子組み込みリストに記載されている必要があります。

FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル名変更要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル名変更操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル名変更操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイル名変更操作を監視するための CLI からの FPolicy の構成:

`fpolicy monitor add` CLI コマンドを使用して、ファイル名変更操作を監視します。

ファイル名変更操作を監視するには、次の CLI コマンドを使用します。 `fpolicy monitor add PolicyName rename`

タスクの結果

この CLI コマンドは、ファイル名変更操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル名変更操作を監視するための ONTAPI からの FPolicy の構成:

fpolicy-operations-list-set ONTAPI 呼び出しを使用して、ファイル名変更操作を監視するためにファイル・ポリシーを構成することができます。

ファイル名変更操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、monitored-operation-info[] は *file-rename* 操作を含む必要があります。monitored-protocols は、監視したい特定のプロトコルを含む必要があります。ファイル名変更操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル名変更要求を監視するための FPolicy の登録:

ファイル名変更操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル名変更操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに FP_registration() 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。FS_OP_RENAME 0x0004

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル名変更要求を監視します。

ファイル削除要求の監視:

FPolicy サーバーは、ストレージ・システムからファイル削除操作の通知を受信します。

ファイル削除要求が CIFS クライアントあるいは NFS クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。チェックが完了し、ファイルがチェックにパスすると、要求通知が FPolicy サーバーに送信されます。FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル削除要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル削除操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル削除操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で no_i2p オプションを off に設定します。これにより、ボリューム上の inode からパスへのファイル名の変換が可能になります。

ファイル削除操作を監視するための CLI からの FPolicy の構成:

fpolicy monitor CLI コマンドを使用して、ファイル削除操作を監視します。

ファイル削除操作を監視するには、次の CLI コマンドを使用します。fpolicy
monitor add *PolicyName* delete

タスクの結果

この CLI コマンドは、ファイル削除操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル削除操作を監視するための ONTAPI からの FPolicy の構成:

fpolicy-operations-list-set ONTAPI 呼び出しを使用して、ファイル削除操作を監視します。

ファイル削除操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用することもできます。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **file-delete** 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル削除操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル削除要求を監視するための FPolicy の登録:

ファイル削除操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル削除操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに **FP_registration()** 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 **FS_OP_DELETE 0x0010**

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル削除要求を監視します。

ファイル書き込み要求の監視:

FPolicy サーバーはストレージ・システムからファイル書き込み操作の通知を受信します。

ファイル書き込み要求が CIFS クライアントあるいは NFS クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。

FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル書き込み要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル書き込み操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル書き込み操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

ファイル書き込み操作を監視するための CLI からの FPolicy の構成:

`fpolicy monitor` CLI コマンドを使用して、ファイル書き込み操作を監視します。

ファイル書き込み操作を監視するには、次の CLI コマンドを使用します。`fpolicy monitor add PolicyName write`

タスクの結果

この CLI コマンドは、ファイル書き込み操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル書き込み操作を監視するための ONTAPI からの FPolicy の構成:

`fpolicy-operations-list-set` ONTAPI 呼び出しを使用して、ファイル書き込み操作を監視するためにファイル・ポリシーを構成することができます。

ファイル書き込み操作を監視するには、次の ONTAPI 呼び出しを使用します。`fpolicy-operations-list-set`

タスクの結果

`monitored-operations` の名前入力フィールドで、`monitored-operation-info[]` は `write` 操作を含む必要があります。`monitored-protocols` は、監視したい特定のプロトコルを含む必要があります。ファイル書き込み操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル書き込み要求を監視するための FPolicy の登録:

ファイル書き込み操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル書き込み操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_WRITE 0x4000`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル書き込み要求を監視します。

ファイル読み取り要求の監視:

FPolicy サーバーはストレージ・システムからファイル読み取り操作の通知を受信します。

ファイル読み取り要求が CIFS クライアントあるいは NFS クライアントからストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。

FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル読み取り要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル読み取り操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル読み取り操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

ファイル読み取り操作を監視するための CLI からの FPolicy の構成:

`fpolicy monitor` CLI コマンドを使用して、ファイル読み取り操作を監視します。

ファイル読み取り操作を監視するには、次の CLI コマンドを使用します。`fpolicy monitor add PolicyName read`

タスクの結果

この CLI コマンドは、ファイル読み取り操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ファイル読み取り操作を監視するための ONTAPI からの FPolicy の構成:

`fpolicy-operations-list-set` ONTAPI 呼び出しを使用して、ファイル読み取り操作を監視することができます。

ファイル読み取り操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。`fpolicy-operations-list-set`

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **read** 操作を含む必要があります。**monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル読み取り操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル読み取り要求を監視するための FPolicy の登録:

ファイル読み取り操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル読み取り操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_READ 0x2000`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル読み取り要求を監視します。

リンク要求の監視 (NFS のみ):

FPolicy サーバーはストレージ・システムからファイル・リンク操作の通知を受信します。

ファイル・リンク要求が NFS クライアントによってストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル・リンク要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル・リンク操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル・リンク操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイル・リンク操作を監視するための CLI からの FPolicy の構成:

`fpolicy monitor` CLI コマンドを使用して、ファイル・リンク操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・リンク操作を監視するには、次の CLI コマンドを使用します。`fpolicy monitor add PolicyName link`

タスクの結果

この CLI コマンドは、ファイル・リンク操作を NFS 要求の監視イベントのリストに追加することができます。

ファイル・リンク操作を監視するための ONTAPI からの FPolicy の構成:

`fpolicy-operations-list-set` ONTAPI 呼び出しを使用して、ファイル・リンク操作を監視することができます。

ファイル・リンク操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。`fpolicy-operations-list-set`

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **link** 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル・リンク操作の場合、NFS 要求のみが監視できます。

ファイル・リンク要求を監視するための FPolicy の登録:

ファイル・リンク操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル・リンク操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_LINK 0x0400`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル・リンク要求を監視します。

symlink (シンボリック・リンク) 要求の監視 (NFS のみ):

FPolicy サーバーは、ストレージ・システムからファイル・シンボリック・リンク操作の通知を受信します。

ファイル・シンボリック・リンク要求が NFS クライアントによってストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。 FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル・シンボリック・リンク要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル・シンボリック・リンク操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル・シンボリック・リンク操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

ファイル・シンボリック・リンク操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、ファイル・シンボリック・リンク操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・シンボリック・リンク操作を監視するには、次の CLI コマンドを使用します。fpolicy mon[itor] add *PolicyName* symlink

タスクの結果

この CLI コマンドは、ファイル・シンボリック・リンク操作を NFS 要求の監視イベントのリストに追加することができます。

ファイル・シンボリック・リンク操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ファイル・シンボリック・リンク操作を監視するためにファイル・ポリシーを構成することができます。

ファイル・シンボリック・リンク操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **symlink** 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル・シンボリック・リンク操作の場合、CIFS および NFS 要求の両方が監視できます。

ファイル・シンボリック・リンク要求を監視するための FPolicy の登録:

ファイル・シンボリック・リンク操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル・シンボリック・リンク操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに FP_registration() 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 FS_OP_SYMLINK 0x0800

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル・シンボリック・リンク要求を監視します。

ディレクトリー削除要求の監視:

FPolicy サーバーは、ストレージ・システムからディレクトリー削除操作の通知を受信します。

ディレクトリー削除が、**RMDIR** 操作を使用して CIFS クライアントによって、あるいは **UNLINK** 操作を使用して NFS クライアントによってストレージ・システムに要求されると、ストレージ・システムはディレクトリー上のすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ディレクトリーが使用可能かのチェック、ディレクトリーが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ディレクトリーがチェックをパスした後、要求は FPolicy サーバーに転送されます。ファイル・ポリシーで **required** オプションが **on** にセットされており、ディレクトリー削除操作が要求された場合、要求は拒否されます。

ストレージ・システムからの通知を受信するためには、ディレクトリー削除操作を FPolicy サーバーの監視操作リストに追加する必要があります。ディレクトリー削除操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ディレクトリー削除操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、ディレクトリー削除操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー削除操作を監視するには、次の CLI コマンドを使用します。

```
fpolicy mon[itor] add PolicyName directory-delete
```

タスクの結果

この CLI コマンドは、ディレクトリー削除操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ディレクトリー削除操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ディレクトリー削除操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー削除操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **directory-delete** 操作を含む必要があります。**monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ディレクトリー削除操作の場合、CIFS および NFS 要求の両方が監視できます。

ディレクトリー削除要求を監視するための FPolicy の登録:

ディレクトリー削除操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ディレクトリー削除操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに FP_registration() 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。FS_OP_DELETE_DIR 0x0020

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのディレクトリー削除要求を監視します。

ディレクトリー名変更要求の監視:

FPolicy サーバーは、ストレージ・システムからディレクトリー名変更操作の通知を受信します。

ディレクトリー名変更要求が CIFS あるいは NFS クライアントからストレージ・システムにされると、ストレージ・システムはディレクトリー上のすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ディレクトリーが使用可能かのチェック、ディレクトリーが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ディレクトリーがチェックをパスした後、要求は FPolicy サーバーに転送されます。ファイル・ポリシーで `required` オプションが `on` にセットされており、ディレクトリー名変更操作が要求された場合、要求は拒否されます。

ストレージ・システムからの通知を受信するためには、ディレクトリー名変更操作を FPolicy サーバーの監視操作リストに追加する必要があります。ディレクトリー名変更操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ディレクトリー名変更操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、ディレクトリー名変更操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー名変更操作を監視するには、次の CLI コマンドを使用します。

```
fpolicy mon[itor] add PolicyName directory-rename
```

タスクの結果

この CLI コマンドは、ディレクトリー名変更操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ディレクトリー名変更操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ディレクトリー名変更操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー名変更操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **directory-rename** 操作を含む必要があります。**monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ディレクトリー名変更操作の場合、CIFS および NFS 要求の両方が監視できます。

ディレクトリー名変更要求を監視するための FPolicy の登録:

ディレクトリー名変更操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ディレクトリー名変更操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_RENAME_DIR 0x0040`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのディレクトリー名変更要求を監視します。

ディレクトリー作成要求の監視:

FPolicy サーバーは、ストレージ・システムからディレクトリー作成操作の通知を受信します。

ディレクトリー作成が CIFS あるいは NFS クライアントからストレージ・システムに要求されると、ストレージ・システムはディレクトリー上のすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ディレクトリーが使用可能かのチェック、ディレクトリーが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ディレクトリーがチェックをパスした後、要求は FPolicy サーバーに転送されます。ファイル・ポリシーで `required` オプションが `on` にセットされており、ディレクトリー作成操作が要求された場合、要求は拒否されます。

ストレージ・システムからの通知を受信するためには、ディレクトリー作成操作を FPolicy サーバーの監視操作リストに追加する必要があります。ディレクトリー作成操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ディレクトリー作成操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、ディレクトリー作成操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー作成操作を監視するには、次のコマンドを使用します。fpolicy mon[itor] add *PolicyName* directory-create

タスクの結果

この CLI コマンドは、ディレクトリー作成操作を CIFS および NFS 要求の監視イベント・リストに追加します。

ディレクトリー作成操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ディレクトリー作成操作を監視するためにファイル・ポリシーを構成することができます。

ディレクトリー作成操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **directory-create** 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ディレクトリー作成操作の場合、CIFS および NFS 要求の両方が監視できます。

ディレクトリー作成要求を監視するための FPolicy の登録:

ディレクトリー作成操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ディレクトリー作成操作を選別するには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_CREATE_DIR 0x0080`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのディレクトリー作成要求を監視します。

ファイル検索要求の監視 (NFS のみ):

FPolicy サーバーは、ストレージ・システムからファイル検索操作の通知を受信します。

ファイル検索要求が NFS クライアントによってストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいてファイル検索要求を許可あるいはブロックします。

ストレージ・システムからの通知を受信するためには、ファイル検索操作を FPolicy サーバーの監視操作リストに追加する必要があります。ファイル検索操作は、CLI または ONTAPI を使用して監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイル検索操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、ファイル検索操作を監視するためにファイル・ポリシーを構成することができます。

ファイル検索操作を監視するには、次の CLI コマンドを使用します。 `fpolicy mon[itor] add PolicyName lookup`

ファイル検索操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、ファイル検索操作を監視するためにファイル・ポリシーを構成することができます。

ファイル検索操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。 `fpolicy-operations-list-set`

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は **lookup** 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。ファイル検索操作の場合、NFS 要求のみが監視できます。

ファイル検索要求を監視するための FPolicy の登録:

ファイル検索操作を、FPolicy サーバーの登録時に登録することで監視することができます。

ファイル検索操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_LOOKUP 0x1000`

タスクの結果

登録が完了した後、FPolicy サーバーはすべてのファイル検索要求を監視します。

getattr 要求の監視 (NFS のみ):

FPolicy サーバーは、ストレージ・システムから `getattr` 操作の通知を受信します。

属性の取得 (`getattr`) 要求が NFS クライアントによってストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。

FPolicy サーバーは、この要求を受け取り、ポリシーの構成に基づいて `getattr` 要求を許可あるいはブロックします

ストレージ・システムからの通知を受信するためには、`getattr` 操作を FPolicy サーバーの監視操作リストに追加する必要があります。 `getattr` 操作は、CLI あるいは ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

属性取得操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、属性取得 (`getattr`) 操作を監視するためにファイル・ポリシーを構成することができます。

`getattr` 操作を監視するには、次の CLI コマンドを使用します。 `fpolicy mon[itor] add PolicyName getattr`

タスクの結果

この CLI コマンドは、`getattr` 操作を NFS 要求の監視イベントのリストに追加することができます。

属性取得操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、属性取得 (getattr) 操作を監視するためにファイル・ポリシーを構成することができます。

getattr 操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用することもできます。fpolicy-operations-list-set

タスクの結果

monitored-operations の名前入力フィールドで、**monitored-operation-info[]** は getattr 操作を含む必要があります。 **monitored-protocols** は、監視したい特定のプロトコルを含む必要があります。 getattr 操作の場合、NFS 要求のみが監視できます。

属性取得要求を監視するための FPolicy の登録:

属性取得 (getattr) 操作を、FPolicy サーバーの登録時に登録することで監視することができます。

getattr 操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに FP_registration() 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 FS_OP_GETATTR 0x0100

タスクの結果

登録が完了した後、FPolicy サーバーはすべての getattr 要求を監視します。

setattr 要求の監視:

FPolicy サーバーは、ストレージ・システムから setattr 操作の通知を受信します。

属性の設定 (setattr) 要求が、NFS クライアントによってストレージ・システムにされた場合、ストレージ・システムはそのファイルにあるすべての関連するチェックを実施します。このチェックにはアクセス権のチェック、ファイルが使用可能かのチェック、ファイルが他のクライアントからアクセスされているか、およびその他のチェックが含まれます。ファイルがチェックをパスした後、ファイルの拡張子が FPolicy の拡張子組み込みリストに含まれている場合、要求は FPolicy サーバーに転送されます。 FPolicy サーバーは、この要求を受信し、ポリシーの構成に基づいて setattr 要求を許可あるいはブロックします。

属性の設定 (setattr) 要求が、 NT_TRANSACT_SET_SECURITY_DESC 操作を使用して CIFS クライアントによってストレージ・システムにされると、ストレージ・システムは CIFS クライアントがセキュリティ記述子を変更した場合は setattr 通知を送信します。セキュリティ記述子情報は、所有者、グループ、任意アクセス制御リスト (DACL)、およびシステム・アクセス制御リスト (SACL) の情報を含みます。 Windows ベースの CIFS クライアントが、 NT_TRANSACT_SET_SECURITY_DESC 操作をセキュリティ記述子情報の変更なしでストレージ・システムに送信した場合は、FPolicy サーバーに要求を転送しません。

ストレージ・システムからの通知を受信するためには、setattr 操作を FPolicy サーバーの監視操作リストに追加する必要があります。 setattr 操作は、CLI あるいは

ONTAPI から監視することができます。また、ビット・マスクを使用して、FPolicy サーバーによっても設定することが可能です。

ファイルの拡張子ベースの選別を可能にするには、NFS 操作に関しては、ボリューム上で `no_i2p` オプションを `off` に設定します。これにより、ボリューム上の `inode` からパスへのファイル名の変換が可能になります。

属性設定操作を監視するための CLI からの FPolicy の構成:

CLI コマンドを使用して、属性設定 (`setattr`) 操作を監視するためにファイル・ポリシーを構成することができます。

`setattr` 操作を監視するには、次の CLI コマンドを使用します。 `fpolicy mon[itor] add PolicyName setattr`

タスクの結果

この CLI コマンドは、`setattr` 操作を NFS 要求の監視イベントのリストに追加することができます。

属性設定操作を監視するための ONTAPI からの FPolicy の構成:

ONTAPI を使用して、属性設定 (`setattr`) 操作を監視するためにファイル・ポリシーを構成することができます。

`setattr` 操作の監視オプションを設定するには、次の ONTAPI 呼び出しを使用します。 `fpolicy-operations-list-set`

タスクの結果

`monitored-operations` の名前入力フィールドで、`monitored-operation-info[]` は `setattr` 操作を含む必要があります。 `monitored-protocols` は、監視したい特定のプロトコルを含む必要があります。 `setattr` 操作の場合、NFS 要求のみが監視できます。

属性設定要求を監視するための FPolicy の登録:

FPolicy サーバーを登録するときに、ビット・マスクを使用した属性設定 (`setattr`) 操作を監視することができます。

`setattr` 操作の選別を有効にするには、FPolicy サーバーをストレージ・システムに登録するときに `FP_registration()` 呼び出しの **OpsToScreen** ビット・マスクに、次のビットを設定します。 `FS_OP_SETATTR 0x0200`

タスクの結果

登録が完了した後、FPolicy サーバーはすべての `setattr` 要求を監視します。

ボリュームによる選別

FPolicy は、表示する必要があるボリュームを組み込むあるいは除外することによって、ボリュームの特定のリストにポリシーを制限することを可能にします。

組み込みリストを使用することで、指定されたボリューム・リストに関する通知を要求することが可能です。除外リストを使用することで、指定したボリューム・リストを除くすべてのボリュームに関する通知を要求することが可能です。

注: 組み込みリストと除外リストの両方が設定されている場合、組み込みリストは無視されます。

それぞれのポリシーに対して、異なる組み込みボリュームおよび除外ボリュームを設定することは可能です。

ファイル・ポリシーに関するデフォルトのボリューム・リストは、以下のとおりです。

- すべてのボリュームが組み込みリストに記載されています。
- 除外リストに記載されているボリュームはありません。

除外リストあるいは組み込みリストで以下の操作を実行することが可能です。

- ボリューム・リストをデフォルトのリストにリセットまたは復元します。
- 組み込みリストまたは除外リストのボリュームを表示します。
- ボリュームを組み込みリストまたは除外リストに追加します。
- ボリュームを組み込みリストまたは除外リストから削除します。
- 既存のリストを新規のボリューム・リストに設定または置換します。
- ワイルドカード文字を使用して、ファイル・ポリシーに関するボリュームのリストを表示します。

コマンド行から、組み込みおよび除外ボリュームのリストを表示または変更することが可能です。

ファイル・ボリューム・リストをリセットまたは表示するコマンド構文は、次のとおりです。 `fpolicy vol[ume] {inc[lude]|exc[lude]} {reset|show} PolicyName`

ファイル・ボリュームを処理するコマンド構文は、次のとおりです。 `fpolicy vol[ume] {inc[lude]|exc[lude]} {add| remove|set|eval} PolicyName vol-spec`

`include` は、組み込みリストを変更するために使用します。

`exclude` は、除外リストを変更するために使用します。

`reset` は、ファイル・ボリューム・リストをデフォルトに復元するために使用します。

`show` は、除外リストまたは組み込みリストを入力したように表示するために使用します。

`add` は、除外リストまたは組み込みリストにボリュームを追加するために使用します。

`remove` は、除外リストまたは組み込みリストからボリュームを削除するために使用します。

`set` は、既存のリストを新規のボリューム・リストに置換するために使用します。

`eval` は、ワイルドカード文字を使用して、ファイル・ポリシーに関するボリュームのリストを表示するために使用します。

`PolicyName` は、ファイル・ポリシーの名前です。

`vol-spec` は、変更したいボリューム・リストの名前です。

ボリュームを使用した選別に関するワイルドカード情報:

ボリュームを指定するのに、疑問符 (?) あるいはアスタリスク (*) ワイルドカード文字を使用することができます。

疑問符 (?) ワイルドカード文字は、単一の文字を意味します。例えば、`vol1`、`vol2`、`vol23`、`vol14` を含むボリュームのリストで `vol?` を入力すると、`vol1` および `vol2` に一致します。

アスタリスク (*) ワイルドカード文字は、特定の文字列を含むあらゆる数の文字を意味します。ファイル選別から除外するためにボリュームのリストで `*test*` を入力すると、`test_vol` や `vol_test` のような文字列を含むすべてのボリュームが除外されます。

ボリュームのリストの表示方法:

ファイル・ポリシーについて組み込みあるいは除外を指定したボリュームのリストを表示するには、`show` または `eval` コマンドを使用します。

`show` コマンドを使用したボリュームの表示:

`show` コマンドを使用して、指定されたボリュームのリストを表示することができます。

このタスクについて

`fpolicy volume` コマンドの `show` コマンドは、コマンド行で入力したとおりに、指定されたボリュームのリストを表示します。ワイルドカード文字を使用してボリュームのセットを指定した場合、`show` コマンドを入力したワイルドカード文字を表示します。例えば、`vol*` を表示します。

ファイル・ポリシーのための指定した除外ボリューム・リストを表示するには、次のコマンドを入力します。 `fpolicy vol[ume] exc[lude] show PolicyName`

タスクの結果

このコマンドを入力すると、Data ONTAP は指定したファイルに関する除外リストからのエントリーのリストで応答します。これは、ボリューム名およびボリュームのセットを表すワイルドカード文字 (例えば `vol*`) を含む場合があります。

注: ファイル選別のための組み込みファイル・リストからボリュームを表示したい場合は、`include (inc)` オプションを `exclude (exc)` オプションの代わりに使用します。

`eval` コマンドを使用したボリュームの表示:

eval コマンドを使用して、指定されたボリュームのリストを表示することができます。

このタスクについて

fpolicy volume コマンドの eval コマンドは、入力したリストに含まれるワイルドカード文字を評価し、指定されたボリュームを表示します。例えば、リストが vol* を含む場合、eval コマンドは、vol1、vol22、あるいは vol_sales のように、文字列 vol を含むすべてのボリュームをリスト表示します。

ワイルドカード文字を評価して、ファイル・ポリシーのための除外ボリューム・リストを表示するには、次のコマンドを入力します。 fpolicy vol[ume] exc[lude]
eval *PolicyName*

タスクの結果

このコマンドを入力すると、Data ONTAP はワイルドカード文字を評価して、指定したファイルに関する除外リストからボリュームのリストを応答します。例えば、vol* を入力した場合、eval は例えば vol1、vol22、あるいは vol_sales のような文字列 vol を含むすべてのボリュームを表示します。

注: ファイル選別に組み込まれるファイルのリストを表示するために eval コマンドを使用するには、exclude (exc) オプションの代わりに include (inc) オプションを使用します。

リストへのボリュームの追加方法:

組み込みボリューム・リストあるいは除外ボリューム・リストにボリュームを追加することができます。

組み込みリストへのボリュームの追加:

fpolicy volume include add CLI コマンドを使用して、組み込みボリューム・リストにボリュームを追加します。

ファイル・ポリシーのための選別されるボリュームの組み込みリストにボリュームを追加するには、次のコマンドを入力します。 fpolicy volume include add
PolicyName vol-spec

タスクの結果

組み込みリストに追加したボリューム内のファイルは、そのポリシーが有効になっている場合は常にファイル選別サーバーによって選別されます。

例

選別されるボリュームのリストに、vol1、vol2、vol3 を組み込むには、次のコマンドを入力します。 fpolicy vol inc add imagescreen vol1,vol2,vol3

ボリュームが追加された後、ポリシー *imagescreen* はボリューム vol1、vol2、vol3 で選別を実行します。

除外リストへのボリュームの追加:

fpolicy volume exclude add CLI コマンドを使用して、除外ボリューム・リストにボリュームを追加することができます。

ファイル・ポリシーのための選別されるボリュームの除外リストにボリュームを追加するには、次のコマンドを入力します。 fpolicy volume exclude add
PolicyName vol-spec

タスクの結果

除外リストに追加したボリューム内のファイルは、(他の有効なファイル選別ポリシーとの矛盾がなければ) そのポリシーが有効になっている場合は、ファイル選別サーバーによって選別されません。

例

選別されるボリュームの除外リストに vol4、vol5、vol6 を追加するには、次のコマンドを入力します。fpolicy vol exc add default vol4,vol5,vol6

ボリュームがリストに追加されると、変更されたデフォルトのポリシーはボリューム vol4、vol5、および vol6 でのファイル選別を実行しません。

リストからのボリュームの削除方法:

組み込みボリューム・リストあるいは除外ボリューム・リストからボリュームを削除することができます。

組み込みリストからのボリュームの削除:

fpolicy volume include remove CLI コマンドを使用して、組み込みボリューム・リストからボリュームを削除することができます。

ファイル選別ポリシーのための組み込みボリューム・リストからボリュームを削除するには、次のコマンドを入力します。 fpolicy volume include remove
PolicyName vol-spec

fpolicy volume include remove default vol4

ボリューム名 vol4 にあるファイルは選別されません。

除外リストからのボリュームの削除:

fpolicy volume exclude remove CLI コマンドを使用して、除外ボリューム・リストからボリュームを削除することができます。

ファイル選別ポリシーのための除外ボリューム・リストからボリュームを削除するには、次のコマンドを入力します。 fpolicy vol[ume] exc[lude] remove
PolicyName vol-spec

fpolicy volume exclude remove default vol4

これにより、vol4 は選別から除外されるボリュームのリストから削除されます。ボリューム vol4 にあるファイルは、組み込みリストで指定されたボリュームがない場合にのみ選別されます (例えば、組み込みリストがどのボリュームも指定していない場合、ボリューム vol4 を含めたすべてのボリュームが選別されます)。しかし、他のボリュームが組み込みリストで指定されている場合は、ボリューム vol4 は選別

されません (例えば、組み込みリストがボリューム *vol1* を指定している場合は、*vol1* のみが選別され、*vol4* を含めた他のボリュームは選別されません)。

タスクの結果

注: ファイル選別に組み込まれるファイルのリストから特定のボリュームを削除したい場合は、`exclude (exc)` オプションの代わりに `include (inc)` オプションを使用します。

ボリュームのリストの指定または置換の方法:

組み込みリストおよび除外リストを指定または置換します。

組み込みボリューム・リストの設定:

`fpolicy volume include set` CLI コマンドを使用して、組み込みボリューム・リストを設定することができます。

ファイル・ポリシーのためのボリューム組み込みリスト全体を設定あるいは置換するには、次のコマンドを入力します。 `fpolicy volume include set PolicyName vol-spec`

このコマンドで入力した新規のボリューム・リストが、既存の組み込みボリューム・リストを置き換えて、新規のボリュームのみが選別に組み込まれます。

タスクの結果

注: `set` オプションを使用して、組み込みリストをオフ (ボリューム無し) にします。例えば、次のコマンドを入力します。 `fpolicy vol inc set PolicyName ""` ただし、これはポリシーを無効に設定することと同じ効果があります。

除外ボリューム・リストの設定:

`fpolicy volume exclude set` CLI コマンドを使用して、除外ボリューム・リストを設定することができます。

ファイル・ポリシーのためのボリューム除外リスト全体を設定あるいは置換するには、次のコマンドを入力します。 `fpolicy volume exclude set PolicyName vol-spec`

このコマンドで入力した新規のボリューム・リストが、既存の除外ボリューム・リストを置き換えて、新規のボリュームのみが選別から除外されます。

リスト内のボリュームのリセット方法:

組み込みボリューム・リストあるいは除外ボリューム・リスト内のボリュームを指定または置換することができます。

組み込みボリューム・リストのリセット:

`fpolicy volume include reset` CLI コマンドを使用して、組み込みボリューム・リストをリセットすることができます。

ファイル・ポリシーのための組み込みリストからすべてのエントリーをデフォルト値にリセットするには、次のコマンドを入力します。: `fpolicy volume include`

`reset PolicyName`

このコマンドは、組み込みリストのすべてのエントリーをリセットします。つまり、組み込みリストにリストされているすべてのボリュームが削除されます。

除外ボリューム・リストのリセット:

CLI コマンドを使用して、除外ボリューム・リストをリセットすることができます。

ファイル・ポリシーのための除外リストからすべてのエントリーをデフォルト値にリセットするには、次のコマンドを入力します。 `fpolicy vol[ume] exc[lude]`

`reset PolicyName`

タスクの結果

ここで、除外リストにリストされているすべてのボリュームが削除されます。

拡張子による選別

FPolicy は、表示する必要がある拡張子を組み込むあるいは除外することによって、ファイル拡張子の特定のリストにポリシーを制限することを可能にします。

組み込みリストを使用することで、指定したファイル拡張子に関する通知を要求することが可能です。

組み込みリストと除外リストの両方を提供することが可能です。拡張子は最初に除外リストでチェックされます。要求されたファイルの拡張子が除外リストにない場合、組み込みリストがチェックされます。ファイル拡張子が組み込みリストにある場合、ファイルが選別されます。ファイル拡張子が組み込みリストにない場合は、要求は選別なしで許可されます。

注: 選別がサポートされるファイル名拡張子の最大長は、260 文字です。

拡張子による選別は、ファイル名の最後のピリオド (.) の後にある文字のみに基づきます。例えば、`file1.txt.name.jpg` という名前のファイルの場合、ファイル・ポリシーが `.jpg` 拡張子について構成されている場合にのみファイル・アクセス通知は行われます。

拡張子による選別機能はポリシー・ベースです。そのため、異なるポリシーには異なる拡張子を指定することが可能です。

以下は、ファイル・ポリシーに関するデフォルトの拡張子リストです。

- すべてのファイル拡張子が組み込みリストに記載されています。
- 除外リストに記載されているファイル拡張子はありません。

除外リストあるいは組み込みリストで以下の操作を実行することが可能です。

- 拡張子リストをデフォルトのリストにリセットまたは復元します。
- 既存のリストを新規の拡張子リストに設定または置換します。
- 拡張子を組み込みリストまたは除外リストに追加します。
- 拡張子を組み込みリストまたは除外リストから削除します。
- 組み込みリストまたは除外リストの拡張子を表示します。

- ワイルドカード文字を使用して、ファイル・ポリシーに関する拡張子のリストを表示します。

コマンド行から、組み込みおよび除外拡張子のリストを表示または変更することが可能です。

ファイル拡張子リストをリセットまたは表示するコマンド構文は、次のとおりです。`fpolicy extensions { include | exclude } { reset | show } PolicyName`

ファイル拡張子処理するコマンド構文は、次のとおりです。`fpolicy extensions { include | exclude } { set | add | remove } PolicyName ext-list`

`include` は、組み込みリストを変更するために使用します。

`exclude` は、除外リストを変更するために使用します。

`reset` は、ファイル拡張子リストをデフォルトに復元するために使用します。

`show` は、除外リストまたは組み込みリストを入力したように表示するために使用します。

`set` は、既存のリストを新規の拡張子リストに置換するために使用します。

`add` は、除外リストまたは組み込みリストに拡張子を追加するために使用します。

`remove` は、除外リストまたは組み込みリストから拡張子を削除するために使用します。

`PolicyName` は、ファイル・ポリシーの名前です。

`ext-list` は、変更したい拡張子のリストです。

拡張子による選別に関するワイルドカード情報:

拡張子を指定するのに、疑問符 (?) ワイルドカードを使用することができます。

疑問符 (?) ワイルドカード文字が文字列の先頭に使用されている場合、一文字であることを意味します。文字列の最後に使用されている場合、あらゆる文字数を意味します。

例:

- ファイル選別に組み込むためのファイル拡張子のリストに `?s` を入力した場合、`s` で終わるすべての 2 文字のファイル拡張子を含みます (例えば、`as` および `js` 拡張子)。
- ファイル選別に組み込むためのファイル拡張子のリストに `??m` を入力した場合、`m` で終わるすべての 3 文字のファイル拡張子を含みます (例えば、`htm` および `vtm` 拡張子)。
- ファイル選別に組み込むためのファイル拡張子のリストに `j?` を入力した場合、`j` で始まるすべてのファイル拡張子を含みます (例えば、`js`、`jpg`、および `jpe` 拡張子)。

拡張子のリストの表示方法:

fpolicy extensions CLI コマンドを使用して、組み込みおよび除外拡張子のリストを表示することができます。

組み込みリスト内の拡張子のリストの表示:

fpolicy extensions include show CLI コマンドを使用して、組み込み拡張子リスト内の拡張子のリストを表示することができます。

ファイル・ポリシーのための組み込みファイル拡張子のリストを表示するには、次のコマンドを入力します。 fpolicy extensions include show *PolicyName*

タスクの結果

このコマンドを入力すると、Data ONTAP が、指定したファイルに関する組み込みリストからの拡張子のリストで応答します。

除外リスト内の拡張子のリストの表示:

fpolicy extensions exclude show CLI コマンドを使用して、除外拡張子リスト内の拡張子のリストを表示することができます。

ファイル・ポリシーのための除外ファイル拡張子のリストを表示するには、次のコマンドを入力します。 fpolicy extensions exclude show *PolicyName*

タスクの結果

このコマンドを入力すると、Data ONTAP が、指定したファイルに関する除外リストからの拡張子のリストで応答します。

リストへの拡張子の追加方法:

fpolicy extensions CLI コマンドを使用して、組み込みおよび除外拡張子のリストに拡張子を追加することができます。

組み込みリストへの拡張子の追加:

fpolicy extensions include CLI コマンドを使用して、組み込み拡張子リストに拡張子を追加します。

ファイル・ポリシーのための選別されるファイル拡張子のリストにファイル拡張子を追加するには、次のコマンドを入力します。 fpolicy extensions include add *PolicyName ext-list* fpolicy ext inc add *imagescreen jpg,gif,bmp*
拡張子がリストに追加された後、ポリシー *imagescreen* は、ファイル拡張子 .jpg、.gif、あるいは .bmp を持つあらゆるファイルの選別を実行します。

タスクの結果

組み込みリストに追加したファイル拡張子は、ポリシーが有効になっている場合は常にファイル選別サーバーによって選別されます。

除外リストへの拡張子の追加:

fpolicy extensions exclude CLI コマンドを使用して、除外拡張子リストに拡張子を追加することができます。

ファイル・ポリシーのためのファイル選別から除外されるファイル拡張子のリストにファイル拡張子を追加するには、次のコマンドを入力します。 `fpolicy extensions exclude add PolicyName ext-list fpolicy ext exc add default txt,log,hlp`

リストに拡張子が追加されると、ファイル選別サーバーによって選別される `.txt`、`.log`、および `.hlp` ファイルを、変更されたポリシーは選別しません。

タスクの結果

除外リストに追加したファイル拡張子は、(他の有効なファイル選別ポリシーとの矛盾がなければ) そのポリシーが有効になっている場合は、ファイル選別サーバーによって選別されません。

リストからの拡張子の削除方法:

`fpolicy extensions CLI` コマンドを使用して、組み込みおよび除外の拡張子リストから拡張子を削除することができます。

組み込みリストからの拡張子の削除:

`fpolicy extensions include remove CLI` コマンドを使用して、組み込み拡張子リストから拡張子を削除することができます。

ファイル・ポリシーのための組み込み拡張子リストからファイル拡張子を削除するには、次のコマンドを入力します。 `fpolicy extensions include remove PolicyName ext-list fpolicy ext inc remove default wav`
`.wav` 拡張子を持つファイルは選別されません。

タスクの結果

このコマンドは、現在のファイル拡張子リストからエントリーを削除します。

除外リストからの拡張子の削除:

`fpolicy extensions exclude remove CLI` コマンドを使用して、除外拡張子リストから拡張子を削除することができます。

ファイル選別ポリシーのための除外拡張子リストからファイル拡張子を削除するには、次のコマンドを入力します。 `fpolicy extensions exclude remove PolicyName ext-list fpolicy ext exc remove default wav`
`.wav` 拡張子を持つファイルが選別されます。

タスクの結果

このコマンドは、現在のファイル拡張子リストからエントリーを削除します。

拡張子のリストの設定または置換の方法:

`fpolicy extensions CLI` コマンドを使用して、組み込みおよび除外拡張子のリストを設定あるいは置換することができます。

組み込み拡張子リストの設定:

fpolicy extensions include set CLI コマンドを使用して、組み込み拡張子リストを設定することができます。

FPolicy のための組み込みリスト全体を置き換えるには、次のコマンドを入力します。 fpolicy extensions include set *PolicyName* *ext-list*

タスクの結果

このコマンドの入力と同時に、このコマンドで指定した新規の拡張子リストが既存の組み込み拡張子リストを置き換えて、新規の拡張子のみが選別に組み込まれます。

注: set オプションを使用して、ファイル拡張子を選別しないように組み込みリストを設定することもできます。例えば、fpolicy ext inc set *PolicyName* "" このコマンドが使用された場合、選別されるファイルはありません。

除外拡張子リストの設定:

fpolicy extensions exclude set CLI コマンドを使用して、除外拡張子リストを設定することができます。

FPolicy のための除外リスト全体を置き換えるには、次のコマンドを入力します。 fpolicy extensions exclude set *PolicyName* *ext-list*

タスクの結果

このコマンドの入力と同時に、このコマンドで指定した新規の拡張子リストが既存の除外拡張子リストを置き換えて、新規の拡張子のみが選別から除外されます。

リスト内の拡張子のリセット方法:

fpolicy extensions CLI コマンドを使用して、組み込みおよび除外拡張子のリストをリセットすることができます。

組み込み拡張子リストのリセット:

fpolicy extensions include reset CLI コマンドを使用して、組み込み拡張子リストをリセットすることができます。

FPolicy のための組み込みリストからすべてのエントリーをデフォルト値にリセットするには、次のコマンドを入力します。 fpolicy extensions include reset *PolicyName*

タスクの結果

このコマンドは、ファイル拡張子組み込みリストをデフォルトのリストに復元します。

除外拡張子リストのリセット:

fpolicy extensions exclude reset CLI コマンドを使用して、除外拡張子リストをリセットすることができます。

FPolicy のための除外リストからすべてのエントリーをデフォルト値にリセットするには、次のコマンドを入力します。 `fpolicy extensions exclude reset`

PolicyName

タスクの結果

このコマンドは、ファイル拡張子除外リストをデフォルトのリストに復元します。

ファイル選別サーバーの管理方法

CLI コマンドを使用して重要なファイル選別サーバーの情報を表示することができます。また、サーバーをセカンダリー・サーバー・リストに割り当てたり、リストから削除することもできます。

ファイル選別サーバー情報の表示:

`fpolicy servers show` CLI コマンドを使用して、ファイル選別サーバーの重要情報を表示することができます。表示された情報は、登録されたサーバーのリスト、接続されたサーバーのリスト、および有効な機能を含みます。

このタスクについて

コマンドは、特定の FPolicy について以下の情報を表示します。

- 登録されている FPolicy サーバーのリスト
- 接続されている FPolicy サーバーのリスト
- サーバーが接続された合計時間
- Data ONTAP 7.3 でサポートされるサーバーに有効な機能のリスト
- プライマリー・サーバーの状況
- セカンダリー・サーバーの状況

ファイル選別サーバーの状況を表示するには、次のコマンドを入力します。:

`fpolicy servers show PolicyName`

タスクの結果

このコマンドを入力すると、Data ONTAP が、指定したポリシーに関するファイル選別サーバーの状況を返します。

接続の無効化:

サーバーの接続が無効に設定されると、FPolicy サーバーとストレージ・システムの間の接続は終了します。

ファイル選別サーバーへの接続を無効にするには、次のコマンドを入力します。

`fpolicy servers stop PolicyName server-IP-address`

PolicyName は、接続を無効にしたいポリシーの名前です。

server-IP-address は、ストレージ・システムから無効にしたい FPolicy サーバーの IP アドレスのリストです。

タスクの結果

サーバーの接続は無効になります。

セカンダリー・サーバー:

FPolicy サーバーは、プライマリー・サーバーおよびセカンダリー・サーバーのいずれとしても使用できます。特定の FPolicy サーバーあるいは FPolicy サーバーのリストを、`fpolicy options` コマンドを使用してセカンダリー・サーバーとして指定することが可能です。

ストレージ・システムは、使用可能なプライマリー・サーバーがない場合にのみ、セカンダリー・サーバーをファイル・ポリシーを実行するために使用します。これは、プライマリー・サーバーが使用可能な限り、FPolicy サーバーがセカンダリー・サーバーとして指定されている場合でもストレージ・システムがそれを使用することはないことを意味します。すべてのプライマリー・サーバーが使用不可の場合、ストレージ・システムはプライマリー・サーバーの 1 つが再び使用可能になるまでの間、ストレージ・システムに接続されているセカンダリー・サーバーのいずれかを使用します。

セカンダリーとして分類されていない FPolicy サーバーは、すべてプライマリー・サーバーと認識されます。

セカンダリー・サーバー・リストの割り当て:

`fpolicy options secondary_servers` CLI コマンドを使用して、特定の FPolicy サーバーをセカンダリー・サーバーとして割り当てあるいは指定することができます。

プライマリー・ファイル選別サーバーが使用不可のときに使用するための、セカンダリー・サーバーのリストを指定するには、次のコマンドを入力します。 `fpolicy options PolicyName secondary_servers [server_list]`

PolicyName は、セカンダリー・サーバーで使用したいポリシーの名前です。

server_list は、セカンダリー・サーバーとして指定したい FPolicy サーバーの IP アドレスのリストです。コンマ (,) を使用して IP アドレスを区切ります。このフィールドにリストされたいずれの IP アドレスからの接続も、ストレージ・システムによってセカンダリー・サーバーとして分類されます。

タスクの結果

このコマンドを入力すると、指定したサーバーが指定した FPolicy のためのセカンダリー・サーバーとして指定されます。

注: IP アドレスのコンマ区切りリストが提供されると、すべての既存のリストは新規のリストに置き換えられます。そのため、既存のセカンダリー・サーバーを保持するには、それらの IP アドレス を新規のリストに追加する必要があります。

すべてのセカンダリー・サーバーの削除:

`fpolicy options` CLI コマンドを使用して、すべてのセカンダリー・サーバーをプライマリー・サーバーに変換することができます。

すべてのセカンダリー・サーバーをプライマリー・サーバーに変換するには、次のコマンドを入力します。 `fpolicy options PolicyName secondary_servers ""`
PolicyName は、セカンダリー・サーバーで使用したいポリシーの名前です。

タスクの結果

このコマンドを実行した後、セカンダリー FPolicy サーバーとして割り当てられていたすべての FPolicy サーバーが、プライマリー FPolicy サーバーになります。

FPolicy を使用した操作の監視方法

`fpolicy monitor` CLI コマンドによって、監視する操作のリストの追加、削除、あるいは設定が可能です。

特定の操作を監視するには、以下のコマンドを入力します。 `fpolicy monitor {add|remove|set} PolicyName [-p { cifs|nfs|cifs,nfs} ] [-f] op-spec`

監視する操作のリストに操作を追加するには `add`、リストから操作を削除するには `remove`、リスト全体をリセットするには `set` をそれぞれ使用します。

PolicyName は、変更したいポリシーの名前です。

`-p` オプションは、FPolicy で監視したいプロトコルを示します。

`cifs` を使用して CIFS 操作の監視、`nfs` を使用して NFS 操作の監視、あるいは `cifs,nfs` を使用して CIFS と NFS 両方の操作の監視を行います。プロトコル情報が監視コマンドで指定されない場合は、ストレージ・システムは CIFS と NFS 両方のプロトコルに関する通知を送信します。

`-f` オプションは、ポリシーを実行するために使用可能なサーバーがない場合でも、ポリシーを強制的に有効にします。

op-spec は、監視する操作のリストです。

操作のリストを `all` オプションに置換することで、すべての操作に関する監視オプションをまとめて設定することも選択できます。

すべての操作を監視するには、以下のコマンド構文を使用します。 `fpolicy mon[itor] {add|remove|set} PolicyName [-p {cifs|nfs|cifs,nfs} ] [-f] all`

CIFS 操作に関して特定の操作が設定されており、その後 NFS 操作に関する設定が行われた場合、操作は両方のプロトコルからの要求に関して監視されます。ただし、プロトコルの 1 つから操作が削除された場合は、その操作の監視は両方のプロトコルについて停止します。

特定の操作が CIFS のみに設定されており、NFS では設定されていない場合は、この操作は両方のプロトコルで監視されます。この操作が NFS に関する監視操作のリストから削除されると、CIFS に関する監視も停止します。

監視リストへの操作の追加:

FPolicy がネイティブ・ファイル・ブロッキングを実装するためには、まずネイティブにブロックされる必要がある操作を監視する必要があります。それは、監視操作のリストにその操作を追加することで実行できます。

FPolicy で選別するための、監視操作のリストに操作を追加するには、次のコマンドを入力します。 `fpolicy mon[itor] add PolicyName [-p {cifs|nfs|cifs,nfs} ] [-f] op-spec`

PolicyName は、操作を追加したいポリシーの名前です。

protocols は、監視を有効にしたいプロトコルです。 `cifs` を使用して CIFS 要求を監視し、`nfs` を使用して NFS 要求を監視し、あるいは `cifs,nfs` を使用して両方を監視します。

op-spec は、追加したい操作のリストです。

タスクの結果

指定された操作が、監視操作のリストに追加されます。

例

監視操作のリストに読み取り、書き込み、および検索操作を追加するには、次のコマンドを入力します。 `fpolicy mon add pl read,write,lookup`

いったん有効に設定されると、ポリシー *pl* は、以前に設定されていた他の操作に加えて、読み取り、書き込み、および検索操作を監視します。

監視リストからの操作の削除:

`fpolicy monitor remove` CLI コマンドを使用して、リストから操作を削除することができます。監視操作のリストから操作を削除するときは、特定の操作は FPolicy によって監視されません。

FPolicy で選別されるための、監視操作のリストから操作を削除するには、次のコマンドを入力します。: `fpolicy mon[itor] remove PolicyName [-p {cifs|nfs|cifs,nfs} ] [-f] op-spec`

タスクの結果

指定された操作が、監視操作のリストから削除されます。

例

読み取りおよび `setattr` 操作の監視を停止し、監視操作のリストからそれらを削除するには、次のコマンドを入力します。 `fpolicy mon remove pl read,setattr`

いったん有効に設定されると、ポリシー *pl* は読み取りおよび `setattr` 操作の監視を停止し、これら 2 つの操作を監視操作のリストから削除します。

監視操作のリストの設定あるいは置換:

`fpolicy monitor set` CLI コマンドを使用して、監視操作のリストを置換することができます。

監視操作リストを置換するには、次のコマンドを入力します。 `fpolicy mon[itor] set PolicyName [-p {cifs|nfs|cifs,nfs } ] [-f] op-spec`

タスクの結果

監視操作のリストは、新しい操作のセットに置き換えられます。

例

監視操作のリストを設定あるいは置換するには、次のコマンドを入力します。

```
fpolicy mon set p1 read,setattr
```

いったん有効に設定されると、ポリシー `p1` は読み取り操作および `setattr` 操作のみを監視します。すべての既存の監視リストが、このリストに置き換えられます。

さまざまな CLI コマンド

以下の表には FPolicy CLI コマンドがリストされています。

入力するコマンド名	説明
<code>fpolicy help [cmd]</code>	CLI のヘルプを表示します
<code>fpolicy create PolicyName PolicyType</code>	ファイル・ポリシーを作成します
<code>fpolicy destroy PolicyName</code>	ファイル・ポリシーを削除します
<code>fpolicy enable PolicyName [-f]</code>	ファイル・ポリシーを有効にします
<code>fpolicy disable PolicyName</code>	ファイル・ポリシーを無効にします
<code>fpolicy show PolicyName</code>	ファイル・ポリシーを表示します
<code>fpolicy servers show PolicyName</code>	FPolicy サーバーの状況情報を表示します
<code>fpolicy servers stop PolicyName IP-address</code>	FPolicy サーバー接続を無効にします
<code>fpolicy options PolicyName required {on off}</code>	ファイル・ポリシーに関する必須選択のオプションをオンまたはオフにします
<code>fpolicy options PolicyName secondary_servers [IP-address [,IP-address]*]</code>	FPolicy サーバーのオプションを構成します
<code>fpolicy extension {excludel include} show PolicyName</code>	組み込みリストあるいは除外リストの拡張子を表示します
<code>fpolicy extension {excludel include} reset PolicyName</code>	組み込みリストあるいは除外リストの拡張子をリセットします
<code>fpolicy extension {excludel include} add PolicyName ext-list</code>	組み込みリストあるいは除外リストの拡張子を追加します
<code>fpolicy extension {excludel include} remove PolicyName ext-list</code>	組み込みリストあるいは除外リストから拡張子を削除します
<code>fpolicy extension {excludel include} set PolicyName ext-list</code>	組み込みリストあるいは除外リストのすべての拡張子をセットまたは置換します
<code>fpolicy volume {include exclude} show PolicyName</code>	組み込みリストあるいは除外リストのボリュームを表示します
<code>fpolicy volume {include exclude} reset PolicyName</code>	組み込みリストあるいは除外リストのボリュームをリセットします
<code>fpolicy volume {include exclude} addPolicyName vol_spec</code>	組み込みリストあるいは除外リストのボリュームを追加します

入力するコマンド名	説明
<code>fpolicy volume {includeexclude} remove <i>PolicyName</i> <i>vol_spec</i></code>	組み込みリストあるいは除外リストからポリシーを削除します
<code>fpolicy volume {includeexclude} set <i>PolicyName</i> <i>vol_spec</i></code>	組み込みリストあるいは除外リストのすべてのポリシーをセットまたは置換します
<code>fpolicy volume {includeexclude} eval <i>PolicyName</i> <i>vol_spec</i></code>	ワイルドカード文字を使用して指定されたポリシーを評価し、組み込みリストあるいは除外リストのポリシーを表示します
<code>fpolicy monitor add <i>PolicyName</i> [-p {nfs cifs nfs}] [-f] <i>op_spec</i> [,<i>op_spec</i>]</code>	監視中の操作リストに、操作を追加します
<code>fpolicy monitor remove <i>PolicyName</i> [-p {nfs cifs nfs}] [-f] <i>op_spec</i> [,<i>op_spec</i>]</code>	監視中のファイル・リストからファイルを削除します
<code>fpolicy monitor set <i>PolicyName</i> [-p {nfs cifs nfs}] [-f] <i>op_spec</i> [,<i>op_spec</i>]</code>	監視中のファイル・リストをセットあるいは置換します

FAQ、エラー・メッセージ、警告メッセージ、およびキーワード

このセクションでは、よくある質問 (FAQ)、エラー・メッセージおよび警告メッセージについて記載しています。

よくある質問 (FAQ)

一般的な FAQ とアクセス権に関する FAQ、およびその他の特定の事柄について、このセクションでカバーしています。

一般的な FAQ:

現在、アクティブ・ファイル・ポリシーの総数に制限はありますか？

はい、現在はアクティブ・ファイル・ポリシーの総数は、VFileer ユニットごとに 20 に制限されています。

2 つのポリシーが作成された場合、ストレージ・システムは要求を順次方式あるいは並列方式のどちらで処理しますか？

2 つのポリシーが作成された場合、ストレージ・システムは要求を順次に処理します。

ポリシーに優先順位付けをして、1 つのポリシーを他のポリシーより優位にすることはできますか？

FPolicy の既存の実装では、ポリシーの順位付けはサポートしていません。

異なる FPolicy サーバーに複数のポリシーを作成することはできますか？

はい。複数のポリシーを作成して、それぞれのポリシーを異なる FPolicy サーバーで使用することができます。例えば、2 つのポリシーを作成し、1 つを FLM 用に、1 つを NTP 用にし、そして 2 つの FPolicy サーバーをこれら 2 つのポリシーにポイントすることができます。

通知が送信される順番は、fpolicy コマンドでリストされるポリシーの順番と同じです。これは、ファイラーでポリシーが作成された順番の逆です。例えば、ポリシー p1 が作成され、続いてポリシー p2 が作成された場合、通知はまず p2 に送信され、続いて p1 に送信されます。

「複数のファイル・ポリシー」と「複数のサーバー」の違いに注意することが重要です。

直面する可能性があるいくつかの問題を以下に示します。

- 現在、FPolicy エンジンでは複数のポリシーについて、要求を（並列に送信するのではなく）順次に送信するため、二重のパフォーマンス低下になる可能性があります。
- FPolicy サーバーは異なるホストで稼働しなければなりません。

ストレージ・システムで FPolicy の処理を有効にするためには、何のライセンスが必要ですか？

FPolicy が動作するためには、ストレージ・システム上で CIFS がライセンス交付を受け、セットアップされている必要があります。

NFS のみのストレージ・システムでも、CIFS がライセンスとセットアップが必要なのはなぜですか？

FPolicy サーバーは多くの権限を行使し、またサーバーがストレージ・システム上でバックアップ・オペレーター特権（以上）を確実に使用できるように CIFS セキュリティーを使用して認証されています。そのため、NFS の排他的な環境でも CIFS がライセンス交付を受けている必要があります。また、NFS ファイルにファイル・ポリシーを適用するために、NFS もライセンス交付を受け、稼働している必要があります。

FPolicy には何か制限がありますか？

はい、以下は FPolicy の制限です。

- FPolicy は、CIFS および NFS に付随するプロトコルのみをサポートします。FTP、HTTP、WebDAV、FileIO、などはサポートしません。
- CIFS および NFS プロトコルのいくつかの操作は、FPolicy を使用して監視することができません。
- CIFS と NFS の操作は、個別に構成することができません。
- 選別はボリューム・レベル以下で実行できます。個々の qtree およびディレクトリーは選別することができません。
- FPolicy では ADS を選別できません。
- 複数のサーバーが登録されている場合、接続されているすべてのサーバーのポリシーは、最後に登録するサーバーの設定に基づいて変更します。
- IP アドレスからの FPolicy サーバーは、ストレージ・システムに一度だけ登録できます。
- 単一の FPolicy サーバーは、一度に 1 つのポリシーにのみ登録できます。FPolicy は、同一の IP アドレス から他のポリシーを登録するためのあらゆる要求を拒否します。

- 1 つのサーバーに関しては、1 つのポリシーのみが構成できます。
- Windows マシンでは、1 つの FPolicy サーバーのみが稼働可能です。

FPolicy は、ウィルス・スキャン (vscan) によって決まりますか？

FPolicy は vscan 操作とは独立して稼働しています。 FPolicy は、ウィルス・スキャン操作の前にあるため、スタブ・ファイルをただスキャンするのではなく、(シンボリック・リンクのような) スタブ・ファイルで指示されたパスを全探索して、実際のファイルをロードすることができます。 vscan 操作は、ファイル・ポリシーから独立しています。つまり、vscan はファイル・ポリシーによってブロックされているファイルをオープンおよびスキャンすることができます。そのため、FPolicy と vscan には相互依存はありません。

FPolicy 設定はどこに保存されますか？

FPolicy 設定はレジストリーに保存されます。

読み取り権限でアクセスした移行済みファイルに、ユーザーが変更を試行した場合、何が起きますか？

FPolicy サーバーは、以下を実行する必要があります。

CIFS および NFS バージョン 4 については、オープン要求が書き込み (または読み取り/書き込み) アクセス・モードの場合は、ファイル・オープン時に再呼び出しすることができます。あるいは、書き込み要求がされた場合にもそれは可能です。ただし、このオプションについては、サーバーが書き込み操作を監視するように登録されている必要があります。

NFSv2 および NFSv3 バージョンはオープン呼び出しを持っていないため、HSM サーバーは、読み取りおよび書き込み操作を監視するために登録する必要があります。 HSM サーバーは書き込み要求を受信したときにファイルを再呼び出しする必要があります。読み取り操作については、HSM サーバーはパススルーの読み取りあるいは書き込みのいずれかを使用するオプションを持っています。

アクセス権と許可に関する FAQ:

ストレージ・システムに接続し、FPolicy イベントを listen する FPolicy サーバーとして登録するアカウントの最小限のアクセス権は何ですか？

FPolicy サーバーは、ストレージ・システムに登録するために、少なくともバックアップ特権が必要です。

ストレージ・システムに接続し、qtree ACL をスキャンするアカウントの最小限のアクセス権は何ですか？

ACL をスキャンする権限は、標準的な Windows 方式を使用して CIFS にログインするために許可されます。バックアップ・オペレーターまたは管理者グループのメンバーのアカウントを使用してストレージ・システムに接続している場合、FILE_FLAG_BACKUP_SEMANTICS オープン・モードを使用して、セキュリティーに関係なくあらゆるファイルにアクセス可能です。

パフォーマンスに関する FAQ:

FPolicy のパフォーマンスを決定する要因は何ですか？

以下は、FPolicy のパフォーマンスを決定するいくつかの要因です。

- 監視されている操作 (読み取り、オープン、クローズなど) の数
- 登録されている FPolicy サーバーの数 (負荷共有)
- 同じ操作を選別しているポリシーの数
- ストレージ・システムと FPolicy サーバー間のネットワーク帯域幅 (選別要求の往復時間)
- FPolicy サーバーの応答時間

CIFS および NFS トラフィックの間でどのように FPolicy トラフィックが分割されているかを、どのように測定しますか？

ストレージ・システムで実行された FPolicy コマンドの出力は、その特定のファイル・ポリシーで選別された要求の総数のカウンターを含んでいます。ただし、現在は CIFS および NFS トラフィックの間の分割を知る方法はありません。

FPolicy 選別を通るすべてのクライアント要求は、内部 FPolicy 通信のためのいくつかの追加の CIFS 要求を生成します。これは CIFS および NFS クライアント両方の要求について当てはまります。現在は、この追加トラフィックを測定する方法はありません。

再呼び出しをする前に FPolicy をオンに切り替えると、パフォーマンスに影響はありますか？

はい、どのような再呼び出しでも、その前に FPolicy をオンに切り替えることは、パフォーマンスに影響します。パフォーマンスの影響は、まず、FPolicy がどのように構成されているかによって決まります。そのため、どのような再呼び出しが実行される前にも FPolicy をオンにしないことをお勧めします。

2 つの FPolicy サーバーが異なるパフォーマンス・レベルでストレージ・システムに登録されている場合、低速のサーバーのパフォーマンスが高速サーバーのパフォーマンスに影響しますか？

はい、低速のサーバーのパフォーマンスは、高速のサーバーのパフォーマンスに影響します。そのため、ストレージ・システムに接続している間は、性能が同じサーバーを使用することをお勧めします。

FPolicy が有効にされたときの、CPU に追加される負荷を測定する測定基準はありますか？

いいえ、現在、FPolicy についてそのようなデータは使用可能ではありません。

ファイル選別に関する FAQ:

ファイル選別はどのように動作しますか？

ファイル選別ポリシーは、何か制限を置きたいファイルまたはディレクトリーを指定するのに使用します。ファイルの操作要求 (オープン、書き込み、作成、あるいは名前変更など) を受信すると、Data ONTAP は、操作を許可する前にファイル選別ポリシーをチェックします。

ポリシーが、ファイルの拡張子に基づくファイル選別を指定する場合は、選別のためにファイル名がファイル選別サーバーに送信されます。ファイル選別サーバーは、ストレージ・システムが要求されたファイル操作を許可するかどうかを判断するために、ファイル名にポリシーを適用します。次に、ファイル選別サーバーは、要求されたファイル操作を許可するかブロックするか応答をストレージ・システムに送信します。

ファイル選別を使用している間、システムのパフォーマンスは低下しますか？

はい、ファイル選別を使用している間、システムのパフォーマンスは低下します。

ファイル選別オプションの設定にデフォルト・オプションを使用することはできますか？

すべてのファイル・ポリシーについてマスター設定 `fpolicy.enable` オプションがあり、これはデフォルトで `on` に設定されています。個々の `FPolicy` が新規に作成されると、これはデフォルトで `off` になります。これにより、システム管理者はアクティブにする前にポリシーを完全に構成することができます。実際に何かが選別されているかどうかは、ストレージ・システムにアクセス可能で稼働している、サポートされる外部のファイル選別サーバーがあるかどうかによって決まります。外部のファイル選別サーバーは、`FPolicy` を使用するための要件であることを覚えておってください。

選別ポリシーを作成したが、選別サーバーがない場合、何が起きますか？

使用可能なファイル選別サーバーがないときにポリシーを有効にした場合、何も起こりません。ただし、ポリシーのために `fpolicy option required` をオンにしている場合は、このポリシーで指定されているファイルへのアクセスは拒否されます。ポリシーの「`required`」設定は、デフォルトで `off` に設定されています。

どうすればファイル選別サーバーの状況を表示できますか？

ファイル選別サーバーの状況を表示するには、コマンド `fpolicy servers show PolicyName` を使用します。Data ONTAP は、指定したポリシーに関する選別サーバーの状況を返します。

セカンダリーの選別サーバーを指定することはできますか？可能な場合、どのようにすればいいですか？

はい、プライマリーのファイル選別サーバーが使用不可になったときに使用できるように、セカンダリー・サーバーのリストを指定することができます。以下のコマンドを使用します。

```
fpolicy options PolicyName secondary_servers [ server_list ]
```

ストレージ・システムに接続されているすべての `FPolicy` サーバーは、IP アドレスがセカンダリー・サーバー・リストに記載されていない限り、プライマリー・サーバーになります。セカンダリー・サーバーは、すべてのプライマリー・サーバーが使用不可にならない限り、ストレージ・システムに使用されることはありません。

どうすればファイル選別サーバーへの接続を無効にすることができますか？

ファイル選別サーバーへの接続を無効にするには、以下のコマンドを使用します。

```
fpolicy servers stop PolicyName server-IP-address
```

FPolicy のファイル選別は、ボリューム・レベルまたは **qtree** レベルのどちらに適用されますか？

FPolicy のファイル選別は、ボリューム・レベルに適用され、qtree レベルには適用されません。

FPolicy サーバーに関する FAQ:

プライマリー・サーバーとセカンダリー・サーバーの違いは何ですか？

プライマリー・サーバーはアクティブなサーバーで、クライアント要求を選別します。セカンダリー・サーバーはフェイルセーフ動作モードのために登録されています。すべてのプライマリー・サーバーが停止すると、すべてのセカンダリー・サーバーが要求の選別を開始します。

セカンダリー・サーバーはどのようにすれば登録できますか？

サーバーをセカンダリー・サーバーとして使用するためには、サーバーの IP アドレスをセカンダリー・サーバー・リストに追加する必要があります。

サーバーが接続したときに、セカンダリーとして処理されます。

エラー・メッセージ

次の表は、一般的な FPolicy のエラー・メッセージ、推定原因、および推奨処置(ある場合)を示しています。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server.connectError severity="ERR"	このエラーは、ストレージ・システムが FPolicy (ファイル・ポリシー) サーバーとの通信を試行している間にエラーを検出したときに生成されます。通信障害は、ストレージ・システムがこのサーバーとの接続を切断する原因になります。 エラーは、ネットワークの問題、ストレージ・システムへのアクセスを拒否する FPolicy サーバーのセキュリティ設定、あるいは FPolicy サーバー上のハードウェアまたはソフトウェアの問題が原因の可能性があります。この問題は、ストレージ・システムの低メモリー状態によって、ストレージ・システムが操作の実行に必要なリソースを取得することができない場合にも起きる可能性があります。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断されていないか、およびその理由を確認してください。 ストレージ・システムの syslog を調査し、手掛かりになりそうなエラー・メッセージを確認してください。 FPolicy サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。セキュリティ設定を変更する可能性があるソフトウェア・パッチが FPolicy サーバーに最近インストールされていないか確認してください。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server.closeError severity="ERR"	このエラーは、ストレージ・システムが FPolicy (ファイル選別) サーバーとの通信の停止を試行している間にエラーを検出したときに生成されます。エラーは、ネットワークの問題、あるいは FPolicy サーバー上のハードウェアまたはソフトウェアの問題が原因の可能性があります。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断されていないか、およびその理由を確認してください。 FPolicy サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。このエラーは、エラーではない可能性があります。ストレージ・システムは、前にサーバーとの通信を試行したときに発生したエラーが原因で、サーバーとの通信を終了しようとしている可能性があります。接続を閉じている間に発生したエラーは、前に発生したエラー状態が継続している可能性があります。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server.requestError severity="ERR"	このエラーは、ストレージ・システムが FPolicy (ファイル・ポリシー) サーバーへの通知要求の送信を試行している間にエラーを検出したときに生成されます。エラーは、ネットワークの問題、あるいは FPolicy サーバー上のハードウェアまたはソフトウェアの問題が原因の可能性があります。 ポリシーに複数のサーバーがある場合、ストレージ・システムはこの通知をこのポリシーの別のサーバーと再試行します。そうでない場合、ストレージ・システムは必要なオプションに関するポリシーの設定に基づいて処理を継続します。 required 設定が on の場合、ストレージ・システムは要求を拒否します。 required 設定が off の場合、ストレージ・システムはクライアント要求の処理を継続することを許可します。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断されていないか、およびその理由を確認してください。 FPolicy サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。
fpolicy.fscreen.server.requestRejected severity="ERR"	このエラーは、 FPolicy (ファイル・ポリシー) サーバーへのストレージ・システムの通知要求が FPolicy サーバーに拒否されたときに生成されます。エラーは、 FPolicy サーバー上のソフトウェアの問題が原因の可能性があります。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、問題を説明するエラーが作成されていないかを確認してください。 FPolicy サーバーは内部エラーを検出している可能性、あるいはこれ以上の要求を承認できない可能性があります。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server.pingRejected severity="ERR"	FPolicy サーバーの接続がアイドル状態の場合、ストレージ・システムは FPolicy サーバーの状況を確認するために状況要求を送信することがあります。このエラーは、FPolicy サーバーへのストレージ・システムの状況要求がエラーを検出したときに生成されます。このエラーは、ストレージ・システムが FPolicy サーバーにコンタクトできない場合、あるいはサーバーがストレージ・システムの要求にエラーを返した場合に発生する可能性があります。エラーは、ネットワークの問題、あるいは FPolicy サーバー上のハードウェアまたはソフトウェアの問題が原因の可能性があります。この要求が失敗すると、ストレージ・システムはサーバーとの接続を切断します。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断されていないか、およびその理由を確認してください。 FPolicy サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。
fpolicy.fscreen.server.completionUnexpectedState severity="ERR"	このエラーは、FPolicy サーバーが選別要求を完了し、完了をリターンしたときに発生します。ただし、この要求に対するストレージ・システムの内部状態は無効です。この完了メッセージは、ストレージ・システムに無視されます。	
fpolicy.fscreen.server.requestStatusError severity="ERR"	このエラーは、FPolicy サーバーが選別要求を承認したが、要求の完了を報告していないときに発生します。ストレージ・システムは、未完了の要求の状況を確認します。ストレージ・システムが要求を送信できない場合、あるいはサーバーが要求をサポートしない場合にこのエラーは発生します。エラーは、ネットワークの問題、あるいはストレージ・システムへのサーバーの接続を切断した FPolicy サーバー上のハードウェアまたはソフトウェアの問題が原因の可能性があります。	問題の原因を指摘するのに役立つエラー・コードがないか調査してください。 FPolicy (ファイル・ポリシー) サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断されていないか、およびその理由を確認してください。サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server. connecting.internalError severity="ERR"	このエラーは、ファイル・ポリシー・サーバーがストレージ・システムに登録され、ストレージ・システムのための FPolicy サーバーとしての動作を提供するときに発生します。ストレージ・システムは、FPolicy サーバーに関連する情報を保持するために必要なメモリーを取得できていません。	NGS に連絡してください。
fpolicy.fscreen.server. connecting.privError severity="ERR"	このエラーは、FPolicy サーバーがストレージ・システムに登録され、ストレージ・システムのための FPolicy サーバーとしての動作を提供するときに発生します。サーバーは、FPolicy サーバーとしての役目を果たすには特権が十分ではないユーザーとして接続しています。ストレージ・システムは、サーバーがストレージ・システムに接続するために名前を使用するユーザーは、少なくともストレージ・システムのバックアップ・オペレーター・グループのメンバーでなければならないことを要求します。この登録試行は拒否されます。	ファイラー・オプション cifs.trace_login をオンにして、サーバーがストレージ・システムに接続するためにどのユーザー名を使用しているかを確認します。トレースがストレージ・システムのパフォーマンスに影響するため、この問題が解決した後はオプションをオフにすることを忘れないでください。 FPolicy サーバー上でファイル・ポリシー・サービスを稼働しているユーザー名を確認してください。 wcc コマンドを使用して、このユーザーが属しているグループを確認します。おそらく、このユーザーを適切なグループに追加するか、あるいは FPolicy サーバーのプロパティーを変更することで、異なるユーザー名でこのサービスは稼働します。

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.cfg.pCreateErr severity="ERR"	このエラーは、ストレージ・システムがレジストリーからの保存されたファイル選別構成情報を処理するときに発生します。ストレージ・システムは新規のポリシーの作成および初期化を要望しています。ただし、ストレージ・システムはそれを実行することができません。このエラーはストレージ・システムのレジストリーの整合性の問題を示しており、発生するべきではない問題です。ストレージ・システムはこのポリシーに関する情報を廃棄します。	fpolicy destroy コマンドによって、ポリシーを削除することが可能です。次に、fpolicy create コマンドを使用してポリシーを再作成し、必要に応じてポリシー構成を設定してください。
fpolicy.fscreen.request.pathError severity="ERR"	このエラーは、ストレージ・システムがファイル選別 (fscreen) サーバーのパスをファイル・アクセスで使用するために作成する際に、エラーを検出すると発生します。考えられるエラーとして、パスが長すぎる、あるいは Unicode の変換問題などが挙げられます。ユーザーは、以下のようなパスでファイルにアクセスします。 shareName¥directories¥fileName ストレージ・システムは、ストレージ・システムのルートからサーバーのための絶対パスを作成します。 ontap_admin\$¥vol\volName¥sharePath¥directories¥FileName 通常は、これがストレージ・システムの内部エラー (バグ) です。	

エラー・メッセージ	原因	推奨処置
fpolicy.fscreen.server.requestTO severity="ERR"	このエラーは、サーバーがファイル選別通知を承認したが、要求の完了を報告していないときに発生します。ストレージ・システムは、タイムアウトが過ぎた後に未完了の要求の状況を確認します。サーバーが、承認したが完了していない要求のすべての認識を否定した場合、要求はタイムアウトになったと考えられます。一般的に、これはサーバーの問題を示します。	サーバーのイベント・ログを調査し、問題を記録していないかを確認してください。サーバー・ソフトウェア・ベンダーに連絡し、それらの製品が要求状況の照会をサポートしているかを確認してください。ストレージ・システムは、サーバーが承認した要求のみをタイムアウトにします。サーバーがまだ要求を処理中であると宣言している限り、要求をタイムアウトにしません。ストレージ・システムは要求状況メッセージをサーバーに送信し、タイムアウトになる可能性のある要求の状況を確認します。
fpolicy.server.fqdn.unavail severity="ERR"	このメッセージは、FPolicy(tm) (ファイル・ポリシー) サーバーの IP アドレスの DNS 逆引きが失敗し、ストレージ・システムが FPolicy サーバーの完全修飾ドメイン名 (FQDN) を判別できないときに発生します。FPolicy サーバーが Microsoft Longhorn OS で稼働している場合、ストレージ・システムは FPolicy サーバーに対して認証のための FPolicy サーバー FQDN を要求します。	DNS サーバー上の DNS 逆引き構成を検証してください。

警告メッセージ

次の表は、一般的な FPolicy の警告メッセージ、推定原因、および推奨処置 (ある場合) を示しています。

警告	原因	推奨
fpolicy.fscreen.server. connectedNone severity="WARNING"	この警告は FPolicy (ファイル選別) サーバーが 1 台もストレージ・システムに接続されていない場合に発生します。ファイルおよびディレクトリーの様々な操作をストレージ・システムが拒否するため、ポリシーが要求された場合にはこれが重大な警告になる可能性があります。どのサーバーも操作を承認していないにも関わらずファイルおよびディレクトリーの様々な操作をストレージ・システムが許可するため、ポリシーが要求されない場合にはこれが重大な警告になる可能性があります。	FPolicy サーバーのイベント・ログを調査し、FPolicy サーバーがストレージ・システムから切断された理由を確認してください。ストレージ・システムの syslog を調査し、手掛かりになりそうなエラー・メッセージを確認してください。 FPolicy サーバー上のネットワーク・エラーやハードウェア障害など、検出された問題を修正してください。

警告	原因	推奨
fpolicy.fscreen.server.completionRequestLost severity="WARNING"	この警告は、FPolicy (ファイル・ポリシー) サーバーが選別要求を完了し、完了をリターンしたときに発生します。ただし、ストレージ・システムは完了として報告された要求を検出することはできません。 この警告は、FPolicy サーバーおよびストレージ・システムの同期が終了したことを示しています。タイミングの問題が原因で、問題が発生する可能性があります。例えば、完了報告は、ストレージ・システムでファイル選別が無効化され、完了を待っていたすべての要求が続行を許可された後、すぐに到着する可能性があります。あるいは、FPolicy サーバーが選別要求の承認の前に完了報告を返しました。あるいは、要求がタイムアウトになり、ストレージ・システムが要求の状況を要求した原因となった可能性があります。FPolicy サーバーが要求を検出できなかった場合、ストレージ・システムは要求が続行することを許可します。次に、FPolicy サーバーが後から要求を完了した場合、その要求は検出されません。	問題が繰り返し発生している場合は、回線トレースが診断の助けになります。ファイラー・コマンド (filer command) <code>pktt</code> が、回線トレースを取得するのに使用できます。

警告	原因	推奨
fpolicy.fscreen.server.completionInconsistent severity="WARNING"	この警告は、FPolicy (ファイル・ポリシー) サーバーが選別要求を完了し、選別完了をリターンしたときに発生します。しかし、完了メッセージのファイル・パスが、ストレージ・システムによって行われた選別要求のファイル・パスと一致しません。 ストレージ・システムが選別要求を行った場合、ファイル・パスと要求 ID の両方を FPolicy サーバーに提供します。 FPolicy サーバーは、有効な要求 ID を持つストレージ・システムに選別完了メッセージを送信しましたが、ファイル・パスがストレージ・システムによって選別要求で提供されたファイル・パスと一致しません。 この問題は、FPolicy サーバーあるいはストレージ・システムのソフトウェア不良の可能性もあります。あるいは、FPolicy サーバーがストレージ・システムのグループに役割を果たしている場合、要求 ID はストレージ・システムで有効だがファイル・パスが要求 ID と関連付けられていないために、要求は完了しているにも関わらず完了報告が間違ったストレージ・システムに送信されている、という可能性があります。	問題が繰り返し発生している場合は、回線トレースが診断の助けになります。ファイラー・コマンド (filer command) <code>pktt</code> が、回線トレースを取得するのに使用できます。

警告	原因	推奨
fpolicy.fscreen.server. connecting. badOperationList severity="WARNING"	この警告は、FPolicy サーバーが通知を受信したい操作のリストをストレージ・システムに提供したときに発生します。操作の例には、ファイル名あるいはディレクトリー名の変更、ファイルの作成、ファイルのオープンあるいはクローズ、などが含まれます。リストは、サーバーが登録したときあるいはその後でストレージ・システムに提供されます。この警告は、FPolicy サーバーによって提供された操作のリストが、ストレージ・システムが通知を提供していない操作を含んでいるために発生しています。ストレージ・システムは、サーバーから提供されたリストを無視します。	ストレージ・システムおよびファイル・ポリシーのソフトウェアのバージョンを確認し、お互いに互換性があることを確認してください。
fpolicy.fscreen.server. connecting.badParameter severity="WARNING"	この警告は、FPolicy サーバーがストレージ・システムに登録され、ストレージ・システムのためのファイル・ポリシー・サーバーとしての動作を提供するときに発生します。サーバーに提供されたパラメーターは、ストレージ・システムが理解する値に設定されていませんでした。ストレージ・システムは、サーバーから提供されたこのパラメーターを無視します。	ストレージ・システムおよびファイル・ポリシーのソフトウェアのバージョンを確認し、お互いに互換性があることを確認してください。ストレージ・システムは無効なパラメーターを無視し、サーバーをストレージ・システムに登録することを許可します。

警告	原因	推奨
fpolicy.srv.conn. badOptParam severity="WARNING"	このメッセージは、FPolicy(tm) サーバーがシステムに登録され、そのシステムのためのファイル・ポリシー・サーバーとして使用可能になったときに発生します。ただし、FPolicy サーバーが提供するオプション・パラメーターは、システムによって認識可能な値の設定がされていないか、オプション・パラメーターに付随するフォーマットが正しくないかのいずれかです。システムは無効なパラメーターを無視し、FPolicy サーバーに登録することを許可します。	システムおよびファイル・ポリシーのソフトウェアのバージョンを確認し、お互いに互換性があることを確認してください。
fpolicy.fscreen.cfg. pCreateInfo severity="WARNING"	この警告は、ストレージ・システムがレジストリーからの保存されたファイル選別構成情報を処理するときに発生します。ストレージ・システムは新規のポリシーの作成および初期化を要望しています。しかし、ストレージ・システムは問題に直面しました。この警告はストレージ・システムのレジストリーの整合性の問題を示しており、発生するべきではない問題です。	fpolicy destroy コマンドによって、ポリシーを削除することが可能です。次に、fpolicy create コマンドを使用してポリシーを再作成し、必要に応じてポリシー構成を設定してください。
fpolicy.fscreen.server. droppedConn severity="WARNING"	この警告は、ファイル・ポリシー (fscreen) サーバーへの接続が失われたときに生成されます。接続は、サーバーが自発的にストレージ・システムから切断したときに失われる可能性があります。接続を失う理由として他には、ネットワーク・エラー、ストレージ・システム上の CIFS サービスの終了、およびサーバー上のハードウェアまたはソフトウェアの障害などが考えられます。	サーバーが機能を継続しているかを確認してください。ストレージ・システムとサーバー間のネットワーク接続を確認してください。切断を説明するエラーがないか、サーバーのイベント・ログを確認してください。ストレージ・システム上で CIFS が稼働していることを確認してください。

警告	原因	推奨
fpolicy.fscreen.vol.i2p.off severity="WARNING"	このメッセージは、FPolicy(tm) サーバーがファイル・ポリシーのためにシステムに登録され、NFS 要求に対するファイル・ポリシーの通知のための inode からパスへの名前変換を要求したときに発生します。ただし、ファイル・ポリシーによってマウントされたボリュームでは、inode からパスへの名前変換は無効に設定されています。FPolicy は、ボリュームで inode からパスへの名前変換が無効になっている場合、NFS 要求のファイル・パスの生成に失敗します。	次のコマンドを使用して、no_i2p オプションをオフにします。vol options volumeName no_i2p off このコマンドによって、ボリューム上のファイルの inode からパスへの名前変換が有効になります。

警告	原因	推奨
fpolicy.fscreen.server. unexpectedFileDataResponse severity="WARNING"	このメッセージは、FPolicy サーバーが RRD (読み取り転送) 要求に対するファイル・データをシステムに送信したが、システムが送信されたファイル・データの要求を検出できないときに発生します。この警告は、FPolicy サーバーとシステムが同期中ではないことを意味します。 タイミングの問題が原因で、この問題が発生する可能性があります。例えば、ファイル・データは、システムでファイル選別が無効化され、完了を待っているすべての要求が続行を許可された後、すぐに到着した可能性があります。あるいは、FPolicy サーバーが、選別要求の承認前にファイル・データを返した可能性があります。あるいは、要求がタイムアウトになったことにより、システムが要求の状況を要求した可能性があります。あるいは、FPolicy サーバーが要求を検出できなかった場合、システムは要求が継続することを許可します。次に、FPolicy サーバーが遅れて要求に対するファイル・データを送信する場合、その要求はシステムに検出されません。	問題が繰り返し発生する場合は、パケット・トレースを使用すると診断の助けになります。 pktt コマンドを使用して、パケット・トレースを取得してください。 例: pktt start all -i FpolicyServerIP

選別操作に関するキーワード・リスト

すべての操作は 3 つの方法で監視することができます。それらは FPolicy サーバーを登録している間にビット・マスクを使用して設定することができ、ONTAPI 呼び出しを使用して構成することができ、CLI を使用して構成することができます。

異なるキーワードを使用して、FPolicy がサポートする各操作の監視を構成することができます。以下の表は、3 つのオプションで構成する場合の、それぞれの操作に使用されるキーワードを記載しています。

操作名	CLI キーワード	ONTAPI キーワード	登録に関するキーワード	
			ビット	値
ファイル・オープン	open	file-open	FS_OP_OPEN	0x0001

操作名	CLI キーワード	ONTAPI キーワード	登録に関するキーワード	
			ビット	値
ファイル作成	create	file-create	FS_OP_CREATE	0x0002
ファイル・クローズ	close	file-close	FS_OP_CLOSE	0x0008
ファイル名変更	rename	file-rename	FS_OP_RENAME	0x0004
ファイル削除	delete	file-delete	FS_OP_DELETE	0x0010
ファイル書き込み	write	file-write	FS_OP_WRITE	0x4000
ファイル読み取り	read	file-read	FS_OP_READ	0x2000
ファイル・リンク	link	link	FS_OP_LINK	0x0400
ファイル・シンボリック・リンク	symlink	symlink	FS_OP_SYMLINK	0x0800
ディレクトリー削除	directory-delete	directory-delete	FS_OP_DELETE_DIR	0x0020
ディレクトリー名変更	directory-rename	directory-rename	FS_OP_RENAME_DIR	0x0040
ディレクトリー作成	directory-create	directory-create	FS_OP_CREATE_DIR	0x0080
ファイル検索	lookup	lookup	FS_OP_LOOKUP	0x1000
属性取得	getattr	getattr	FS_OP_GETATTR	0x0100
属性設定	setattr	setattr	FS_OP_SETATTR	0x0200

CIFS over IPv6

Data ONTAP 7.3.1 から、ご使用のストレージ・システム上のファイルに CIFS クライアントが IPv6 上でアクセスすることを許可することができます。

Data ONTAP は、デュアル・スタック・メカニズムを使用して IPv4 から IPv6 に移行します。そのため、ご使用のストレージ・システムは、以下の 3 つのモードで CIFS クライアントがファイルにアクセスすることを許可することができます。

- IPv4 モードのみ
- IPv6 モードのみ
- IPv6/IPv4 モード

デュアル・スタック・メカニズムに関する詳細については、「*Data ONTAP Network Management Guide*」を参照してください。

ご使用のストレージ・システムは、IPv6 上での CIFS サービスの提供のために、ポート 445 上でのみデータの送受信を行います。

注: NetBIOS over TCP (NBT) は、IPv6 上での CIFS サービスをサポートしません。

CIFS over IPv6 の有効化あるいは無効化

CIFS over IPv6 を、`cifs.ipv6.enable` オプションを `on` あるいは `off` に設定することで、それぞれ有効あるいは無効にすることができます。

始める前に

ip.v6.enable オプションを on に設定することで、ストレージ・システムの IPv6 を有効にする必要があります。ストレージ・システムでの IPv6 の有効化に関する詳細情報については、*Data ONTAP Network Management Guide* を参照してください。

このタスクについて

- CIFS over IPv6 を有効にしており、次に ip.v6.enable オプションを off に設定することで IPv6 をストレージ・システムで無効にする場合、CIFS over IPv6 は自動的に無効になります。
- IPv6 グローバル・オプションの再始動の後、CIFS over IPv6 を再始動する必要はありません。CIFS over IPv6 がストレージ・システム上で有効になっている場合、そして IPv6 グローバル・オプションを無効化および再有効化した場合、CIFS over IPv6 ソケットが IPv6 アドレスを listen するために自動的に作成されます。

以下を実施したい場合、	以下を実行してください。
CIFS over IPv6 を有効にする	次のコマンドを入力します。options cifs.ipv6.enable on
CIFS over IPv6 を無効にする	次のコマンドを入力します。options cifs.ipv6.enable off 注: CIFS over IPv6 が無効にされると、新規の CIFS セッションは IPv6 上で承認されませんが、既存の IPv6 CIFS セッションは引き続き IPv6 上で動作します。

IPv4 あるいは IPv6 CIFS セッションのリスト表示

cifs sessions コマンドを使用して、ストレージ・システムで稼働している IPv4 および IPv6 CIFS セッションをリストすることができます。また、cifs sessions コマンドと一緒に -i オプションを使用することで、over IPv4 で稼働している CIFS セッションのみ、あるいは over IPv6 で稼働している CIFS セッションのみを表示することができます。

以下を実施したい場合、	以下を実行してください。
すべての CIFS セッションをリストする	次のコマンドを入力します。cifs sessions 例: <pre>cifs sessions Server Registers as 'MACHINE1' in Windows 2000 domain 'IPV6LH1' Root volume language is not set. Use vol lang. Selected domain controller ¥¥WIN2K8-204-121 for authentication ===== PC IP(PC Name) (user) #shares #files 10.73.9.35(machine5-lxp) (ipv6lh1¥administrator-root) 1 0 fd20:81be:b255:4204:fd3d:e44:9ab1:6ae5 (VISTA204-123) (ipv6lh1¥administrator - root)</pre>
over IPv4 で稼働している CIFS セッションをリストする	次のコマンドを入力します。cifs sessions -i ipv4 例: <pre>cifs sessions -i ipv4 Server Registers as 'MACHINE1' in Windows 2000 domain 'IPV6LH1' Root volume language is not set. Use vol lang. Selected domain controller ¥¥WIN2K8-204-121 for authentication ===== PC IP(PC Name) (user) #shares #files 10.73.9.35(machine5-lxp) (ipv6lh1¥administrator - root) 1 0</pre>

以下を実施したい場合、	以下を実行してください。
over IPv6 で稼働している CIFS セッションをリストする	次のコマンドを入力します。cifs sessions -i ipv6 例: <pre> cifs sessions -i ipv6 Server Registers as 'MACHINE1' in Windows 2000 domain 'IPV6LH1' Root volume language is not set. Use vol lang. Selected domain controller ¥¥WIN2K8-204-121 for authentication ===== PC IP(PC Name) (user) #shares #files fd20:81be:b255:4204:fd3d:e44:9ab1:6ae5 (VISTA204-123) (ipv6lh1¥administrator - root) 1 0 </pre>

累積の IPv4 あるいは IPv6 CIFS セッションのリスト表示

cifs sessions コマンドと一緒に -t オプションを使用して、over IPv4 あるいは IPv6 で稼働している累積の CIFS セッションを表示することができます。

次のコマンドを入力します。cifs sessions -t

例

以下の出力は、over IPv4 で稼働している 2 つの累積 CIFS セッションと、over IPv6 で稼働している 1 つの累積 CIFS セッションを表示しています。

```
cifs sessions -t  
Using domain authentication. Domain type is Windows 2000.  
Root volume language is not set. Use vol lang.  
Number of WINS servers: 0  
Total CIFS sessions: 2  
CIFS open shares: 2  
CIFS open files: 0  
CIFS locks: 0  
CIFS credentials: 2  
CIFS sessions using security signatures: 0  
IPv4 CIFS sessions: 1  
IPv6 CIFS sessions: 1  
Cumulative IPv4 CIFS sessions: 2  
Cumulative IPv6 CIFS sessions: 1
```

NFS と CIFS 間のファイル共有

NFS と CIFS のクライアント間でエラーなく迅速にファイルを共有するために、Data ONTAP を最適化することができます。

NFS および CIFS ファイルの命名について

ファイルの命名規則は、ネットワーク・クライアントのオペレーティング・システムとファイル共有プロトコルの両方によって決まります。

オペレーティング・システムおよびファイル共有プロトコルは、以下のことを決定します。

- ファイル名の長さ
- ファイル名に使用できる文字
- ファイル名の大/小文字の区別

ファイル名の長さ

Data ONTAP は、PC のロング・ファイル名フォーマットをサポートする CIFS クライアントおよび 8.3 フォーマットをサポートする CIFS クライアントのために、それぞれ異なる長さのファイル名をサポートしています。

Data ONTAP は、以下のファイル名の長さをサポートします。

- PC のロング・ファイル名フォーマットをサポートする NFS クライアントおよび CIFS クライアントのために最大 255 文字
- MS-DOS あるいは Windows 3.x クライアントのような 8.3 フォーマットをサポートする CIFS クライアントのために、最大 8 文字のファイル名および 3 文字のファイル名拡張子

ファイル名に使用できる文字

異なるオペレーティング・システムのクライアント間でファイルを共有する場合、両方のオペレーティング・システムで有効な文字を使用する必要があります。

例えば、UNIX でファイルを作成する場合、ファイル名にコロン (:) を使用しないでください。コロンは MS-DOS のファイル名で許可されていないからです。有効とされる文字の制限がオペレーティング・システムによって異なるため、より詳細な禁止文字についてはクライアントのオペレーティング・システムに関する資料を参照してください。

ファイル名の大/小文字の区別

ファイル名は NFS クライアントでは大/小文字の区別があり、CIFS クライアントでは大/小文字を区別しませんが、大/小文字を保存します。

例えば、CIFS クライアントが Spec.txt を作成した場合、CIFS クライアントおよび NFS クライアントの両方がファイル名を Spec.txt と表示します。しかし、CIFS ユ

ユーザーが後から `spec.txt` を作成しようとした場合、CIFS クライアントにとってはその名前は既に存在しているため、許可されません。NFS ユーザーが後から `spec.txt` と名付けたファイルを作成した場合は、NFS クライアントと CIFS クライアントは以下のように異なるファイル名を表示します。

- NFS クライアントでは、ファイル名が大/小文字の区別をするため、作成したとおり両方のファイル名 `Spec.txt` と `spec.txt` が表示されます。
- CIFS クライアントでは、`Spec.txt` と `Spec~1.txt` が表示されます。Data ONTAP は 2 つのファイルを区別するために、`Spec~1.txt` ファイル名を作成します。

小文字のファイル名の作成

`cifs.save_case` オプションを `off` に設定することで、Data ONTAP にファイル名の入力時の大/小文字を無視して、それらのファイル名を強制的に小文字テキストに変換させることができます。

このタスクについて

このオプションを `off` に設定することで、16 ビット・アプリケーションといくつかの UNIX ツールの間の互換性を向上させることができます。ただし、デフォルトではこのオプションは `on` に設定されています。

次のコマンドを入力します。 `options cifs.save_case off`

Data ONTAP によるファイル名作成方法

Data ONTAP は、CIFS クライアントからアクセス権があるすべてのディレクトリ内のファイルについて、それぞれ 2 つのファイル名を作成および維持します。2 つのファイル名は、オリジナルのロング・ネームおよび 8.3 フォーマットのファイル名です。

8 文字の名前または 3 文字の拡張子の制限を超えるファイル名については、Data ONTAP は 8.3 フォーマットのファイル名を以下のように生成します。

- ファイル名が 6 文字を越えている場合、オリジナルのファイル名を 6 文字で切り捨てます。
- チルド (~) および 1 から 5 の番号を、切り捨てによって固有ではなくなったファイル名に追加します。5 つより多い類似の名前のファイルが存在することで番号を使い尽くした場合は、オリジナルのファイル名とは無関係な固有のファイル名を作成します。
- ファイル名拡張子を 3 文字に切り捨てます。

例: NFS クライアントが `specifications.html` と名付けたファイルを作成した場合、Data ONTAP が作成する 8.3 フォーマットのファイル名は、`specif~1.htm` となります。この名前が既に存在する場合、Data ONTAP はファイル名の末尾に異なる番号を使用します。例えば、NFS クライアントが `specifications_new.html` と名付けた別のファイルを作成した場合、`specifications_new.html` の 8.3 フォーマットは `specif~2.htm` となります。

CIFS クライアントからのドット・ファイルの表示のコントロール

ドット・ファイルは、通常は UNIX ベースのシステムでは表示されません。Windows クライアントにドット・ファイルを非表示にするオプションを提供したい場合は、`cifs.show_dotfiles` オプションを `off` に設定してください。

このタスクについて

デフォルトでは、隠しファイルの表示あるいは非表示についての Windows 「フォルダ オプション」の表示設定に関わらず、これらのファイルは CIFS クライアント・システムでは表示されます。

`cifs.show_dotfiles` オプションをオフに設定するには、次のコマンドを入力してください。`options cifs.show_dotfiles off` このシステム上のドット・ファイルは、Windows クライアント・ユーザーが「フォルダ オプション」ボックスの「表示」タブから「隠しファイルおよび隠しフォルダーを表示しない」を選択した場合は、表示から除外することができます。（「フォルダ オプション」ボックスを表示するには、Windows エクスプローラ の「ツール」メニューから「フォルダ オプション」を選択してください。）

UNIX と Windows 間のファイル名文字変換の有効化

両方のオペレーティング・システム (Windows と UNIX) 上で、両方のオペレーティング・システムで有効ではない文字を含んだ既存のファイル名がある場合、`charmap` コマンドを使用して、CIFS クライアントが CIFS に無効な NFS 名を持つファイルにアクセスすることを許可することができます。

このタスクについて

NFS クライアントが作成したファイルに CIFS クライアントがアクセスするとき、ストレージ・システムはファイル名を見て、名前が有効な CIFS ファイル名ではなかった場合 (例えば、コロン (:) 文字が組み込まれていた場合)、ストレージ・システムは各ファイルに保持されている 8.3 ファイル名を返します。ただし、重要情報を長いファイル名にエンコードするアプリケーションにとって、これは問題の原因となります。

そのため、異なるオペレーティング・システムのクライアント間でファイルを共有する場合、両方のオペレーティング・システムで有効な文字をファイル名に使用する必要があります。

ただし、両方のオペレーティング・システム (Windows と UNIX) 上で、両方のオペレーティング・システムで有効ではない文字を含んだ既存のファイル名がある場合は、無効な NFS 文字を CIFS および特定の Windows アプリケーションの両方が受け入れることができる Unicode 文字に変換するマッピングを定義することができます。

詳細情報については、`na_charmap(1)` のマニュアル・ページを参照してください。

注: この機能は、この要件を持つ他のアプリケーションと同様に、CATIA MCAD および Mathematica アプリケーションをサポートします。

次のコマンドを入力します。charmap [volname [mapspec]]

パラメーター	説明
volname	ストレージ・システム上のボリューム名
mapspec	mapspec のフォーマットは以下のとおりです。 hh:hhhh [,hh:hhhh]... それぞれの hh は、16 進値を表します。コロンで分離された各 hh ペアの最初の値は、変換したい NFS 文字の 16 進値で、各 hh ペアの 2 番目の値は、CIFS が使用する Unicode 値です。 mapspec の値を指定しない場合は、現在のマッピングがあれば表示されます。 volname の値を指定しない場合は、すべてのボリュームのマッピングが表示されます。

タスクの結果

CATIA アプリケーションで使用されるマッピング文字

CATIA アプリケーションで使用される文字をマッピングするには、次のコマンドを入力します。charmap desvol 3e:ff76,3c:ff77,2a:ff78,3a:ff79,22:ff7a

このコマンドは、文字のセット (>、<、*、:、"、?、¥、および |) を通常はファイル名で標準の文字としては使用されない日本語 Unicode 文字にマッピングします。このマッピングは、「desvol」という名前のボリュームに適用されます。

文字の制限

無効あるいは正しくない文字を表すのに使用される Unicode 文字が、通常はファイル名に使用されない文字であることを確認してください。そうでなければ、不要なマッピングが起きる可能性があります。

例えば、コロン (:) をハイフン (-) にマッピングしようと試みたが、ハイフン (-) はファイル名として正しく使用されていた場合、「a-b」と名付けられたファイルにアクセスを試みる Windows クライアントは、その要求が「a:b」という NFS 名にマッピングされることになります。これは目的とする結果ではありません。

再マッピングを試みる際には、以下の NFS 文字のリストを参照してください。

- 22 = 二重引用符 (")
- 2a = アスタリスク (*)
- 3a = コロン (:)
- 3c = 左不等号 (<)
- 3e = 右不等号 (>)
- 3f = 疑問符 (?)
- 5c = 円記号 (¥)

- 7c = パイプ (|)
- b1 = (±)

さらに、CIFS クライアントから Unicode 文字 0x0080 を含む名前のファイルまたはディレクトリーの作成あるいは名前変更を試みた場合、エラー・メッセージが表示されます。Unicode 文字 0x0080 は、ストレージ・システムではサポートされません。

ボリュームからの文字マッピングの消去

文字マッピングが必要でなくなった場合、(例えば、文字マッピングを使用していたアプリケーションをストレージ・システムから削除した場合)、`charmap` コマンドを使用してその文字マッピングをボリュームから消去することができます。

コマンド `charmap volname ""` を入力します。*volname* は、ストレージ・システム上のボリューム名です。

プロトコル間のファイル・ロックについて

ファイル・ロックは、他のユーザーによって先に開かれたファイルにユーザーがアクセスすることを防ぐために、クライアント・アプリケーションが使用する方式です。次に示すように、Data ONTAP はクライアントのプロトコルに応じてファイルをロックします。

クライアントが NFS クライアントの場合は、ロックは任意です。クライアントが CIFS クライアントの場合は、ロックは必須です。

NFS と CIFS のファイル・ロックの違いにより、CIFS アプリケーションによって開かれたファイルへの NFS クライアントによるアクセスの試行が失敗する場合があります。

以下は、CIFS アプリケーションによってロックされたファイルに、NFS クライアントがアクセスを試みた際に起こります。

- 混合あるいは NTFS qtree では、`rm`、`rmdir`、および `mv` のようなファイル操作は NFS アプリケーションの障害の原因となる可能性があります。
- NFS の読み取りおよび書き込み操作は、それぞれ CIFS `deny-read` (読み取り不可) および `deny-write` (書き込み不可) のオープン・モードによって拒否されます。
- ファイルの書き込み範囲が排他的 CIFS バイトロックによってロックされている場合、NFS 書き込み操作は失敗します。

例外: ストレージ・システム上の CIFS クライアントによるロックの設定の適用における 1 つの例外は、ストレージ・システムが `dump` コマンドを実行した場合です。 `dump` コマンドは、CIFS クライアントによる読み取りアクセスのファイル・ロック設定をすべて無視します。ファイル・ロックの無視は、ストレージ・システムがすべてのファイルをバックアップすることを可能にします。

注: CIFS アプリケーションによって開かれたファイルへの NFS クライアントによるアクセスの試行が失敗した場合は、`cifs terminate` コマンドを使用して、アクセスしたいオープン・ファイルを持つセッションを切断することができます。 `cifs`

sessions * コマンドまたは Server Manager (サーバー・マネージャー) を使用して、そのオープン・ファイルを持つセッションを決定することができます。ただし、CIFS セッションを終了すると、クライアントはエラーを受信する可能性があります。

読み取り専用ビットについて

読み取り専用ビットは 2 進数で 0 または 1 の値を持ち、ファイルが書き込み可能 (無効) か、あるいは読み取り専用 (有効) かを示すためにファイルごとに設定されています。

MS-DOS および Windows を使用している CIFS クライアントは、ファイルごとに読み取り専用ビットを設定することができます。NFS クライアントでは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を持たないため、ファイルごとに読み取り専用ビットを設定することはできません。

Data ONTAP は MS-DOS あるいは Windows を使用した CIFS クライアントがファイルを作成する際に、そのファイルに読み取り専用ビットを設定することができます。Data ONTAP は、ファイルが NFS クライアントと CIFS クライアントの間で共有される際にも、読み取り専用ビットを設定することができます。ソフトウェアによっては、NFS クライアントと CIFS クライアントによって使用される際に、読み取り専用ビットを有効にするように要求します。

Data ONTAP では、NFS クライアントと CIFS クライアントの間で共有されるファイルの読み取りおよび書き込み許可を適切に保持するために、読み取り専用ビットを以下の規則で扱います。

- NFS は読み取り専用ビットが有効なすべてのファイルを、書き込み許可ビットが有効ではないファイルとして扱います。
- NFS クライアントがすべての書き込み許可ビットを無効にし、それらのビットのうち少なくとも 1 つが以前は有効であった場合、Data ONTAP はそのファイルに関して読み取り専用ビットを有効にします。
- NFS クライアントが書き込み許可ビットを有効にした場合、Data ONTAP はそのファイルに関して読み取り専用ビットを無効にします。
- ファイルの読み取り専用ビットが有効で、NFS クライアントがそのファイルに関する許可を見つけようと試みる場合、そのファイルの許可ビットは NFS クライアントには送信されません。そのかわりに、Data ONTAP が書き込み許可ビットでマスクされた許可ビットを NFS クライアントに送信します。
- ファイルの読み取り専用ビットが有効で、CIFS クライアントが読み取り専用ビットを無効にする場合、Data ONTAP はそのファイルの所有者の書き込み許可ビットを有効にします。
- 読み取り専用ビットが有効なファイルは、root ユーザーによってのみ書き込み可能です。

注: ファイル許可への変更は、CIFS クライアントではすぐに有効になりますが、NFS クライアントでは属性キャッシュを有効にしている場合はすぐに有効になりません。

読み取り専用ビットがセットされているファイルの削除

Windows は、読み取り専用ビットが有効になっているファイルの削除を許可しません。いくつかのマルチプロトコル・ソース制御アプリケーションは、UNIX の削除セマンティクスを必要とします。これらのアプリケーションに関するファイルも、読み取り専用ビットが有効になっている場合は削除することができません。

読み取り専用ビットが有効になっているときに UNIX の削除セマンティクスを使用してファイルの削除を許可するには、次のコマンドを入力します。options cifs.perm_check_ro_del_ok on このオプションはデフォルトでは off です。

CIFS クライアントのための UNIX 資格情報の管理

ストレージ・システムへの接続時に、CIFS クライアントのユーザーは CIFS 資格情報を受信します。ユーザーは、Data ONTAP にコントロールされているリソースにアクセスするために、1 つ以上の UNIX 資格情報も所有する必要があります。

CIFS ユーザーが UNIX 資格情報を取得する方法

UNIX 資格情報は、UNIX スタイルのユーザー ID (UID) およびグループ ID (GID) から成り立ちます。

Data ONTAP は、以下の目的で UNIX 資格情報を使用します。

- ユーザーが UNIX スタイルのセキュリティを持つファイルへのアクセスを試行した場合、Data ONTAP は UID および GID を使用してユーザーのアクセス権を判別します。
- CIFS ユーザーを含むグループでグループ quota を使用したい場合、これらの CIFS ユーザーは UNIX 資格情報を持っている必要があります。グループ quota に関する詳細情報については、「ストレージ管理ガイド」を参照してください。

CIFS ユーザーがストレージ・システムへの接続を試行すると、Data ONTAP は CIFS ユーザーの UID およびプライマリー GID を判別しようと試みます。Data ONTAP が CIFS ユーザーの UID を判別できなかった場合、ユーザーはアクセスを拒否されます。

Data ONTAP は、UNIX パスワード・データベースを検索することで UNIX 資格情報を取得します。このデータベースは、NIS マップあるいは /etc/passwd ファイルで、ユーザーの UID を取得できます。データベースは、ストレージ・システムにアクセスする可能性があるすべてのユーザーに関するアカウントを含んでいます。各アカウントは UNIX スタイルのユーザー名と UID を含んでいます。

Data ONTAP が CIFS ユーザーの UID を取得するために、最初にユーザーの UNIX スタイルの名前を判別する必要があります。Data ONTAP は、ユーザーの Windows 名が UNIX 名と一致することは要求しません。/etc/usermap.cfg ファイルに情報を入力することで、Windows 名がそれぞれどのように UNIX 名にマッピングされるかを指定することができます。デフォルトのマッピングを受け入れた場合は、この情報を入力する必要はありません。デフォルトでは、Data ONTAP は UID を検索する際に Windows 名を UNIX 名として使用します。(ストレージ・システムは、検索の前に Windows 名の太文字を小文字に変換します。)

UNIX パスワード・データベースのユーザー名が Windows 名と一致した場合は、`/etc/usermap.cfg` ファイルにマッピング情報を提供する必要はありません。UNIX パスワード・データベースにユーザー名が見つからず、`wafld.default_unix_user` オプションが指定された場合は、このオプションで指定されたデフォルトのログイン名を使用します。`wafld.default_unix_user` オプションの設定に関する詳細情報については、`options(1)` のマニュアル・ページを参照してください。

Data ONTAP は、ユーザーの GID を以下の方法で取得します。

- Data ONTAP は、ユーザーのプライマリー GID を UNIX パスワード・データベースから取得します。UNIX パスワード・データベースの各アカウントは、そのユーザーのプライマリー GID を含みます。
- Data ONTAP は、ユーザーの他の GID をグループ・データベースから取得します。このデータベースは NIS グループ・マップあるいは `/etc/group` ファイルです。グループ・データベースでは、様々なグループのメンバーシップを定義します。

CIFS セッション情報を表示すると、接続された CIFS ユーザーの UNIX 資格情報を確認することができます。

確実な、意図された CIFS ユーザーのみの UNIX 資格情報の受信

`/etc/usermap.cfg` ファイルの編集、UNIX グループおよびユーザーの作成、および Windows ゲスト・ユーザー・アカウントの有効化によって、どの CIFS ユーザーが UNIX 資格情報を受信するかを構成することができます。

1. いくつかの Windows 名が UNIX 名と異なる場合や、いくつかの CIFS ユーザーがストレージ・システムにアクセスするのを防止したい場合は、`/etc/usermap.cfg` ファイルを編集します。
2. UNIX グループ・データベースにグループを作成します。
3. マッピングされた UNIX 名を持つ各 CIFS ユーザーについて、UNIX パスワード・データベースにユーザー・アカウントを入力します。
4. 管理者アカウントの名前を変更する場合は、少なくとも 1 つ以上の CIFS ユーザーが UNIX root アカウントにマッピングされていることを確認してください。
5. UNIX パスワード・データベースにエントリを持たない CIFS ユーザーをストレージ・システムにアクセスさせたい場合は、UNIX パスワード・データベースにデフォルト・ユーザー・アカウントを作成し、そのユーザーに対して `wafld.default_unix_user` オプションを設定します。
6. 非認証ユーザーをストレージ・システムにアクセスさせたい場合は、Windows ゲスト・ユーザー・アカウントを有効にします。

`/etc/usermap.cfg` ファイルでのエントリーの指定

Data ONTAP は、ユーザー名をマッピングするために `/etc/usermap.cfg` ファイルを使用します。最もシンプルな形式では、`/etc/usermap.cfg` の各エントリーは名前のペア (Windows 名と UNIX 名) を含んでいます。Data ONTAP は、Windows 名と UNIX 名を両方向に変換することができます。

このタスクについて

CIFS が始動するときに `/etc/usermap.cfg` ファイルがない場合は、デフォルト・ファイルが作成されます。そのファイルには、セキュリティを改善するのに役立つコメント化されたマッピング・エントリーの例が含まれます。

Data ONTAP が CIFS ユーザーからの接続要求を受信すると、エントリーがユーザーの Windows ドメインおよびユーザー名と一致するかを参照するために、`/etc/usermap.cfg` ファイルを検索します。

エントリーが検出されると、Data ONTAP はエントリーで指定された UNIX 名を使用して UNIX パスワード・データベースから UID および GID を検索します。UNIX 名が `ヌル・ストリング` の場合、Data ONTAP は CIFS ユーザーのアクセスを拒否します。

エントリーが検出されない場合は、Data ONTAP は Windows 名を小文字に変換し、UNIX 名が Windows 名と同じであると見なします。Data ONTAP はこの UNIX 名を使用して、UNIX パスワード・データベースから UID および GID を検索します。

Data ONTAP はファイルを順次にスキャンします。Data ONTAP は、最初のマッチング・エントリーをマッピングに使用します。

`/etc/usermap.cfg` ファイルの文字コードに関する情報については、「ストレージ管理ガイド」の `/etc` ディレクトリーのコンテンツに関する情報を参照してください。

次のフォーマットを使用して、各エントリーを指定します。[*IP_qualifier*:]
Windows_name [*direction*] [*IP_qualifier*:] *UNIX_name*

次のタスク

を使用してコメント行を始めることで、ファイルにコメントを埋め込むことが可能です。エントリーの末尾のコメントも、# を先頭につけることで許可されます。ブランク行は無視されます。

IP_qualifier フィールドについて:

IP_qualifier フィールドは、マッチングを限定することでユーザー名を絞り込む IP アドレスです。

IP qualifier は、以下のいずれかです。

- ビット表記の IP アドレス。サブネット・マスクにビット数を含めることでサブネットを指定することができます。例えば、192.4.1.0/24 は 192.4.1.0 クラス C サブネットを意味します。
- 名前。Data ONTAP は、最初にホスト名として使用されている名前を検証します。ホスト名データベース内にマッチングするホスト名を検出できない場合は、ネットワーク名として使用されている名前を検証します。
- ネットワーク名あるいは IP アドレス を含むサブネット・アドレスとサブネット・マスク (例えば、corpnet/255.255.255.0)

注: Data ONTAP は IP qualifier をマッチングにのみ使用します。IP qualifier が Map エントリーの宛先側に存在する場合は、Data ONTAP はその IP qualifier からのログイン要求を考慮しません。

Windows_name フィールドについて:

Windows_name フィールドは Windows ドメイン名 (オプション) と Windows ユーザー名で構成されています。

Map エントリーの送信側で、ドメインはユーザーが属するドメインを指定します。Map エントリーの宛先側で、マッピングされた UNIX エントリーに使用されるドメインを指定します。エントリー内のアカウント名がローカル・ユーザー・アカウントの場合は、Windows ドメイン名はストレージ・システム名です。

Windows_name フィールドでドメイン名を省略する場合は、ストレージ・システムがインストールされたドメインであると見なされます。ストレージ・システムがローカル・ユーザー・アカウントを認証に使用する場合は、ドメイン名はストレージ・システム名です。

以下の方法でアスタリスク (*) をワイルドカード文字として使用できます。

- すべてのドメイン内の特定の名前が特定の UNIX 名にマッピングされていることを示すために、送信側で使用できます。
- 特定の UNIX 名がすべての信頼されたドメイン内の Windows 名にマッピングされていることを示すために、宛先側で使用できます。マッピングに使用される信頼されたドメインは、Data ONTAP がどこで最初のマッチングした Windows 名を検出するかによって決まります。Data ONTAP は cifs.search_domains オプションで指定した信頼されたドメインのみを、信頼されたドメインが指定されている順序で検索します。このオプションを設定しない場合は、Data ONTAP は指定された順序なしで、すべての信頼されたドメインを検索します。

ユーザー名がスペースやシャープを含む場合は、例えば "bob smith" あるいは "eng#lab"¥"joe" のように、名前を二重引用符で囲みます。

注: ¥ を引用符で囲まないでください。

Windows 名にアスタリスク (*) を使用することができます。アスタリスクの使用方法についての詳細は、254 ページの「ユーザー名におけるワイルドカード文字に関するガイドライン」を参照してください。

Map エントリーの宛先側で ユーザー名が空やブランク (" " として指定) の場合、マッチングした UNIX 名はアクセスが拒否されます。いくつか、あるいはすべての UNIX ユーザーへのアクセスを拒否するには、ブランクのユーザー名を持つエントリーを使用してください。IP_qualifier との連結においてこれらのエントリーを使用する場合は、特定のホストあるいはサブネットを除いたすべての UNIX ユーザーを排除することができます。

Direction フィールドについて:

Direction フィールドは、マッピングの方向を表します。

Direction フィールドは、以下の表にある値の 1 つである可能性があります。

Direction フィールドの値	意味
==	マッピングは双方向です。エントリーは Windows から UNIX、および UNIX から Windows にマッピングしています。 Direction フィールドの省略は == が指定されているのと同じ意味を持ちます。
<=	エントリーは UNIX から Windows にマッピングしています。
=>	エントリーは Windows から UNIX にマッピングしています。

UNIX_name フィールドについて:

UNIX_name フィールドは、UNIX パスワード・データベース内の UNIX 名です。

Map エントリーの宛先側で UNIX_name フィールドが空やブランク ("" として指定) の場合、指定された送信元の名前はログインできません。 Windows ユーザーは、たとえネットワークの参照中にストレージ・システムを見ることができても、ストレージ・システムにログインすることはできません。

UNIX 名にアスタリスク (*) を使用することができます。アスタリスクはワイルドカード文字として考慮されます。それはあらゆるユーザーを意味します。 Windows 名や UNIX 名にアスタリスクが含まれている場合は、これらのガイドラインを思い出してください。

- マッピングの送信側にアスタリスクがある場合は、あらゆるユーザーが宛先側の指定の名前にマッピングされています。
- 宛先側がアスタリスクを含んでおり、送信側はアスタリスクを含んでいない場合は、マッピングはされていません。 Data ONTAP は、特定の名前をアスタリスクを含んだ名前に明示的にマッピングすることはありません。
- 送信側と宛先側の両方がアスタリスクを含む場合は、一致する名前がマッピングされています。

Data ONTAP が /etc/usermap.cfg 内のドメイン名を解釈する方法:

Data ONTAP がドットを含んだ /etc/usermap.cfg ファイル内のドメイン名を解釈する方法は、ストレージ・システムが Windows NT ドメインにあるか、あるいは Windows Active Directory ドメインにあるかによって決まります。

ストレージ・システムが Windows NT ドメインにインストールされている場合、ドメイン名フィールドの長さがドメイン名を解釈する方法に影響します。

ストレージ・システムが Windows Active Directory ドメインにインストールされている場合、Data ONTAP は Windows サーバーを同じ方法でドメイン名を解釈します。

ストレージ・システムが Windows NT ドメインにある場合、Data ONTAP は `domain¥user` フォーマットでドットを含むドメイン名を解釈する場合は、以下の規則に従います。

- `domain` が 15 文字以下の場合、Data ONTAP はドットを含めてストリング全体をドメイン名の NetBIOS 形式として認識します。例えば、`my_company.com` は、以下の名前におけるドメイン名の NetBIOS 形式です。
`my_company.com¥john_smith`
- `domain` が 16 文字以上の場合、ドットは分離文字として扱われ、最初のドットの前のストリングがドメイン名の NetBIOS 形式になります。例えば、`engineering` は以下の名前のドメイン名の NetBIOS 形式です。
`engineering.1234567890corporation.com¥john_smith`

ストレージ・システムが Windows Active Directory ドメインにある場合、ユーザー名を `domain¥user` フォーマットで指定することができます。 `domain` での最初のドットの前のストリングが、ドメイン名の NetBIOS 形式で、`domain` のストリング全体は DNS ドメイン名です。

例えば、以下の名前では `engineering` はドメイン名の NetBIOS 形式で、`engineering.1234567890corporation.com` は DNS ドメイン名です。

`engineering.1234567890corporation.com¥john_smith`

usermap.cfg エントリーの例:

usermap.cfg エントリーの例をいくつか示します。

以下の表は、いくつかのシンプルな /etc/usermap.cfg エントリーを示します。

エントリー	意味
<code>"Bob Garj" == bobg</code>	Windows 名 Bob Garj と UNIX 名 bobg は双方向にマッピングされています。
<code>mktg¥Roy => nobody</code>	mktg ドメインにある Windows 名 Roy が、UNIX 名 nobody にマッピングされています。このエントリーは、UNIX 形式のセキュリティによって Roy がファイルへの制限されたアクセス権でログインすることを可能にします。
<code>engr¥Tom => ""</code>	engr ドメインのユーザー名 Tom でのログインを許可しません。

以下の表は、Windows 名におけるアスタリスクの使用のいくつかの例を示しています。

エントリー	意味
<code>uguest <= *</code>	すべての未一致の UNIX 名を Windows ユーザー <code>uguest</code> にマッピングします。
<code>*¥root => ""</code>	すべてのドメインから Windows 名 <code>root</code> でのログインを許可しません。

エントリー	意味
corporate¥* == pcuser	corporate ドメイン内のすべてのユーザーを UNIX 名 pcuser にマッピングします。アスタリスクが Windows ユーザー名に使用されているため、UNIX 名 pcuser はマッピングされません。
Engineer == *	すべての UNIX 名が、ストレージ・システムのドメイン内の Windows 名 Engineer にマッピングされます。アスタリスクが UNIX ユーザー名に使用されているため、Windows 名 Engineer はマッピングされません。
以下のエントリーのいずれかです。 - homeusers¥* * - homeusers¥* == *	すべての UNIX ユーザーが、homeusers ドメイン内の一致する名前にマッピングされます。例えば、UNIX ユーザー名 bob は homeusers¥bob にマッピングされます。 homeusers ドメインのすべての Windows ユーザーは、一致する UNIX 名にマッピングされます。例えば、homeusers ドメインの Windows ユーザー名 john は、UNIX 名 john にマッピングされます。

以下の表は、IP qualifier に関するいくつかの例を示しています。

エントリー	意味
Engineering¥* <= sunbox2:*	ホスト名 sunbox2 からの UNIX 名は、Engineering ドメイン内の同じ名前にマッピングされます。
Engineering¥* <= 192.9.200.70:*	IP アドレス 192.9.200.70 からの UNIX 名は、Engineering ドメイン内の同じ名前にマッピングされます。
"" <= 192.9.200.0/24:*	192.9.200.0 サブネットからのすべての NFS 要求は、このサブネットからの UNIX 名がヌル・ストリングにマッピングされているため、拒否されます。
192.9.200.0/24:test-dom¥* => ""	test-dom ドメイン内のすべてのユーザーは、192.9.200.0 サブネットからのアクセスを拒否されます。

エントリー	意味
¥ == corpnet/255.255.0.0:*	すべてのドメインからのすべてのユーザー名は、同じ UNIX 名にマッピングされます。ドメイン全体でユーザー名が固有でない場合、このエントリーは異なる Windows 名を同一の UNIX 名にマッピングする原因となる可能性があります。 IP qualifier が唯一のマッチングであるため、corpnet/255.255.0.0: の指定は Windows を UNIX にマッピングする結果に影響しません。 マッピングが双方向であるため、corpnet/255.255.0.0 ネットワークからのすべての UNIX ユーザー名は、ストレージ・システムの信頼されたドメインの 1 つにある同じ名前にマッピングされます。

ユーザー名のマッピングに関するガイドライン:

エントリーを単純かつ理解しやすくするために、いくつかのガイドラインに従う必要があります。

マッピングを実行する際には、以下のガイドラインに注意する必要があります。

- Windows ユーザー名と UNIX ユーザー名を、可能な限り同じにします。名前が同一であれば、/etc/usermap.cfg ファイルにマッピングのエントリーを作成する必要がありますがありません。
- 以下のような混乱するマッピング・エントリーを作成しないようにしてください。"tome s" => tjs bill <= tjs
- IP qualifier を使用してユーザー別にマッピングしないようにしてください。例えば、UNIX ユーザー tjs を UHOST1 から Windows ユーザー「Tom S」にマッピングしたにもかかわらず、UNIX ユーザー tjs を UHOST2 からは Windows ユーザー「Smith」にマッピングすると混乱します。IP qualifier は、制限されたアクセスにのみ使用してください。

セキュリティ強化に推奨されるエントリー:

認可されていないユーザーがストレージ・システムにアクセスすることを防ぐために、/etc/usermap.cfg ファイルにいくつかのエントリーを追加することをお勧めします。

Data ONTAP はマッピングを判別するために最初のマッチング・エントリーを使用するため、これらの推奨されるエントリーをファイルにコピーする際には、エントリーの順番が重要であることを覚えておいてください。

マッピング・エントリー	意味
*¥root => nobody	root と命名されたあらゆる Windows ユーザーがログインできますが、UNIX のアクセス権は持っていません。別にマッピングされるべき root と命名された Windows ユーザー名のインスタンスについて、/etc/usermap.cfg ファイルの前の方に明示的にマッピングのエントリーを追加します。
guest <= administrator guest <= root	最初のエントリーは、(管理者アカウントが名前変更されていない場合) Windows 管理者アカウントが UNIX からスプーフィングされるのを防ぎます。 2 番目のエントリーは、UNIX ユーザー root を Windows のゲスト・アカウントにマッピングします。 2 番目のエントリーを /etc/usermap.cfg ファイルの最後近く、root 特権がある UNIX ホストあるいはサブネットに関する明示的なマッピング・エントリーの後に、入力します。
** => "" "" <= *	ファイルの最後に位置するこれらのエントリーは、他のマッピングが発生することを防ぎます。エントリーが一致しない場合、同じ名前を試行するというデフォルトの動作を無効にします。

NFS クライアントの確認:

マルチプロトコルのストレージ・システムでは、usermap.cfg ファイルでマッピングされているクライアントのみを許可するように NFS アクセスを制限することができます。

このタスクについて

主として CIFS クライアントを扱う一方で、特定の既知の (IP マッピングされた) NFS クライアントからの接続を許可したい 非 Kerberos 環境においては、このセキュリティ制限は最適であると考えられます。 nfs.require_valid_mapped_uid オプションに関する詳細情報については、options(1) のマニュアル・ページを参照してください。

Windows アカウントの root へのマッピング

ご使用の環境に CIFS クライアントしかなく、ストレージ・システムがマルチプロトコル・ストレージ・システムとしてセットアップされている場合は、ストレージ・システム上のファイルにアクセスするためには少なくとも 1 つ以上の root 特権を持つ Windows アカウントが必要です。そうでなければ、/etc ディレクトリーにいくつかの構成ファイルを含む場合がある UNIX スタイルのセキュリティを持つファイルへのアクセス権を持たないために、ストレージ・システムを管理することができません。

このタスクについて

ただし、ご使用のストレージ・システムが NTFS のみでセットアップされている場合は、`/etc` ディレクトリーは管理者グループによる Data ONTAP 構成ファイルへのアクセスを有効にするファイル・レベル ACL を持っています。

以下を実施したい場合は、	以下を実行してください。
管理者のグループのアカウントを <code>root</code> にマッピングする	<code>waf1.nt_admin_priv_map_to_root</code> オプションが <code>on</code> に設定されていることを確認します。 結果: アカウントを <code>root</code> にマッピングしている <code>/etc/usermap.cfg</code> エントリーがない場合でも、管理者グループのすべてのアカウントが <code>root</code> と見なされます。管理者グループに属するアカウントを使用してファイルを作成した場合、UNIX クライアントからファイルを表示するときには <code>root</code> がファイルを所有しています。
選択されたアカウントを <code>root</code> にマッピングする	<code>root</code> にマッピングする各アカウントについて、<code>/etc/usermap.cfg</code> エントリーを追加します。 注: マルチプロトコル・ストレージ・システム上で <code>root</code> にマッピングする Windows アカウントを、少なくとも 1 つ以上所有していることが重要です。そうでなければ、<code>/etc</code> ディレクトリー内の構成ファイルにアクセス可能なアカウントがありません。次に、<code>waf1.nt_admin_priv_map_to_root</code> オプションを、次のコマンドを入力して無効にします。 <pre>options waf1.nt_admin_priv_map_to_root off</pre> 結果: 管理者グループのアカウントは、<code>root</code> にマッピングされていません。UNIX スタイルのセキュリティーを持つファイルにアクセスするために使用できるのは、<code>/etc/usermap.cfg</code> ファイルで <code>root</code> にマッピングしたこれらのアカウントのみです。管理者グループの各アカウントは個別の UNIX ID を持ちます。

UNIX 名の UID および GID へのマッピング

CIFS ユーザーが UID および GID を持つために、UNIX パスワード・データベースにユーザーの UNIX 名と一致する UNIX アカウントを作成する必要があります。

このタスクについて

各 UNIX 名について、Data ONTAP は UID およびプライマリー GID を UNIX パスワード・データベースから取得します。Data ONTAP は、UNIX 名のためのセカ

ンダリー GID を UNIX グループ・データベースから取得します。パスワード・データベースに UNIX 名を持たない CIFS ユーザーは、デフォルト UNIX ユーザー・アカウントを有効にしている場合は UID を取得することができます。

cifs setup を実行する前にご使用のストレージ・システムが NIS クライアントであった場合は、Data ONTAP は /etc/passwd ファイルを自動的に作成しません。 cifs setup を実行するときに NIS が有効ではなかった場合、Data ONTAP は /etc/passwd ファイルを自動的に作成します。

NIS サーバーが失敗し、ストレージ・システムが /etc/passwd ファイルを所有していない場合、CIFS ユーザーはストレージ・システムに接続することができません。 /etc/passwd ファイルを作成することで、NIS が使用不可の場合でも、確実にストレージ・システムが CIFS ユーザーのための UNIX 資格情報を取得できるようになります。

デフォルトの /etc/passwd ファイルは、以下の UNIX 名のエントリーを含んでいます。

- root
- pcuser
- nobody

/etc/group および /etc/passwd ファイルのフォーマットに関する情報については、「ストレージ管理ガイド」を参照してください。

以下を使用したい場合、	以下を実行してください。
NIS (/etc/passwd ファイルは使用しない)	各 CIFS ユーザーの UNIX 名を NIS パスワード・マッピングに追加します。
/etc/passwd ファイル (NIS は使用しない)	各ユーザーの UNIX 名について /etc/passwd ファイルにエントリーを追加します。 Data ONTAP がパスワード・エントリーを作成するコマンドをサポートしないため、ホストに /etc/passwd ファイルを作成するためには passwd コマンドをサポートする UNIX ホストを使用します。次に、ホストからストレージ・システムにファイルをコピーします。

UNIX デフォルト・ユーザー・アカウントの有効化あるいは無効化

ときどきストレージ・システムに接続する必要があるが、UNIX パスワード・データベースへの個々のエントリーは必要ないユーザーがある場合、UNIX デフォルト・ユーザー・アカウントを作成する必要があります。これらのユーザーは、ストレージ・システムに接続するために、デフォルト・ユーザー・アカウントを使用することができます。

このタスクについて

デフォルト・ユーザーのデフォルトの UNIX 名は pcuser です。他の名前を wafl.default_unix_user オプションで指定することができます。このオプションがヌル・ストリングで設定されている場合は、誰も UNIX デフォルト・ユーザーとして

ストレージ・システムにアクセスすることができません。つまり、ストレージ・システムにアクセスするためには、各ユーザーがパスワード・データベースにアカウントを持っている必要があります。

デフォルト・ユーザー・アカウントを使用してストレージ・システムに接続するためのユーザーについて、ユーザーは以下の前提条件を満たしている必要があります。

- ユーザーは認証されています。
- ユーザーは信頼されたドメインにいます。
- ユーザー名は `/etc/usermap.cfg` ファイルのヌル・ストリングにマッピングしていません。

quota が有効な場合は、デフォルト・ユーザー・アカウントは他のユーザーと同じ方法で quota 制限の対象です。例えば、デフォルト・ユーザー名が `pcuser` で、デフォルト・ユーザーの quota が `/vol/vol0` に適用されている場合、`pcuser` はこのデフォルト・ユーザーの quota で制限されます。デフォルト・ユーザーの quota に関する詳細情報については、「*Data ONTAP ストレージ管理ガイド*」の quota を使用したディスク・スペース管理に関する章の、デフォルト・ユーザーが所有するディスク・スペースをどのようにカウントするかについてのセクションを参照してください。

以下を実施したい場合、	以下を実行してください。
UNIX デフォルト・ユーザー・アカウントを無効にする	次のコマンドを入力します。options <code>waf1.default_unix_user ""</code> 結果: パスワード・データベースにアカウントがあるユーザーのみが、ストレージ・システムにアクセスできます。
UNIX デフォルト・ユーザー・アカウントを有効にする	NIS パスワード・データベースあるいは <code>/etc/passwd</code> ファイルのいずれかに、 <code>pcuser</code> アカウントに関するエントリーを作成します。
UNIX デフォルト・ユーザー・アカウントの名前を <code>pcuser</code> から他の名前に変更する	<code>waf1.default_unix_user</code> オプションを UNIX デフォルト・ユーザー・オプションの新規の名前に設定する。 例えば、デフォルト・ユーザー名を <code>someuser</code> に変更するには、次のコマンドを入力します。options <code>waf1.default_unix_user someuser</code>

Windows ゲスト・ユーザー・アカウントの有効化あるいは無効化

Windows ゲスト・ユーザー・アカウントを有効にする効果は、ストレージ・システムがどのようにユーザーを認証するかによって決まります。

このタスクについて

以下のようなことが起こる可能性があります。

- ストレージ・システムがユーザーの認証にドメイン・コントローラーあるいはローカル・ユーザー・アカウントを使用する場合、Windows ゲスト・ユーザー・アカウントを有効にすることは、信頼されていないドメインからログインするユーザー

ザーがストレージ・システムに接続可能であることを意味します。これらのユーザーは、Guest アカウントのために明確に作成した UNIX UID を使用します。Guest としてログインしたユーザーは、ホーム・ディレクトリーを持ちません。

- ストレージ・システムがユーザーの認証に UNIX パスワード・データベースを使用する場合、Windows ゲスト・ユーザー・アカウントを有効にすることは、Guest としてログインしたユーザーがホーム・ディレクトリーを持たないこと以外は、UNIX デフォルト・アカウントを有効にすることと同じ効果があります。

以下を実施したい場合、	以下を実行してください。
Windows ゲスト・ユーザー・アカウントを無効にする	次のコマンドを入力します。options cifs.guest_account ""
Windows ゲスト・ユーザー・アカウントを有効にする	ゲスト・アカウントが使用するユーザー・アカウントを NIS パスワード・データベースあるいは /etc/passwd ファイルに作成します。次に、次のコマンドを入力して UNIX パスワード・データベースで使用するゲスト・ユーザー・アカウント名を指定します。 options cifs.guest_account <i>unix_name</i> <i>unix_name</i> は、UNIX パスワード・データベース内のユーザー・アカウント名です。

SID-to-name マッピング・キャッシュの管理

CIFS は、しばしばユーザー認証、quota 管理、コンソール・コマンド処理、および様々な RPC 応答のために、セキュリティ ID (SID) とユーザーおよびグループ名を両方向にマッピングすることを要求されます。SID-to-name マッピング・キャッシュは、SID を Windows 2000 より前のユーザーおよびグループ名にマッピングするエントリーを含みます。

このタスクについて

ストレージ・システムは、ドメイン・コントローラーに照会することで SID-to-name マッピング情報を取得します。同じ名前の複数の検索を最小化するために、ドメイン・コントローラーから受信した SID-to-name 情報は、ストレージ・システム上の SID-to-name マッピング・キャッシュに保存されます。

SID-to-name マッピング・キャッシュは、デフォルトでストレージ・システム上で有効になっています。エントリーの存続時間の変更、エントリーの消去、あるいは SID-to-name マッピング・キャッシュのオフ/オンによって、手動でキャッシュをコントロールすることができます。キャッシュは、CIFS が終了あるいは再始動しても持続しますが、リブートあるいはテークオーバーおよびギブバックを越えては持続しません。

ストレージ・システムが SID-to-name マッピング情報を要求すると、まず SID-to-name マッピング・キャッシュで一致するエントリーを探します。マッチング・エントリーが検出できない場合、あるいは有効期限が切れたマッチング・エントリーが検出された場合は、ストレージ・システムは現在のマッピング情報につい

て適切なドメイン・コントローラーに照会します。ドメイン・コントローラーが使用不可の場合、有効期限が切れたマッピング・エントリーがストレージ・システムに使用される場合があります。

名前検索に SID-to-name マッピング・キャッシュを使用する主な利点は以下のとおりです。

- 許可のパフォーマンス向上
- マッピング操作を実行するコンソール・コマンドに対する高速なユーザー応答

SID-to-name マッピング・キャッシュの有効化あるいは無効化

cifs.sidcache.enable オプションを on あるいは off に設定することで、SID-to-name をそれぞれ有効あるいは無効にすることができます。

以下を実施したい場合、	以下を実行してください。
SID-to-name マッピング・キャッシュを有効にする	次のコマンドを入力します。options cifs.sidcache.enable on
SID-to-name マッピング・キャッシュを無効にする	次のコマンドを入力します。options cifs.sidcache.enable off

SID-to-name マッピング・エントリーの存続期間の変更

SID-to-name マッピング・エントリーの存続期間を、cifs.sidcache.lifetime オプションの設定によって変更することができます。

コマンド options cifs.sidcache.lifetime *time* を入力します。*time* は、有効期限が切れる前に新規のマッピング・エントリーが使用される分数です。

SID-to-name マッピング・キャッシュのすべてあるいは一部の消去

1 週間より長く経過して有効期限が切れたエントリーは、定期的に SID-to-name マッピング・キャッシュから自動的に消去されます。ただし、ユーザーがそのアカウントあるいはユーザー名を変更した場合は、手動で SID-to-name マッピング・キャッシュのエントリーを消去することをお勧めします。あるいは、ドメイン・コントローラーが使用不可のときにストレージ・システムが有効期限が切れたエントリーを使用することを防ぐために、すべての SID-to-name マッピング・キャッシュ・エントリーを手動で消去することをお勧めします。

以下を実施したい場合、	以下を実行してください。
すべての Windows ドメイン、ユーザー、グループ、および SID の SID-to-name マッピング・キャッシュ・エントリーを消去する	次のコマンドを入力します。cifs sidcache clear all

以下を実施したい場合、	以下を実行してください。
特定の Windows ドメインの SID-to-name マッピング・キャッシュ・エントリーを消去する	次のコマンドを入力します。cifs sidcache clear [domain] <i>domain</i> は、消去したいキャッシュ・エントリーの Windows ドメインです。 ドメインを指定しない場合は、ストレージ・システムのホーム・ドメインのエントリーがキャッシュから消去されます。
特定のユーザーあるいはグループの SID-to-name マッピング・キャッシュ・エントリーを消去する	次のコマンドを入力します。cifs sidcache clear user <i>username</i> ここで <i>username</i> は、キャッシュから消去したい特定の Windows ユーザーあるいはグループのエントリーです。ユーザー名は以下の方法で指定することができます。 • <i>domain\username</i> • <i>username</i> ユーザー名がドメインなしで指定された場合、ストレージ・システムのホーム・ドメインがドメインとして使用されます。
特定の SID の SID-to-name マッピング・キャッシュ・エントリーを消去する	次のコマンドを入力します。cifs sidcache clear sid <i>textualSid</i> ここで <i>textualSid</i> は、キャッシュから消去したい SID のテキスト形式です。標準「S-1-5...」構文を使用して SID を指定します。 例: cifs sidcache clear sid S-1-5-21-4503-17821-16848-500

LDAP サービスの使用

Data ONTAP は、ユーザー認証、ファイル・アクセス許可、NFS と CIFS の間のユーザー検索およびマッピング・サービス、および LDAP over SSL のための LDAP をサポートします。

このタスクについて

LDAP サーバーによって、ユーザー情報を中央に集約して保持することができます。その結果、ネットワーク上にない各ストレージ・システムに関する個々の構成ファイルを保持する必要がなくなります。ネットワーク上にいくつかのストレージ・システムがある場合、ユーザー情報を中央に保持することで、ユーザーあるいはグループを追加または削除するたびに各ストレージ・システム上でこれらのファイルを更新する必要がなくなります。

LDAP サーバー上にユーザー・データベースを保管すると、ユーザー情報を LDAP データベースで検索するようにストレージ・システムを構成することができます。例えば、ご使用の LDAP サーバーで、コンソールと rsh、Telnet、HTTP、HTTPS、

および SSH プロトコルの管理ユーザーのためのログインおよびパスワードを保管することができ、それらを中央で管理することが可能になります。

Data ONTAP の LDAP サポートは、以下のタイプの LDAP サーバーを含みます。

- Netscape
- iPlanet
- OpenLDAP
- Windows Active Directory
- Novell NDS

Data ONTAP は署名が必要な LDAP サーバーへの接続をサポートします。LDAP 署名のサポートは、デフォルトで有効にされています。

LDAP サービスの構成

このセクションでは、LDAP データベースに接続するための Data ONTAP の構成を助ける情報を記載しています。

汎用の検索ベースおよび有効範囲の指定

LDAP ベースはユーザー情報が保管される LDAP ツリーの識別名です。LDAP サーバーに送信されるすべての検索要求は、さらに特定のベースおよび有効範囲の検索値 (例えば、`ldap.base.passwd` あるいは `ldap.base.group`) によって制限されていなければ、`ldap.base` オプションの値で指定された検索ベースおよび有効範囲に制限されます。

コマンド `options ldap.base name` を入力します。*name* は、ベース識別名です。スペースを含む名前は引用符で囲みます。

例

```
options ldap.base "o=networkappliance,c=us"
```

ユーザー検索のための検索ベースおよび有効範囲値の指定

必要ではない場合も、LDAP データベースのユーザー・アカウント・ブランチへのユーザー検索照会を制限するために、LDAP 検索要求のベースおよび有効範囲値を具体的に指定することができます。すべての照会の検索ベースおよび有効範囲を制限することで、パフォーマンスが大きく向上します。

このタスクについて

注: 以下の手順を使用して割り当てた値は、ユーザー・マッピングのために個別のベースおよび有効範囲値を入力しない限りは、すべての LDAP 検索に適用されます。

1. パスワード検索のためのベースおよび有効範囲の検索値を、LDAP データベースに定義するときに `ldap.base.passwd` オプションの値を指定することで設定します。例: `options ldap.base.passwd "ou=People,dc=companydomain,dc=com"`
2. グループ検索のためのベースおよび有効範囲の検索値を、LDAP データベースに定義するときに `ldap.base.group` オプションの値を指定することで設定します。例: `options ldap.base.group "ou=Groups,dc=companydomain,dc=com"`

タスクの結果

いったん `ldap.base.passwd` および `ldap.base.group` に関する検索ベースおよび有効範囲値を指定すると、これらの値はパスワードおよびグループ検索のための `ldap.base` に関する検索ベースおよび有効範囲の設定より優先されます。

LDAP サーバーの指定

`ldap.servers` オプションを設定することで、LDAP 照会のために使用される LDAP サーバーを指定することができます。

コマンド `options ldap.servers "name[ name...]"` を入力します。 *name* は、LDAP サーバーの名前です。引用符で囲んだスペース区切りのリストを使用して、複数のサーバー名を入力することができます。 Data ONTAP は、これらのサーバーを指定した順番に接続の確立を試みます。

タスクの結果

注: Windows LDAP サーバーは、次の条件に当てはまらない場合は SASL の代わりに単純な認証を使用します。Windows LDAP サーバーを IP アドレスではなく名前で指定する場合、および Windows LDAP サーバーの IP アドレスおよび名前を `/etc/hosts` ファイルで指定する場合。 `/etc/hosts` ファイルの編集に関する詳細情報については、「System Administration Guide」を参照してください。

例

```
options ldap.servers "server1 server2"
```

優先 LDAP サーバーの指定

より速いリンク上にある LDAP サーバーを、優先サーバーとして指定することをお勧めします。

コマンド `options ldap.servers.preferred "name [name...]"` を入力します。 *name* は、優先 LDAP サーバーの名前です。引用符で囲んだスペース区切りのリストを使用して、複数のサーバー名を入力することができます。

例

```
options ldap.servers.preferred "server1 server2"
```

LDAP の有効化あるいは無効化

`ldap.enable` オプションを `on` あるいは `off` に設定することで、LDAP をそれぞれ有効あるいは無効にすることができます。

以下を実施したい場合、	以下を実行してください。
LDAP を有効にする	次のコマンドを入力します。 <code>options ldap.enable on</code>
LDAP を無効にする	次のコマンドを入力します。 <code>options ldap.enable off</code>

LDAP トラフィックのための SSL の有効化あるいは無効化

ldap.ssl.enable オプションを on あるいは off に設定することで、LDAP トラフィックの Secure Sockets Layer (SSL) 暗号化をそれぞれ有効あるいは無効にすることができます。

以下を実施したい場合、	以下を実行してください。
LDAP の SSL を有効にする	次のコマンドを入力します。options ldap.ssl.enable on
LDAP の SSL を無効にする	次のコマンドを入力します。options ldap.ssl.enable off

次のタスク

LDAP の SSL を有効に設定するのに加えて、root 権限が署名された証明書がストレージ・システムにインストールされている必要があります。

注: 同じ証明書署名機関が、ストレージ・システム上の証明書およびサーバー上の証明書の両方を発行する必要があります。

LDAP トラフィックのための SSL のルート証明書のインストール

keymgr コマンドを使用して、ストレージ・システム上の LDAP トラフィックを暗号化する Secure Sockets Layer (SSL) を使用するための、ルート証明書をインストールすることができます。

1. 優先の信頼された署名機関からストレージ・システムに証明書をダウンロードします。ストレージ・システム上の証明書の位置を覚えておきます。
2. 次のコマンドを入力します。keymgr install root *certificate_filename*
certificate_filename は、証明書のための完全なファイル名です。keymgr コマンドが証明書をインストールした後、ストレージ・システム上に置いたコピーを削除することができます。

例 keymgr install root /etc/my_cert

注: 同じ証明書署名機関が、ストレージ・システム上の証明書およびサーバー上の証明書の両方を発行する必要があります。

3. LDAP ポートを、ポート 636 に設定します。

/etc/nsswitch.conf ファイルへの ldap エントリーの追加

UNIX クライアント認証のための LDAP を有効にするために、/etc/nsswitch.conf ファイルに ldap エントリーを追加することができます。

1. 編集のためにストレージ・システム上の /etc/nsswitch.conf ファイルを開きます。
2. パスワード、グループ、およびネットグループの行で、次を入力します。ldap

オプションで、パスワードの行に files または nis、あるいはその両方を追加することができますが、ユーザー情報を取得するためのプライマリー・メカニズムとして LDAP を使用したい場合は、それらを ldap の後に入力する必要があります。

例

```
passwd: ldap files nis
```

3. このファイルを保存します。

管理ユーザー名の指定

ご使用の環境で匿名の認証が動作しない場合、UID および GID の検索のための管理照会に使用される管理ユーザー名を指定する必要があります。

コマンド `options ldap.name name` を入力します。*name* は、管理照会に使用される LDAP 識別名です。ベスト・プラクティスとして、この名前は LDAP データベースに読み取り専用のアクセス権を持つユーザー名にするべきです。スペースを含む名前は引用符で囲みます。

例

```
options ldap.name "cn=root,o=networkappliance,c=us"
```

管理パスワードの指定

`ldap.passwd` オプションを設定することで、管理パスワードを設定することができます。

コマンド `options ldap.passwd password` を入力します。*password* は、管理ユーザーのためのパスワードです。パスワードは、アスタリスクの連続で表示されます。

Enabling the centraliz管理ユーザーの集中管理の有効化

コンソール、および rsh、Telnet、HTTP、および HTTPS プロトコルの Data ONTAP 管理ユーザーを、適切なオプションを設定することで集中管理することができます。

1. `security.admin.authentication` オプションのボリュームが `nsswitch` を含んでいることを確認してください。

例えば、以下のコマンドのいずれかを入力します。

```
options security.admin.authentication nsswitch
```

```
options security.admin.authentication internal,nsswitch
```

```
options security.admin.authentication nsswitch,internal
```

2. `security.admin.nsswitchgroup` オプションの値を、管理アクセス権を生成したいユーザーを指定する `nsswitch.conf` ファイルの範囲内のグループ名に設定します。

例

組織のすべてのエンジニアに管理アクセス権を生成したい場合、`engineers` と呼ばれるグループを作成し、組織内のすべてのエンジニアをそのグループに追加した後、次のコマンドを入力します。

```
options security.admin.nsswitchgroup engineers
```

LDAP ポートの指定

LDAP サーバーが LDAP のデフォルトのポート (ポート 389) 以外を使用するようにセットアップされている場合、LDAP 照会のために使用するポートを指定する必要があります。

コマンド `options ldap.port N` を入力します。N は、LDAP ポート番号です。

LDAP サーバー・オプションの優先順位

Data ONTAP は、ご使用の LDAP サーバー・オプション設定に基づいて LDAP サーバーを選択します。

サーバー指定オプション	サーバー選択順序
ldap.preferred.servers	指定すると、このオプション値にリストされているサーバーが、リストの順序に応じて最初に試行されます。
ldap.servers	ldap.preferred.servers が指定されていない場合、あるいは指定されたサーバーが使用不可の場合、このオプション値で指定されたサーバーがリストの順番に応じて試行されます。
ldap.ADdomain	ldap.preferred.servers と ldap.servers がいずれも指定されていない、または使用不可の場合、このオプション値に指定されたサーバーがドメイン・コントローラーの選択方法を使用して試行されます。

現行の認証および権限の管理

UNIX および Windows クライアントの LDAP 認証を有効にすることができます。さらに、Windows クライアントから UNIX ファイルへのアクセス、および UNIX クライアントから NTFS あるいは混合のファイルへのアクセスの LDAP 権限を有効にすることができます。

LDAP ベースの UNIX クライアント認証の有効化

/etc/nsswitch.conf ファイルのパスワード行に ldap が入力されていることを確認することで、LDAP ベースの UNIX クライアント認証を有効にすることができます。

LDAP ベースの Windows クライアント認証の有効化

/etc/nsswitch.conf ファイルの passwd 行に ldap を追加することに加えていくつかの手順を実行することで、LDAP サーバーから Windows クライアントを認証することができます。

1. アクセスされるストレージ・システム上で `cifs setup` を実行し、そのストレージ・システム上で CIFS クライアントに使用される認証方式として、NIS/LDAP を指定します。
2. 各 Windows クライアントのローカル・セキュリティ設定を、Kerberos あるいは他の暗号化された認証方式ではなく、平文 (非暗号化) パスワード認証を使用するように構成します。
3. Windows クライアントが、LDAP ユーザー・データベースで構成された `userpassword` 属性を持っていることを確認します。

Windows クライアントからの NFS ファイル・アクセスの LDAP 権限の有効化

LDAP 認証を使用しているストレージ・システム上の UNIX ファイルへの Windows クライアントのアクセス権限を有効にするには、次の 2 つのタスクを実行します。

1. アクセスするストレージ・システム上で、UNIX ファイルへのアクセス権が必要なすべての CIFS ユーザーが、`usermap.cfg` ファイルで関連する UNIX ユーザー名にマッピングされていることを確認します。
2. すべての関連する UNIX ユーザー名が LDAP データベースにエントリーを持っていることを確認します。

UNIX クライアントからの NTFS あるいは混合ファイル・システム・アクセスのための LDAP 権限の有効化

いくつかのタスクを実行することで、LDAP 認証を使用しているストレージ・システム上の NTFS あるいは混合ファイル・システムへの UNIX クライアントのアクセス権限を有効にすることができます。

1. NTFS あるいは混合ファイル・システムへのアクセス権が必要なすべての UNIX ユーザーが、LDAP データベースにエントリーを持っていることを確認します。
2. アクセスするストレージ・システムで、NTFS あるいは混合ファイル・システムへのアクセス権が必要なすべての UNIX ユーザーが、`usermap.cfg` ファイルの関連する CIFS ユーザー名にマッピングされていることを確認します。

LDAP ユーザー・マッピング・サービスの管理

NIS データの使用あるいは `usermap.cfg` ファイルへのエントリーの追加の代わりに LDAP サービスを使用して、UNIX ユーザー・アカウントと Windows ユーザー・アカウントの間のマッピングを行うことができます。デフォルトでは、Data ONTAP は両方向 (UNIX-to-Windows マッピングおよび Windows-to-UNIX マッピング) に同一の (1 対 1) ユーザー・アカウント解決処理を使用します。

このタスクについて

デフォルトでは、LDAP ベースのユーザー・マッピングは無効に設定されています。(Data ONTAP はユーザー・マッピング情報を `/etc/usermap.cfg` ファイルから取得します。)

ファイル・ベースのユーザー・マッピングから LDAP への変換時に、`usermap.cfg` ファイルから (NULL セッション・エントリーを除いて) マッピング・エントリーを削除する必要があります。そのファイルにマッピング・エントリーがあると、LDAP レコードの代わりにユーザー・マッピングに使用されます。

NULL セッションについて Data ONTAP を構成済みの場合、`usermap.cfg` ファイルに NULL セッション・クライアント・エントリーを残すことを確認してください。

UNIX ユーザー・アカウント情報が非 Active Directory LDAP サーバーに保管されている場合に、Data ONTAP が LDAP 検索サービスにアクセスすることを許可するには、LDAP サーバーは単純な認証あるいは匿名ユーザー検索のいずれかを許可するように構成されている必要があります。

1. Data ONTAP コマンド行から、オプション `ldap.usermap.attribute.windowsaccount` の値を指定します。options `ldap.usermap.attribute.windowsaccount account_name` ここで `account_name` は、Data ONTAP が Windows アカウント検索に使用するユーザー・オブジェクト属性です。
2. ステップ 1 で入力したユーザー・オブジェクト属性を組み込むように LDAP スキーマを拡張します。
3. Data ONTAP コマンド行から、`ldap.usermap.attribute.unixaccount` オプションの値を指定します。options `ldap.usermap.attribute.unixaccount account_name` ここで `account_name` は、Data ONTAP が UNIX アカウント検索に使用するユーザー・オブジェクト属性です。
4. ステップ 2 および ステップ 3 で入力した値を組み込むように LDAP スキーマを拡張します。
5. コマンド `options ldap.usermap.enable on` を入力します。LDAP サーバーに重大な負荷がある場合、次のセクションで記載されているように、ユーザー・マッピングのための個別の検索ベースおよび有効範囲を設定することでパフォーマンスを改善することを推奨します。

ユーザー・マッピングのためのベースおよび有効範囲値の指定

LDAP オプションによって、LDAP データベースの適切な領域への属性検索を制限するための、検索ベースおよび有効範囲を設定することができます。これらのオプションの設定は、LDAP 検索の速度を改善します。

検索ベースおよび有効範囲を指定する場合は、次の構文を使用します。ベースおよび有効範囲の値は LDAP データの構造に一致する必要があります。options `ldap.usermap.base "base[:scope][;base2[:scope2]]"`

タスクの結果

例

このコマンドの入力によって、ユーザー・マッピングのための検索ベースを `ou=People,dc=domain0` に設定し、(未指定の) 検索有効範囲をデフォルトの SUBTREE に設定します。options `ldap.usermap.base ou=People,dc=domain0"`

括弧の使用は、指定した検索有効範囲 (BASE) を `ou=People,dc=domain0` に適用します。o ("org") オブジェクトについて未指定の検索有効範囲は、デフォルトの SUBTREE になります。options `ldap.usermap.base "(ou=People,dc=domain0):BASE;o=org"`

次のタスク

検索ベースおよび有効範囲値の設定に関する詳細情報については、LDAP の資料を参照してください。

Active Directory LDAP サーバーの管理

Data ONTAP によって、LDAP 検索サービスのために Active Directory に接続することが可能になります。

Active Directory LDAP サーバーの使用

完全修飾された Active Directory ドメインを Data ONTAP の `ldap.ADdomain` オプションに入力することで、LDAP サービスのために Active Directory を使用することができます。

このタスクについて

Windows から UNIX へのマッピングが Active Directory を使用して実行されるときに、Data ONTAP は以下を行います。

- このアカウントのために指定された Active Directory ドメイン内にそのユーザー・アカウントが存在することを確認する
- `ldap.ADdomain` オプションで指定された Active Directory ドメインへの照会を実行する
- UNIX ユーザー情報を返し、そのユーザー・アカウントが存在することを確認する

Active Directory LDAP サーバーの要件

LDAP サーバーとして Active Directory を使用するには、いくつかの要件が必要です。

LDAP サーバーとして Active Directory を使用するには、以下の要件が必要です。

- 有効な CIFS ライセンス
- Active Directory ドメインに参加しているストレージ・システム
- ストレージ・システムのドメインと LDAP サーバーのドメインが異なる場合、そのドメイン間に両方向の信頼関係が確立されていること

Active Directory LDAP 検索サービスの有効化

いくつかのタスクを実行することで、LDAP 検索サービスのための Active Directory を有効にすることができます。

1. UNIX ユーザー・アカウント情報が Active Directory にない、あるいは匿名ユーザー検索を許可するように構成された LDAP サーバーにない場合、LDAP 検索に使用するユーザー名およびパスワードを、それぞれ `ldap.name` および `ldap.passwd` オプションに入力します。 `options ldap.name user_name options ldap.passwd password`
2. `etc/nsswitch.conf` ファイルで、`passwd` エントリー、`group` エントリー、あるいは両方の `ldap` を指定し、検索サービスとして使用する LDAP を指定します。
3. カスタム・スキーマを所有している場合、`NSSMAP` オプションの値を入力します。
4. Data ONTAP コマンド行から、次のコマンドを入力します。 `options ldap.ADdomain fully_qualified_domain_name`

例 `options ldap.ADdomain group.company.com`

注: 入力したドメインは、ローカル・ドメインまたはローカル・ドメインを信頼関係を共有するドメインである必要があります。

Active Directory LDAP サーバー接続の監視

Active Directory LDAP サーバー接続を監視するために、Active Directory LDAP サーバー情報およびすべての LDAP サーバー・タイプの接続状況を表示することができます。

以下を実施したい場合、	以下を実行してください。
Active Directory LDAP サーバー情報の表示	次のコマンドを入力します。 <code>cifs domaininfo</code> 結果: ドメイン・コントローラー接続およびドメイン・コントローラー選択設定のリストに従って、Active Directory LDAP サーバー接続のリスト、その後に LDAP サーバー選択設定のリストが表示されます。
すべての LDAP サーバー・タイプの接続状況の表示	次のコマンドを入力します。 <code>netstat</code> 結果: Active Directory および非 Active Directory 両方の LDAP サーバー接続状況の情報が、ポート 389 (あるいは <code>ldap.port</code> オプションで割り当てられたデフォルト値ではないポート) に表示されます。

Active Directory LDAP サーバー接続のトラブルシューティング

`cifs.trace_dc_connection` オプションを `on` に設定することで、Data ONTAP にすべてのドメイン・コントローラーのアドレス・ディスカバリーおよび接続アクティビティをログに記録するように指示することができます。

コマンド `options cifs.trace_dc_connection on` を入力します。Data ONTAP は、すべてのドメイン・コントローラーのアドレス・ディスカバリーおよび接続アクティビティをシステム・ログに記録します。

Active Directory LDAP サーバー接続のプールおよび選択について

Data ONTAP は LDAP パフォーマンスを改善するためにいくつかの操作を実行します。

これらの操作には次の操作が含まれます。

- Active Directory LDAP サーバー 接続は、ドメインごとにプールされます。
- 現行の LDAP サーバーからの応答を受信しない場合は、その後の接続は次善の使用可能な LDAP サーバーと行います。
- 1 分おきに、Data ONTAP はより良い LDAP サーバー が使用可能になっているかを確認するためにチェックを実行します。
- 4 時間に 1 回、Data ONTAP は使用可能な Active Directory LDAP サーバーをディスカバリーしてリストを再配列し、以下の順序でサーバーをソートします。
- `prefdc` コマンドで特定され、配列の左方にリストされた、優先サーバー
- 応答時間の速さによってソートされた、候補となるサーバー
- 応答時間の速さによってソートされた、他の Active Directory LDAP サーバー

ldap.servers あるいは ldap.preferred.servers オプションの、Active Directory サーバーへの使用の禁止

Data ONTAP は、ldap.servers および ldap.preferred.servers オプションで指定されたサーバーに接続し、単純なバインドを使用して認証を試みます。単純なバインドは、Active Directory サーバーとの接続を確立するのに十分な認証を提供しないため、これら 2 つのオプション値で Active Directory サーバーを指定しないでください。

LDAP スキーマの管理

デフォルトで、Data ONTAP はネットワーク情報サービス (NIS) スタイルのスキーマを指定する RFC 2307 に適合している LDAP サーバーをサポートします。

LDAP オプションのデフォルト値をカスタム属性名に置き換えて、Data ONTAP が (RFC 2307 適合ではない) そのカスタム・スキーマに照会するように構成することができます。

このタスクについて

RFC 2307 適合スキーマは、LDAP 照会のために使用したい LDAP サーバー上に拡張される必要があります。

詳細情報については、RFC 2307 あるいはサード・パーティーのディレクトリー統合ベンダーによる資料を参照してください。

デフォルト・スキーマについて

デフォルトでは、Data ONTAP のスキーマ変数は適切な RFC 2307 値に設定されています。

オプション	デフォルト値 (RFC 2307 ごと)
ldap.nssmap.objectClass.posixAccount	posixAccount
ldap.nssmap.objectClass.posixGroup	posixGroup
ldap.nssmap.attribute.groupname	cn
ldap.nssmap.attribute.netgroupname	cn
ldap.nssmap.attribute.nisNetGroupTriple	nisNetGroupTriple
ldap.nssmap.attribute.memberUid	memberUid
ldap.nssmap.attribute.uid	uid
ldap.nssmap.attribute.uidNumber	uidNumber
ldap.nssmap.attribute.gidNumber	gidNumber
ldap.nssmap.attribute.userPassword	userPassword
ldap.nssmap.attribute.homeDirectory	homeDirectory
ldap.nssmap.attribute.loginShell	loginShell
ldap.nssmap.attribute.gecos	gecos

LDAP スキーマに一致させるためのカスタム・スキーマ・オプションの変更

適切な ldap.nssmap.* オプションを変更することで、Data ONTAP のスキーマを LDAP スキーマに一致するように変更することができます。

例

オブジェクトがグループ ID (GID) 番号を含むカスタム LDAP スキーマを「groupid」にするには、次のコマンドを入力します。

```
options ldap.nssmap.attribute.gidNumber groupid
```

fsecurity コマンドを使用したストレージ・レベル・アクセス・ガードの有効化

Data ONTAP 7.2.2 から、ストレージ管理者は fsecurity コマンドを使用して、ボリュームおよび qtree にセキュリティ（アクセス権および監査）を設定することができます。この機能は、ストレージ・レベル・アクセス・ガードと呼ばれます。

このタスクについて

適切に配置されたストレージ・レベル・アクセス・ガードによって、いずれのストレージ・オブジェクトも 3 つまでのタイプのセキュリティ・レイヤーを含むことができます。

- NTFS/UNIX/NFSv4 セキュリティ。ストレージ・オブジェクトにあるディレクトリまたはファイル上に存在します。このセキュリティも、クライアントから設定可能な同一のセキュリティです。
- ストレージ・レベル・アクセス・ガード・ファイル・セキュリティ。ストレージ・オブジェクト内のすべてのファイルに適用されます。このセキュリティの適用は、ディレクトリへのアクセスおよびディレクトリの監査には影響しません。
- ストレージ・レベル・アクセス・ガード・ディレクトリ・セキュリティ。ストレージ・オブジェクト内のすべてのディレクトリに適用されます。このセキュリティの適用は、ファイルへのアクセスおよびファイルの監査には影響しません。

注: 現在は、NTFS アクセス許可のみがストレージ・レベル・アクセス・ガードでサポートされます。ストレージ・レベル・アクセス・ガードが適用されている qtree あるいはボリュームでのセキュリティ・チェックを UNIX ユーザーが実施するには、UNIX ユーザーが Windows ユーザーにマッピングされている必要があります。

ストレージ・レベル・アクセス・ガード・セキュリティは、ファイルおよびディレクトリに適用されますが、継承はされません。ファイルあるいはディレクトリのセキュリティ設定を表示する場合、ストレージ・レベル・アクセス・ガードを見ることはできません。

ただし、Data ONTAP でのファイルあるいはディレクトリへのアクセスは、ファイルまたはディレクトリ、あるいはその両方に適用された固有のアクセス権と、qtree またはボリューム、あるいはその両方に設定されたストレージ・レベル・アクセス・ガードの両方の結合効果によって決定されます。両方のセキュリティ・レベルが、ファイルあるいはディレクトリが持つ効果的なアクセス権を判別するために評価されます。

fsecurity コマンドについて

fsecurity コマンドの使用によって、ストレージ管理者は顕著な性能低下を経験することなく大規模なディレクトリー全体にセキュリティを適用することが可能です。なぜなら、セキュリティ設定はリモート・クライアントからではなく、ストレージ・システム上でローカルに管理されるからです。さらに、ストレージ管理者は多くのファイルおよびディレクトリー上のセキュリティを同じコマンドを使用して一度に設定することができます。

注: すべての fsecurity コマンドのリストについては、ストレージ・システム・コマンド行で fsecurity help を入力するか、fsecurity(1) のマニュアル・ページを参照してください。

ジョブ定義ファイルの生成および編集

ストレージ・レベル・アクセス・ガード・セキュリティを qtree あるいはボリュームに適用するために、あるいはファイルおよびディレクトリー上の一括アクセス権を設定するために、ジョブ定義ファイルを生成することができます。

このタスクについて

ジョブ定義ファイルは、例えばセキュリティ記述子や任意アクセス制御リスト (DACL) およびシステム・アクセス制御リスト (SACL) のパスのような情報を含む Unicode テキスト・ファイルです。

この情報は、Security Descriptor Definition Language (SDDL) を使用してエンコードされます。

いったんこのファイルが生成あるいは編集され、ストレージ・システムにコピーされると、fsecurity apply コマンドを使用して、ファイルのセキュリティ定義を検証および適用します。このコマンドをファイルに実行することで、ストレージ・システム上のバックグラウンドで稼働するジョブが作成されます。いったんジョブが完了すると、ストレージ・システム・コンソールから結果を表示することができます。

ジョブ定義ファイルの名前およびストレージ・システムの場所について、要件はありません。これらの例では、以下の名前および場所が使用されています。

```
/vol/vol0/templates/security-base.sec
```

ジョブ定義ファイルのフォーマットは、ASCII あるいは Unicode (UCS-2) でなければなりません。

テキスト・エディターを使用したジョブ定義ファイルの管理

テキスト・エディターを使用して、ジョブ定義ファイルを生成、更新、そして検証することができます。

1. テキスト・ファイル (例えば security-base.sec) を作成、あるいは既存のジョブ定義ファイルを編集します。
2. 新規あるいは更新したファイルをストレージ・システム上のディレクトリー (例えば /vol/vol0/templates/) にコピーします。

3. `fsecurity apply` コマンドを `-c` オプションをつけて実行して定義をジョブに適用する前に、ファイルの妥当性をチェックします。

注: 定義ファイルのいずれかの行が無効であった場合は、`fsecurity apply` コマンドが実行されてもセキュリティ・ジョブは作成されません。

ジョブ定義ファイル要素の指定

ジョブ定義ファイルにセキュリティ設定を定義するときに、伝搬モードを指定することで一括セキュリティ設定 (アクセス権および監査) を適用することができます。

このタスクについて

伝搬モードを指定することで、ネットワーク上での適用によるパフォーマンスの低下を起こすことなく、これらの設定を迅速に、そして効果的に設定することができます。

使用可能な伝搬モードは以下のとおりです。

- 0 = 相続可能なアクセス権をすべてのサブフォルダーおよびファイルに伝搬する (Propagate)
- 1 = このファイルあるいはフォルダーのアクセス権が置き換えられることを許可しない (Ignore) (このモードは現在は使用不可)
- 2 = すべてのサブフォルダーおよびファイルの既存のアクセス権を、相続可能なアクセス権と置き換える (Replace)

以下は、`fsecurity` ジョブ定義ファイルの例です。

```
cb56f6f4
```

```
1,0,"/vol/vol0/qt1",0,"D:(A;CIOI;0x1f01ff;;;DOMAIN\Administrator)"
```

```
1,1,"/vol/vol0/qt2",0,"D:(D;CIOI;0x000002;;;Everyone)"
```

最初の行のストリング `cb56f6f4` は必須で、常に同じです。以下の表は、例の 2 行目の要素がどのようにセキュリティ設定を `/vol/vol0/qt1` と呼ばれる `qtree` に適用するかを示しています。

要素の例	説明
1	NTFS セキュリティ・タイプ
0	標準のセキュリティ (ストレージ・レベル・アクセス・ガードの設定はありません)
<code>/vol/vol0/qt1</code>	ターゲット・ストレージ・オブジェクトのパス (このフィールドには二重引用符が必要です)
0	伝搬モード (この例では 0 は「Propagate」を意味します)

要素の例	説明
D:(A;CIOI;0x1f01ff;;;DOMAIN\Administrator)	ドメイン管理者にフル・コントロールを提供する DACL の SDDL 表記 (このフィールドには二重引用符が必要です)

ジョブ定義ファイルのフォーマットおよび構文に関する詳細情報については、`fsecurity(5)` のマニュアル・ページを参照してください。

セキュリティ・ジョブの作成およびストレージ・オブジェクトへの適用

`fsecurity apply` コマンドは、ジョブ定義ファイルに基づいてセキュリティ・ジョブを作成するために使用されます。このコマンドは、ストレージ・レベル・アクセス・ガードの `qtree` あるいはボリュームへの適用、あるいはファイルおよびディレクトリへのセキュリティの一括設定にも使用されます。また、このコマンドを使用して、`qtree` およびボリューム・レベルでの監査のための `SACL` を設定することもできます。

このタスクについて

セキュリティ・ジョブの作成時に次のオプションを適用することができます。

- `-c` オプションによって、実際にコンテンツを適用せずにジョブの妥当性を確認することができます。
- `-i` オプションによって、エラーを無視してジョブのプロセスを継続することができます。
- `-v` オプションによって、ジョブ内の各タスクを、タスクが生成されたときに表示することができます。

`fsecurity apply` コマンドおよびオプションの完全な説明については、`fsecurity_apply(1)` のマニュアル・ページを参照してください。

セキュリティ・ジョブは、異なる管理者によって同時に実行すること、および他のセキュリティ・ジョブと競合することが可能です。

次のコマンドを入力します。 `fsecurity apply job_definition_file_path`

例

```
fsecurity apply /vol/vol0/templates/security-base.sec
```

```
Added security job 94089
```

ジョブ ID は、ジョブの状況の監視あるいは取り消しに使用されます。

セキュリティ・ジョブの状況の確認および取り消し

`fsecurity status` コマンドを使用して、現在稼働しているジョブの状況および直前の 15 個のジョブの完了状況を表示することができます。

このタスクについて

`fsecurity cancel` コマンドを使用して、現在稼働しているジョブをすべて停止することができます。ジョブ ID が指定された場合は、そのジョブのみが停止します。

注: 完了しているジョブは取り消すことができません。

これらのコマンドの完全な説明については、`fsecurity_status(1)` および `fsecurity_cancel(1)` のマニュアル・ページを参照してください。

以下を実施したい場合、	以下を実行してください。
ジョブ状況の表示	次のコマンドを入力します。 <code>fsecurity status [job_id]</code>
ジョブの取り消し	次のコマンドを入力します。 <code>fsecurity cancel [job_id] all</code> 結果: ジョブ ID は特定のジョブを取り消すために使用し、オプション <code>all</code> はすべてのジョブをキャンセルするために使用します。

ファイルおよびディレクトリーのセキュリティ設定の表示

`fsecurity show` コマンドを使用して、ファイルおよびディレクトリー上のセキュリティ設定を表示することができます。

このタスクについて

このコマンドの出力は、ファイルあるいはディレクトリーがある `qtree` またはボリュームのセキュリティ・スタイルを含みます。現行のセキュリティ・スタイルは、混合 `qtree` 環境でさまざまで、現在どのセキュリティ・スタイルがストレージ・オブジェクト上でアクティブかによって決まります。

ファイルあるいはディレクトリー・パスを指定するときには、ディレクトリーのコンテンツのセキュリティをリストするためにワイルドカードを使用することができます。

このコマンドの完全な説明については、`fsecurity_show(1)` のマニュアル・ページを参照してください。

次のコマンドを入力します。`fsecurity show file_directory_qtree_path [option]`
また、以下の例に示すように、ファイルあるいはディレクトリーの `inode` 番号を (ファイルあるいはディレクトリー・パスの代わりに) 指定することもできます。

`fsecurity show -v volume_name -i inode_number [option]`

このオプションの完全なリスト表示およびコマンド出力の説明については、`fsecurity_show(1)` のマニュアル・ページを参照してください。

ストレージ・レベル・アクセス・ガードの削除

`fsecurity remove-guard` コマンドを使用して、`qtree` あるいはボリュームからストレージ・レベル・アクセス・ガードを削除することができます。 `qtree` は、ストレージ・レベル・アクセス・ガードを削除することができます。

ジ・レベル・アクセス・ガードが適用されていると、削除することができません。詳細情報については、`fsecurity remove-guard(1)` のマニュアル・ページを参照してください。

次のコマンドを入力します。`fsecurity remove-guard volume_qtree_path`

タスクの結果

ストレージ・レベル・アクセス・ガードの削除によって、`qtree` 内あるいはボリューム内のファイルおよびディレクトリーにある標準のファイル・レベル・セキュリティ (例えば NTFS セキュリティー) は削除されません。

システム・アクセス・イベントの監査

Data ONTAP は、Windows へのログオン、ログオフ、およびファイル・アクセス・イベントを同様に監査します。ただし、監査を有効にする方法、および監査イベント情報をログに記録するファイルの管理方法に、いくつかの違いがあります。

監査について

監査のために Data ONTAP を構成すると、イベント・ログ・ファイルおよびすべてのオプションに関する設定は、リブートの後も、あるいは CIFS が終了または再始動する場合は、存続します。

Data ONTAP 監査は、次の 2 つの方法で実行可能です。

- CIFS 監査が、ストレージ・システム上のデータに CIFS プロトコルを使用してアクセスする Windows クライアントからの監査アクセス・イベントを参照する。
- NFS 監査が、ストレージ・システム上のデータに NFS プロトコルを使用してアクセスする UNIX クライアントからの監査アクセス・イベントを参照する。

CIFS および NFS 監査の両方を、ストレージ・システム上で構成することができます。タイプによって、構成要件および監査機能が異なります。

監査は、現在は他のファイル・アクセス・プロトコルではサポートされていません。

Data ONTAP が監査可能なイベント

イベントのいくつかのカテゴリーについて監査を有効にすることができます。

以下のカテゴリーが監査可能です。

- ログオンおよびログオフ・イベント (CIFS 監査が有効に設定されている場合のみ有効)
- ローカルユーザーおよびグループ・アカウントの管理 (CIFS 監査が有効に設定されている場合のみ有効)
- ファイルおよびディレクトリー・レベルでのファイル・アクセス・イベント

注: それぞれのファイルおよびディレクトリーについて、アクセス監査をアクティブにしておく必要があります。

- qtree あるいは ボリューム・レベルでのファイル・アクセス・イベント

注: ストレージ・レベルでのアクセス・ガード・セキュリティが適用されている場合のみ、qtree あるいはボリューム・レベルでのイベントの監査が有効です。

イベント ID	イベント	説明	カテゴリー
516	AdtEvtntDiscard	監査イベントが消失しました	監査ログ
517	AdtLogClear	監査ログが消去されました	監査ログ
528	AdtSuccessfulLogon	ローカル・ログオン	ログオン/ログオフ
529	AdtUnknownUser	不明なユーザー名または不良パスワード	ログオン/ログオフ
530	AdtCantLogonNow	アカウント・ログオン時間の制限	ログオン/ログオフ
531	AdtAccountDisabled	アカウントが無効に設定されています	ログオン/ログオフ
532	AdtUserAccountExpired	ユーザー・アカウントの有効期限が切れています	ログオン/ログオフ
533	AdtCantLogonHere	ユーザーはこのコンピュータにログオンできません	ログオン/ログオフ
534	AdtLogonTypeRestricted	ユーザーは認可されていないログオン・タイプです	ログオン/ログオフ
535	AdtPasswordExpired	ユーザーのパスワードは有効期限が切れています	ログオン/ログオフ
536	AdtNetLogonInactive	NetLogon コンポーネントはアクティブではありません	ログオン/ログオフ
537	AdtUnsuccessfulLogon	上記以外の理由でログオンに失敗しました	ログオン/ログオフ
538	AdtUserLogoff	ローカルあるいはネットワーク・ユーザーがログオフしました	ログオン/ログオフ
539	AdtLockedOut	アカウントはロックアウトされました	ログオン/ログオフ
540	AdtSuccessfulNetLogon	ネットワーク (CIFS) ログオンしました	ログオン/ログオフ
560	AdtObjOpen	オブジェクト (ファイルまたはディレクトリ) が開きました	ファイル・アクセス

562	AdtHandleClosed	AdtObjOpen という結果になったハンドルが閉じました	ファイル・アクセス
563	AdtObjOpenForDelete	オブジェクト (ファイルまたはディレクトリー) が削除のために開きました	ログオン/ログオフ
567	AdtObjAccessAttempt	オブジェクトにアクセスしました (読み取り、書き込み、他)	ファイル・アクセス
612	AdtPolicyChange	監査ポリシーが変更されました	ポリシー変更
624	AdtUserCreated	ユーザーが作成されました	アカウント管理
630	AdtUserDeleted	ユーザーが削除されました	アカウント管理
635	AdtGroupCreated	グループが作成されました	アカウント管理
636	AdtLclGrpMemberAdded	セキュリティが、追加されたローカル・グループのメンバーを有効にしました	アカウント管理
637	AdtLclGrpMemberRemoved	セキュリティが、削除されたローカル・グループのメンバーを有効にしました	アカウント管理
638	AdtGroupDeleted	グループが削除されました	アカウント管理

システム・イベント監査の構成

システム・イベント監査を構成するために、いくつかのタスクを実行する必要があります。

1. どのイベントを監査するかを決定します。例えば、ボリュームあるいは `qtree` 上のすべてのイベントを監査する場合、`fsecurity` コマンドを使用してストレージ・レベル・アクセス・ガード・セキュリティを適用します。
2. ファイルおよびディレクトリー・アクセスのイベントを監査する場合は、システム・アクセス制御リスト (SACL) を設定します。
3. CIFS 監査または NFS 監査、あるいはその両方を有効にします。
4. 監査を管理するために Live View を使用したい場合は、Live View を使用可能に設定します。そうでない場合は、監査ログ管理を頻繁に行います。
5. イベント・ビューアーを使用して監査イベントを表示します。

SACL の設定

システム・アクセス制御リスト (SACL) は、ファイルおよびディレクトリー上のアクセスの監査を有効にするために使用できます。

このタスクについて

アクセスを監査するために SACL を設定するには、次の 3 つの方法があります。

- ボリュームあるいは qtree 内のすべてのファイルおよびディレクトリー上でアクセス・イベントを監査したい場合は、ストレージ・レベル・アクセス・ガード・セキュリティを適用することで SACL を設定することを推奨します。
- 個々のファイルおよびディレクトリー上でアクセス・イベントを監査したい場合は、SACL を次の 2 つの方法で設定することができます。
- Windows エクスプローラ GUI を使用する。
- fsecurity コマンドを使用する。

注: 監査オプションを多く選択しすぎるとシステム・パフォーマンスに影響する可能性があるため、監査する必要があるイベントのみを選択することを確認してください。

個々のファイルおよびディレクトリー上のアクセスの監査を有効にするには、以下の手順を Windows 管理ホスト上で完了します。

1. アクセスの監査を有効にしたいファイルあるいはディレクトリーを選択します。
2. ファイルあるいはディレクトリーで右クリックし、「プロパティ」を選択します。
3. 「セキュリティ」タブを選択します。
4. 「詳細」をクリックします。
5. 「監査」タブを選択します。
6. 必要に応じて、監査オプションを追加、編集、あるいは削除します。これらのオプションの設定方法に関する詳細情報に付いては、Windows の資料を参照してください。

CIFS 監査のための Data ONTAP の構成

CIFS 監査を有効あるいは無効に設定する場合、ポリシー変更イベントの監査を有効にします。このとき、ポリシー変更イベントを有効にする個別の CIFS オプションはありません。

始める前に

以下は、CIFS 監査の前提条件です。

- 監査を有効に設定する前に、ストレージ・システム上で CIFS がライセンス交付を受けて有効に設定されている必要があります。
- 監査されるファイルあるいはディレクトリーは、混合あるいは NTFS ボリュームまたは qtree にある必要があります。ストレージ・レベル・アクセス・ガードが有効になっていなければ、UNIX のボリュームまたは qtree のファイルおよびディレクトリーの CIFS イベントを監査することはできません。
- 記録するアクセス・イベントを指定する必要があります。

- デフォルトでは、イベント監査はオフにされています。監査するイベントを特定するために、個々のオプションを有効にし、監査を有効にする必要があります。

以下の監査をオンまたはオフにしたい場合、	以下を実行してください。
ファイル・アクセス・イベント	次のコマンドを入力します。options cifs.audit.file_access_events.enable on off
ログオンおよびログオフ・イベント	次のコマンドを入力します。options cifs.audit.logon_events.enable on off
ローカル・アカウント管理イベント	次のコマンドを入力します。options cifs.audit.account_mgmt_events.enable on off 注: アカウント管理イベントに対する変更を表示するには、MMC イベント・ビューアーを使用します。
すべてのイベント	次のコマンドを入力します。cifs audit start stop あるいは、cifs.audit.enable オプションを使用して、CIFS 監査を開始および停止することができます。例えば、次のコマンドを入力することは、cifs audit start コマンドを使用するのと同様です。 options cifs.audit.enable on off CIFS 監査を開始するには on を、停止するには off を使用します。 注: デフォルトでは、CIFS 監査は無効に設定されています。

NFS 監査のための Data ONTAP の構成

NFS 監査はファイルおよびディレクトリーのアクセス・イベントを記録することはできますが、ログオン、ログオフ、およびその他の CIFS 監査でサポートされるイベントは記録できません。監査されるファイルあるいはディレクトリーは、いずれのセキュリティー・スタイル (NTFS、UNIX、あるいは混合) のボリュームまたは qtree にも存在することが可能です。

始める前に

以下は、NFS 監査の前提条件です。

- NFS 監査を有効に設定する前に、ストレージ・システム上で CIFS がライセンス交付を受けて有効に設定されている必要があります。
- NFS 監査が有効に設定される前に、CIFS 監査がストレージ・システム上で有効に設定されている必要があります。監査はデフォルトでは無効に設定されています。
- 記録するイベントを特定する必要があります。

NFS 監査イベントの指定:

NTFS あるいは混合のセキュリティー・スタイルの `qtree` あるいはボリュームでの NFS 監査に関するイベントを指定するには、ファイルおよびディレクトリーにシステム・アクセス制御リスト (SACL) を設定する必要があります。

1. ログ・フィルター・ファイル (通常は `/etc/log/nfs-audit` と呼ばれます) を、ストレージ・システム上に作成します。このファイルは、デフォルトでどのファイル・イベントが監査ログに含まれるかを識別するために使用します。フィルター・ファイルはコンテンツを含みません。

注: NTFS あるいは混合スタイルのボリュームまたは `qtree` に、NFS ログ・フィルター・ファイルを作成する必要があります。そうしない場合は、監査に必要なフィルター・ファイル上の SACL を設定することができません。

2. `cifs.audit.nfs.filter.filename` オプションを設定し、ファイル・フィルターを識別します。 `cifs.audit.nfs.filter.filename` オプションに関する詳細情報については、`options(1)` のマニュアル・ページを参照してください。
3. フィルター・ファイルのシステム・アクセス制御リスト (SACL) を設定します。

次のタスク

NTFS あるいは混合のセキュリティー・スタイルの `qtree` に監査イベントのための NFS フィルター・ファイルを作成することができますが、個々のファイルおよびディレクトリーに設定された SACL が、フィルター・ファイルに設定された SACL より優先になります。

フィルター・ファイルによる NFS 監査イベントのコントロール方法:

ログ・フィルター・ファイルは、設定した SACL を用いてファイル監査イベントをコントロールします。フィルター・ファイル上の SACL の設定は、ストレージ・システム上のすべてのファイルおよびディレクトリーで同一の SACL を設定するのと同じ効果があります。

注: ログ・フィルター・ファイル SACL はストレージ・システム上のすべてのファイルおよびディレクトリーからの監査イベントを潜在的に生成することが可能なため、ログ・フィルター・ファイルを使用して NFS 監査を有効にすることは、システム・パフォーマンスに影響する可能性があります。

フィルター・ファイルの効果は、ファイルがある `qtree` のセキュリティー設定によります。

UNIX セキュリティー・スタイルのファイルで操作が実行された場合、イベントはフィルター・ファイル上の SACL に応じてログに記録されます。

SACL が設定されていない NTFS または混合のセキュリティー・スタイルの `qtree` にあるファイルで操作が実行された場合、イベントはフィルター・ファイル上の SACL によってログに記録されます。

ただし、SACL が個々のファイルまたはディレクトリー上で設定されている場合は、これらの SACL がフィルター・ファイル上の SACL 設定より優先されます。

NFS 監査の有効化:

いくつかのタスクを実行することで、NFS 監査を有効にすることができます。

1. ストレージ・システムの /etc/log ディレクトリーで、nfs-audit と呼ばれるファイルを作成します。

注: ステップ 1 および 2 は、UNIX セキュリティー・スタイルの qtree での監査には必須ですが、NTFS あるいは混合スタイルの qtree での監査にはオプションです。

2. NFS ログ・フィルター・ファイルを識別するには、次のコマンドを入力します。`options cifs.audit.nfs.filter.filename /etc/log/nfs-audit`
3. ファイル・アクセス・イベントの監査を有効にするには、次のコマンドを入力します。`options cifs.audit.file_access_events.enable on`

注: ファイル・アクセスおよびログオン・イベントの監査は、デフォルトではオフにされています。

4. NFS 監査を有効にするには、次のコマンドを入力します。`options cifs.audit.nfs.enable on`
5. 監査ログ管理を構成します。
6. Windows 管理ホストで、フィルター・ファイルのシステム・アクセス制御リスト (SACL) を設定します。

タスクの結果

これらのステップで記載されているオプションに関する詳細情報については、options(1) のマニュアル・ページを参照してください。

Live View の構成

Live View が有効になっている場合、アクセス・ロギング機能 (ALF) デーモンが 1 分に 1 回実行され、監査イベントをメモリーからディスク上の内部ログ・ファイル /etc/log/cifsaudit.alf にフラッシュします。

このタスクについて

また、ALF デーモンは、ALF レコードをイベント・ビューアーで表示することができる EVT レコードへの保存および変換も試みます。これは、毎分 1 回、または .alf ファイルが 75 パーセント満たされたときに実行されます。

EVT レコードは、/etc/log ディレクトリーの 3 つのファイルに保管されます。

- fixedsection
- varsectiona
- varsectionb

ALF デーモンは、イベント・ビューアーが稼働している Windows クライアントからのイベント・ログ RPC 要求に情報を提供するために、これら 3 つのファイルを使用します。Live View が有効にされている場合、イベント・ビューアーは最新の監査イベントを最大で 5,000 レコードまで表示します。

内部ログ・ファイルから新規のレコードが保存されるたびに、それらのレコードは Live View ファイルに書き込まれ、EVT ファイルにもバックアップされます。バックアップ・ファイルは、/etc/log ディレクトリーにファイル名の一部としてのタイム・スタンプと一緒に保存されます。

監査イベントはリアルタイムに表示することができ、バックアップ・ファイルはイベント・ビューアーを使用して静的ファイルとして表示することができます。

注: Data ONTAP 7.2.2 から、Live View は内部の監査ファイルのサイズおよび保存方法をコントロールする `cifs.audit.autosave` オプションと一緒に有効になりました。

以下を実施したい場合、	以下を実行してください。
Live View を有効あるいは無効にする	次のコマンドを入力します。options <code>cifs.audit.liveview.enable on off</code> Live View を有効にする場合は <code>on</code> を使用し、無効にする場合は <code>off</code> を使用します。 注: Live View を有効にする前に、ストレージ・システムの監査を有効にする必要があります。Live View はデフォルトで無効にされています。
現在の ALF および EVT ファイルを消去する	次のコマンドを入力します。cifs audit clear 結果: /etc/log ディレクトリー内の <code>cifsaudit.alf</code> 内部ログ・ファイルおよび現在の EVT ログ・ファイルが消去されます。ただし、タイム・スタンプ付きのすべての EVT バックアップ・ファイルには、このコマンドによる影響はありません。

監査イベントの保存および消去

自動保存が発生したときの、自動的に保存されるファイルの最大数、および `cifsaudit.alf` ファイルの最大サイズを指定することができます。 `cifsaudit.alf` ファイルを消去することも可能です。

Data ONTAP による監査イベント情報の記録場所:

監査イベント情報は内部ログ・ファイルの `/etc/log/cifsaudit.alf` に保管されます。Live View を使用しない場合、手動あるいは自動保存を設定することで、このファイルの内容を定期的に外部の EVT イベント・ログ・ファイルに保存する必要があります。

デフォルトでは、外部のイベント・ログは `/etc/log/adtlog.evt` ファイルです。他のファイルをイベント・ログとして指定することが可能です。指定したファイルが存在しない場合、Data ONTAP は情報をファイルに保存するときにファイルを作成します。ただし、ファイルを置くディレクトリーは存在していなければなりません。さもないければ、ファイルを指定したときにエラー・メッセージが表示されます。

内部および外部ログ・ファイルのサイズおよびフォーマット:

内部の `cifsaudit.alf` ログ・ファイルの最大サイズを、524,288 バイト (521K) から 68,719,476,736 バイト (64GB) の間で指定することができます。デフォルト・サイズは 524,288 バイトです。

`cifsaudit.alf` ファイルから生成される外部イベント・ログ (.evt ファイル) は、`cifsaudit.alf` ファイルの圧縮コンテンツが外部イベント・ログ・ファイルで展開およ

び再フォーマットされるため、内部ログより大きくなります。外部イベント・ログは Windows フォーマットです。外部イベント・ログはイベント・ビューアーで表示することができます。cifsaudit.alf ログ・ファイルは内部フォーマットのため、イベント・ビューアーで表示することはできません。

Data ONTAP によるイベント・ログ更新方法:

Data ONTAP は、次に cifs audit save コマンドを発行するか、自動保存が起こったときにイベント・ログを更新します。

監査イベント情報を外部のイベント・ログに保存するには、cifs audit save コマンドを発行するか、イベント情報の自動保存を有効にします。Data ONTAP は、クライアントによってログが表示される際にはイベント・ログを更新しません。ただし、イベント・ログが開かれるときに収集されるファイル・アクセス情報は失われません。

イベント情報の消失を避けるために、cifs audit save コマンドを頻繁に発行するか、常習的な自動保存を有効にしておくことが重要です。イベント生成頻度が高すぎると、cifsaudit.alf ファイルがすぐにいっぱいになり、イベント・ログに保存される前に古いイベントを上書きする可能性があります。

イベント・ログへの監査イベントの手動保存:

cifs audit save コマンドを使用して、イベント・ログを手動で更新することができます。

始める前に

Data ONTAP が監査イベント情報をログに記録する場所を指定するには、コマンド options cifs.audit.saveas *filename* を入力します。*filename* は、Data ONTAP が監査イベント情報をログに記録するファイルの完全なパス名です。ファイル拡張子として、**.evt** を使用します。スペースを含むパス名は、引用符で囲みます。例:

```
options cifs.audit.saveas /etc/log/mylog.evt
```

```
options cifs.audit.saveas "/home/my event log/audit.evt"
```

このタスクについて

次のコマンドを入力して、イベント・ログを更新します。cifs audit save [-f] イベント・ログが存在しない場合は、-f オプションを省略します。既存のイベント・ログを上書きするには、-f オプションを使用します。

タスクの結果

Data ONTAP は最後のイベント・ログ更新以降に収集されたイベント情報をイベント・ログに書き込みます。

自動保存がいつ起こるかの指定:

時間間隔あるいは内部ログ・ファイルのサイズ (cifsaudit.alf ファイルがどの程度いっぱいになっているか) に基づいて、イベント・ログに監査イベントが自動的に保存されることを指定することができます。

このタスクについて

サイズのしきい値と時間間隔の両方を指定した場合、サイズのしきい値あるいは時間間隔が到達すると必ず監査イベントはイベント・ログに保存されます。

内部ログ・ファイルが外部イベント・ファイルに自動的に保存されるときは毎回、イベント・ファイルのベース名に拡張子が追加されます。追加される拡張子のタイプを以下から 1 つ選択します。

- カウンター
- タイム・スタンプ

これらの拡張子が指定されない場合は、タイム・スタンプがファイル拡張子として使用されます。ただし、「タイム・スタンプ」という値は表示されません。

ストレージ・システムは、最大で 6 週間分のイベント・ファイルを保存します。保存可能なイベント・ファイルの数の制限を指定することができます。

内部ログ・ファイル・サイズに基づく自動保存の有効化:

内部ログ・ファイルのサイズに基づく自動保存を有効にしている場合、サイズのしきい値を指定することができます。

このタスクについて

内部ログ・ファイルに関するデフォルトのサイズのしきい値は、75 パーセントで、内部ログ・ファイルが 75 パーセントまで満たされている場合は、内容が常に外部イベント・ファイルに自動的に保存されます。しきい値は、内部ログ・ファイルのサイズのパーセンテージあるいは絶対サイズで指定することができます。

以下の表は、自動保存のための内部ログ・ファイルのサイズのしきい値を指定するのに使用できる計測単位および値を示しています。

計測単位	値
% (cifsaudit.alf ファイルのパーセンテージ)	1 から 100
k (キロバイト)	1 から 67108864
m (メガバイト)	1 から 65526
g (ギガバイト)	1 から 64

以下を実施したい場合、	以下を実行してください。
内部ログ・ファイルが自動的に保存されるサイズのしきい値を指定する	次のコマンドを入力します。options cifs.audit.autosave.onsize.threshold <i>Nsuffix</i> ここで <i>N</i> は、サイズのしきい値の値で、 <i>suffix</i> は計測単位です。 例: options cifs.audit.autosave.onsize.threshold 90% 注: 有効な値およびサイズのしきい値の単位については、前出の表を参照してください。

以下を実施したい場合、	以下を実行してください。
内部ログ・ファイルのサイズに基づく自動保存の有効化あるいは無効化	次のコマンドを入力します。options cifs.audit.autosave.onsize.enable on off

時間間隔に基づく自動保存の有効化:

時間間隔に基づく自動保存を有効にしている場合、時間間隔を指定することができます。

このタスクについて

以下の表は、自動保存のための時間間隔を指定するのに使用できる計測単位および値を示しています。

計測単位	値
s (秒)	1 から 60
m (分)	1 から 60
h (時間)	1 から 24
d (日)	1 から 7

以下を実施したい場合、	以下を実行してください。
内部ログ・ファイルから外部イベント・ファイルへの自動保存について異なる時間間隔を指定する	次のコマンドを入力します。options cifs.audit.autosave.ontime.interval <i>Nsuffix</i> ここで <i>N</i> は時間間隔の値で、 <i>suffix</i> は計測単位です。 例: options cifs.audit.autosave.ontime.interval 60s
時間間隔に基づく自動保存の有効化	次のコマンドを入力します。options cifs.audit.autosave.ontime.enable on off

カウンター拡張子の指定:

自動ファイル命名に「カウンター (counter)」を選択すると、拡張子は数値になります。

このタスクについて

自動保存が起きると、古いイベント・ファイルは連番の拡張子を使用して名前変更されます。最新のイベント・ファイルは、ファイル名に追加された数値はありません。

例えば、基本のファイル名が eventlog で自動保存が起きると、最新のイベント・ファイルは eventlog.evt という名前になり、以前の eventlog.evt ファイルは eventlog1.evt にコピーされ、eventlog1.evt ファイルは eventlog2.evt にコピーされます。

次のコマンドを入力します。options cifs.audit.autosave.file.extension
counter

タイム・スタンプ拡張子の指定:

自動ファイル命名のために timestamp を選択した場合、ファイル名はタイム・スタ
ンプ・フォーマットになります。

このタスクについて

フォーマットは、*base name of event file.YYYYMMDDHHMMSS.evt* です。

パラメーター	説明
YYYY	年 (4 桁)
MM	月 (2 桁)
DD	日 (2 桁)
HH	時 (2 桁)
MM	分 (2 桁)
SS	秒 (2 桁)

次のコマンドを入力します。options cifs.audit.autosave.file.extension
timestamp

自動的に保存されるファイルの最大数の指定:

cifs.audit.autosave.file.limit オプションを使用して、自動的に保存可能なイベント・フ
ァイルの最大数を指定することができます。

次のコマンドを入力します。options cifs.audit.autosave.file.limit *value value*
は、0 から 99 の数値です。

注: このオプションの数値が 1 から 999 の間で設定された場合、いったんストレ
ージ・システム上に存在するファイルが制限に達すると、最も古いファイルが常に
上書きされます。ただし、このオプションの値が 0 に設定された場合は、システム
に自動的に保存される EVT ファイルの数に制限はありません。

cifsaudit.alf ファイルの最大サイズの指定:

cifs.audit.logsize オプションを使用して、cifsaudit.alf ファイルの最大サイズを指定す
ることができます。

コマンド options cifs.audit.logsize *size* を入力します。*size* は、バイト数で
す。無効な数を入力すると、許容値の範囲を示すメッセージが表示されます。

注: Data ONTAP は、cifsaudit.alf ファイルが最大サイズに到達した後は最も古いデ
ータを上書きします。イベント・データの損失を防ぐには、cifsaudit.alf ファイルが
いっぱいになる前に保存する必要があります。デフォルトでは、ファイルが 75 パ
ーセントまでいっぱいになると、警告メッセージが発行されます。ファイルがいっ
ぱいに近づきデータがまもなく上書きされるとき、およびデータが上書きされたと
きに、追加の警告メッセージが送信されます。

監査イベントの SNMP トラップ:

Data ONTAP は、特定の監査イベントに基づく特定の処置 (通知など) のトリガーを提供する SNMP トラップを組み込んでいます。

CIFS クライアントで監査イベントの SNMP トラップを受信したい場合、Data ONTAP の SNMP 機能を使用するクライアントを登録する必要があります。登録されたクライアントは、SNMP トラップを listen する SNMP ソフトウェアを持つ必要があります。

以下のいずれかが発生すると、SNMP トラップが発行されます。

- 指定された時間間隔に到達し、cifsaudit.alf ファイルが保存された場合。
- 指定されたサイズのしきい値に到達し、cifsaudit.alf ファイルが保存された場合。
- デフォルトのサイズのしきい値 75 パーセントが満たされた状態に到達し、cifsaudit.alf ファイルでラッピングおよびイベント・データの上書きの危険性があるが、cifs.audit.autosave.onsize.enable および cifs.audit.autosave.ontime.enable オプションがオフになっているためにファイルが保存されない場合。
- オンになっている自動保存オプションがないために、cifsaudit.alf ファイルがラップされ、イベント・データが上書きされた場合。

cifsaudit.alf ファイルの消去:

cifs audit clear コマンドを使用して、内部 cifsaudit.alf ファイルを消去することができます。

次のコマンドを入力します。cifs audit clear

タスクの結果

監査が既に開始している場合は、内部 cifsaudit.alf ログ・ファイルは消去されます。監査が停止している場合は、cifsaudit.alf ファイルは削除されます。外部イベント・ログは、このコマンドによって影響を受けません。

イベント詳細表示の表示および理解

Live View を使用して収集されたリアルタイム監査イベント、保存した外部のイベント・ログ (.evt ファイル)、あるいは Live View によって作成されたバックアップ・ログ・ファイルを表示することができます。

このタスクについて

以下のイベント詳細表示が使用可能です。

- ネットワーク・ログオン
- 失敗したネットワーク・ログオン
- ネットワーク・ログオフ
- Windows ファイル・アクセス
- UNIX ファイル・アクセス
- 失敗したファイル・アクセス
- 失われたレコード・イベント

- 監査ログ消去イベント

監査イベントを表示する方法

監査イベントは、Windows クライアントから Microsoft イベント・ビューアーで、コントロール・パネルの中の管理ツールあるいは Microsoft 管理コンソール (MMC) のいずれかから表示することができます。

監査イベントを表示するには、2 つの方法があります。

- リアルタイムで表示。Live View 機能が有効になっている場合、EVT イベント・ログ・ファイルは 1 分ごとに自動的にリフレッシュされます。これによって、5,000 個の最新の監査イベントを、イベント・ビューアーで継続的に表示します。

注: Live View 機能を使用するには、Windows クライアントに Windows 2000 以降を使用する必要があります。

- 静的な表示。EVT イベント・ログを、手動あるいは自動保存の設定のいずれかによって管理することができます。この場合、イベント・ビューアーはファイルの管理方法に応じて、ログ・ファイルを最後に保存した内容で表示します。

Live View を使用したリアルタイム監査イベントの表示

Windows イベント・ビューアーを使用して、Live View で収集されたリアルタイム監査イベントを表示することができます。

始める前に

リアルタイム監査イベントを表示する前に、Live View を構成する必要があります。

1. Windows クライアントから、コントロール・パネルの管理ツールあるいは Microsoft 管理コンソールからイベント・ビューアーを開始します。
2. 「操作」メニューから、「別のコンピュータへ接続」を選択します。
3. ダイアログ・ボックスで、監査したいストレージ・システムの名前を入力し、「OK」をクリックします。
4. アプリケーションの左側で「セキュリティ」エントリーを選択します。アプリケーションの右側には、ストレージ・システム上で収集された最新の監査イベント (最大 5,000 イベント) が表示されます。

静的イベント・ログ・ファイルの表示

Windows クライアントを使用して、保存した外部のイベント・ログ (.evt ファイル) あるいは Live View によって作成されたバックアップ・ログ・ファイルを表示することができます。

1. Windows クライアントから、コントロール・パネルの管理ツールあるいは Microsoft 管理コンソールからイベント・ビューアーを開始します。
2. 「ログ」メニューで、「ログ ファイルを開く (Open)」を選択します。

注: 「ログ」メニューから「コンピュータを選択する」を選択してストレージ・システムをダブルクリックすることでイベント・ログを開こうとしないでください。そうした場合、Live View が有効にされていないと Data ONTAP が RPC

呼び出しを使用してイベント・ビューアーと通信を行わないため、イベント・ビューアーはエラー・メッセージ「RPC サーバーは使用できません (The RPC server is unavailable)」を表示します。

3. ストレージ・システム上のイベント・ログを選択します。

Windows ファイル・アクセスの詳細表示

Windows ファイル・アクセスの詳細表示は、多くのタイプの情報を表示します。

以下の表は、Windows ファイル・アクセスの詳細表示のフィールドを記載しています。

フィールド	説明
Object Server	監査チェック機能呼び出すサブシステム・サーバーのプロセス名。これはセキュリティ・ログのため、常に SECURITY です。
Object Type	アクセスされているオブジェクトのタイプ。
Object Name	アクセスされているオブジェクトの名前 (ファイル名など)。
New Handle ID	オープン・オブジェクトの新規のハンドル ID。
Operation ID	単一の操作から生じた、複数のイベントを関連付ける固有 ID。
Process ID	オブジェクトにアクセスしているクライアント・プロセスの ID。
Primary User Name	オブジェクトへのアクセスを要求しているユーザーのユーザー名。偽名が使用された場合は、サーバー・プロセスがログオンされる際に使用されるユーザー名です。
Primary Domain	コンピューター名。あるいはプライマリー・ユーザー名によって識別されたユーザーが SYSTEM の場合は SYSTEM。コンピューターが Windows NT サーバー・ドメインのメンバーの場合、これはプライマリー・ユーザーのアカウントを含むドメインの名前になる可能性があります。
Primary Logon ID	プライマリー・ユーザーがログオンしたときに割り当てられた固有 ID。
Client User Name	ご使用のログイン名。
Client Domain	ご使用のコンピューター名、あるいはクライアント・ユーザー・アカウントを含むドメインの名前。
Client Logon ID	クライアント・ユーザーがログインしたときに割り当てられた固有 ID。
Accesses	オブジェクトに対して試行されたアクセスのタイプ。
Privileges	特権。

UNIX ファイル・アクセスの詳細表示

UNIX ファイル・アクセスの詳細表示は、Windows ファイル・アクセスの詳細表示と同じ種類の情報を表示しますが、ファイルが NFS を通してアクセスされるため、オブジェクト名の代わりに NFS アクセスが表示されます。

さらに、UNIX ファイル・アクセスの詳細表示は、監査しているファイルに関する以下の情報を表示します。

- ファイルが置かれているボリュームの ID
- ファイルが置かれている最新のスナップショット・コピーの ID
- ファイルの inode

この情報により、NFS クライアントから `find -inum` コマンドを使用してファイルを検出することが可能になります。

不成功のファイル・アクセスおよび損失レコード・イベントの詳細表示

不成功のファイル・アクセスの詳細表示は、失敗したファイル・アクセスを表示します。さらに、Data ONTAP が監査レコードを作成できない場合、損失レコード・イベントの詳細表示は、その理由を提供します。

例えば、不成功のファイル・アクセスは、ユーザーがアクセス権を持たずにファイルへのアクセスを試行した場合に発生します。この詳細表示は、ファイル・アクセスを試みたユーザーの ID およびアクセス試行が不成功であったことを表示します。

Data ONTAP が監査レコードを作成できない場合、損失レコード・イベントの詳細表示は、以下のような理由を提供します。

Internal resources allocated for the queueing of audit messages have been exhausted,

Number of audit records discarded: 1

シンボリック・リンクへの CIFS アクセスのコントロール

シンボリック・リンクは、NFS クライアントが作成した特別なファイルで、他のファイルあるいはディレクトリを指し示します。シンボリック・リンクは、いくつかの点で、Windows 環境の「ショートカット」と似ています。

このタスクについて

2 種類のシンボリック・リンクがあります。

- 絶対シンボリック・リンクは、スラッシュ (/) から始まり、ファイル・システムのルートから派生したパスとして処理されます。
- 相対シンボリック・リンクは、スラッシュ (/) 以外の文字から始まり、シンボリック・リンクの親ディレクトリと関連するパスとして処理されます。

CIFS クライアントは、シンボリック・リンクを作成できませんが、NFS クライアントが作成したシンボリック・リンクをたどることはできます。

以下のタイプのシンボリック・リンクに CIFS がアクセスすることを可能にするには、特別な要件があります。

- 絶対シンボリック・リンク。絶対シンボリック・リンクの宛先は、UNIX マウントのタイプによって決まるため、CIFS クライアントは絶対シンボリック・リンクを解釈するための追加情報が必要です。
- 相対シンボリック・リンクがある共有の外部にある、同じストレージ・システム上の宛先への相対シンボリック・リンク。デフォルトでは、Data ONTAP は、CIFS クライアントが認証されている共有の外部へのシンボリック・リンクをたどることを許可しません。

CIFS クライアントによるシンボリック・リンクの追跡の有効化

`cifs.symlinks.enable` オプションを使用して、シンボリック・リンクが無効にされた後の、CIFS のシンボリック・リンクへのアクセスを可能にします。

このタスクについて

`cifs.symlinks.enable` オプションは、デフォルトで有効になっています。

シンボリック・リンクへの CIFS アクセスを有効にするには、次のコマンドを入力します。`options cifs.symlinks.enable on`

タスクの結果

CIFS クライアントは、同じ共有内の宛先への相対シンボリック・リンクに直接従います。

CIFS クライアントのシンボリック・リンクとの対話方法の指定

`/etc/symlink.translations` ファイルに Map エントリーを作成すること (絶対シンボリック・リンクのみ)、`/etc/symlink.translations` ファイルに Widelink エントリーを作成すること (絶対シンボリック・リンクのみ)、あるいはシンボリック・リンクに関する NT 共有境界を無効にすること (相対および絶対シンボリック・リンク) で、CIFS クライアントがどのようにシンボリック・リンクを対話するかを指定することができます。

このタスクについて

以下の表を使用すると、どのオプションを実装したいかを判別するのに役立ちます。表は各オプションに関して、シンボリック・リンクがポイント可能な宛先のタイプを示しています。

可能なシンボリック・リンクの宛先	Map エントリー	Widelink エントリー	共有境界 チェックなし
同じストレージ・システム上の同じ共有	X	X	X
同じストレージ・システム上の別の共有		X	X
同じストレージ・システム上の非共有領域			X

可能なシンボリック・リンクの宛先	Map エントリー	Widelink エントリー	共有境界 チェックなし
別のストレージ・システム上の共有		X	
別の CIFS サーバー あるいはデスクトップ PC 上の共有		X	

ファイルへのシンボリック・リンクを回避する必要がある理由

Data ONTAP が間違えたファイルを更新する可能性があるため、ファイルをポイントするシンボリック・リンクに CIFS クライアントが従うことを防止する必要があります。

多くの CIFS クライアント・アプリケーションが、一時ファイルへの書き込み、オリジナルのファイルのバックアップ名への名前変更、そして一時ファイルのオリジナル名への名前変更、といった操作を実行するため、間違えたファイルが更新される可能性があります。

クライアント・アプリケーションがこれらの操作を実行するときに、オリジナルのファイルが直接シンボリック・リンクのターゲットになっていると、ファイルはシンボリック・リンクがあったディレクトリーに保管され、名前変更されたシンボリック・リンクは更新されたファイルではなくオリジナルのファイルをポイントします。

注: 個々のファイルではなくディレクトリーへのシンボリック・リンクに従う CIFS クライアントは、この問題を経験することはありません。

Map エントリーについて

Map エントリーはストレージ・システム上で絶対シンボリック・リンクをリダイレクトするために使用されます。Map エントリーは `/etc/symlink.translations` ファイル内で作成することができます。Map エントリーは CIFS クライアントが、同一の共有にあるターゲットの宛先への絶対シンボリック・リンクに従うことを許可します。

注: リンクの共有の外部にあるリソースへのシンボリック・リンクに従う CIFS クライアントのユーザーは、`cifs share -nosymlink_strict_security` オプションがソース共有のために指定されていない場合は、動作しません。

Map エントリーには以下の要件があります。

- 絶対シンボリック・リンクを解決するために、リンクの宛先を決定する `/etc/symlink.translations` ファイルに Map エントリーが登録されている必要があります。
- シンボリック・リンクの宛先は、リンク自体と同一の共有内にある必要があります。あるいは、リンクは `-nosymlink_strict_security` オプションが指定されている共有内にある必要があります。

Map エントリーを使用して絶対シンボリック・リンクをリダイレクトする場合は、Windows 共有セキュリティはシンボリック・リンクと宛先が同一の共有にあるた

め、その両方が保持されます。 Map エントリーと Widelink エントリーの両方を `symlink.translations` ファイルに持つ場合は、ストレージ・システムは最初に発見した適合エントリーを使用します。

Widelink エントリーについて

Widelink エントリーはご使用のストレージ・システム上で絶対シンボリック・リンクをリダイレクトするためのもう 1 つの方法です。 Widelink エントリーは `/etc/symlink.translations` ファイル内で作成することができます。

Widelink エントリーは、宛先 (同一のストレージ・システムにある場合も、ストレージ・システムの外部にある場合も) をターゲットとする絶対シンボリック・リンクに CIFS クライアントが従うことを許可します。 Widelink エントリーは、共有ごとに有効にすることができます。

Widelink エントリーには以下の要件があります。

- 絶対シンボリック・リンクが置かれている共有は、ワイド・シンボリック・リンクに対して有効になっている必要があります。
- 絶対シンボリック・リンクを解決するために、リンクの宛先を決定する `/etc/symlink.translations` ファイルに Widelink エントリーが登録されている必要があります。
- Widelink エントリーの宛先は、以下のいずれかである必要があります。
 - シンボリック・リンクと同一の共有
 - 同じストレージ・システム上の別の共有
 - 別のストレージ・システム上の共有
 - 別の CIFS サーバーまたはデスクトップ PC 上の共有
- CIFS クライアントは Microsoft 分散ファイル・システム (DFS) に関するクライアント・サイドのサポートがあることが必要です。 Windows NT 以降のクライアントは、デフォルトで DFS をサポートします。

Widelink エントリーに従うために、CIFS クライアントは自動的にストレージ・システムからの DFS 参照を要求および受信して、ターゲットの共有と認証された接続を確立します。これにより、シンボリック・リンクおよび宛先の両方について NT 共有セキュリティが保持されます。いったん接続が確立されると、CIFS クライアントはターゲットの共有あるいはサーバーへの新規の要求を直接行うことができ、それによってパフォーマンスが向上します。

Map エントリーと Widelink エントリーの両方を `symlink.translations` ファイルに持つ場合は、ストレージ・システムは最初に発見した適合エントリーを使用します。

Widelink エントリーには以下の制限があります。

- たとえワイド・シンボリック・リンクの宛先がファイルであっても、ディレクトリー・リストではディレクトリーとして表示されます。ファイルを開くためのシステム API は、ワイド・シンボリック・リンクに正確に従いますが、これは一部のアプリケーションを混乱させる可能性があります。この問題を回避するために、ファイルよりはディレクトリーへ帰着するワイド・シンボリック・リンクを作成することをお勧めします。

- Windows 95、Windows 98、および Windows ME クライアントは、別のワイド・シンボリック・リンクへのワイド・シンボリック・リンクをたどることはできません。
- Windows NT クライアントは、ワイド・シンボリック・リンクについて有効にされた共有内の ACL を表示あるいは変更することができません。この制限は、Windows 2000 以降のクライアントでは適用されません。
- ワイド・シンボリック・リンクは、クライアントを宛先マシン上の非共有領域へ方向づけすることはできません。

シンボリック・リンクに関する共有境界チェックの無効化について

シンボリック・リンクに関する共有境界チェックを無効にする際には、CIFS クライアントはストレージ・システム上のすべてのシンボリック・リンクに従います。この動作は共有ごとに設定されており、相対および絶対シンボリック・リンクのいずれにも影響します。

シンボリック・リンクに関する共有境界チェックの無効化には、以下の要件があります。

- シンボリック・リンクを持つ共有は、`nosymlink_strict_security` に設定されなければなりません。
- 絶対シンボリック・リンクを解決するために、リンクの宛先を決定する `/etc/symlink.translations` ファイルに `Map` エントリーが登録されている必要があります。
- 相対シンボリック・リンクおよびマッピングされた絶対シンボリック・リンクの宛先は、ストレージ・システムのいずれかの共有領域あるいは非共有領域にある可能性があります。

シンボリック・リンクに関する共有境界チェックの無効化には、以下の制限があります。

- 相対シンボリック・リンクはボリューム間をまたぐ場合には使用することができません。絶対シンボリック・リンクを使用してください。
- シンボリック・リンクは、ストレージ・システムから別のシステムにたどることはできません。
- CIFS クライアントは、シンボリック・リンクが置かれている共有への接続を認証する必要があるため、NT 共有セキュリティは、シンボリック・リンク自体については保持されます。
- NT 共有セキュリティは、宛先が同一の共有内にある場合に限り、シンボリック・リンクの宛先については保持されます。
- NT 共有セキュリティは、宛先が共有の外部にある場合は、CIFS クライアントが (CIFS 共有であろうとなかろうと) 宛先への認証を行う必要がないため、シンボリック・リンクの宛先について保持されません。

注: シンボリック・リンクに関する共有境界チェックを無効にする場合は、ユーザーにアクセスさせたくないストレージ・システムの領域の保護を確実にしてください。このことは、ユーザーがストレージ・システム上のあらゆるパスにシンボリック・リンクを作成することができるため、必要となります。

絶対シンボリック・リンクのリダイレクト

Map エントリーを `/etc/symlink.translations` ファイルに作成する、あるいは Widelink エントリーを `/etc/symlink.translations` ファイルに作成することで、ストレージ・システム上の絶対シンボリック・リンクをリダイレクトすることができます。

このタスクについて

NFS クライアントは、絶対シンボリック・リンクによって示されたファイル・システムの位置を、ファイル・システムがどのようにクライアントにマウントされているかに基づいて解釈します。CIFS クライアントは、NFS クライアントのマウント情報へのアクセス権を持っていません。

CIFS クライアントがストレージ・システム上の絶対シンボリック・リンクに従うことを許可するには、絶対シンボリック・リンクをリダイレクトして CIFS クライアントが絶対シンボリック・リンクによって示されたファイル・システムの位置を解釈できるようにする必要があります。 `/etc/symlink.translations` ファイルにエントリーを作成することで、絶対シンボリック・リンクをリダイレクトすることができます。 `/etc/symlink.translations` ファイルは、UNIX サーバーでの自動マウント機能と同じ役割をストレージ・システム上で実行します。

Map エントリーの作成

`/etc/symlink.translations` ファイルを編集することで、Map エントリーを作成することができます。

1. 編集のために `/etc/symlink.translations` ファイルを開きます。
2. 次のフォーマットを使用して、ファイルに 1 行以上入力します。Map *template* *result*

パラメーター	説明
<i>template</i>	絶対シンボリック・リンクとマッチングするために使用されます
<i>result</i>	絶対シンボリック・リンクのマッチングのために置換されたストレージ・システム・パス

注: ファイル・パスのスペースあるいはシャープ (#) を示すために、円記号 (¥) エスケープ文字を前に付加する必要があります。

例

```
Map /u/users/charlie/* /home/charlie/*
```

```
Map /temp1/* /vol/vol2/util/t/*
```

```
Map /u/users/bob¥ smith/* /home/bob¥ smith/*
```

Widelink エントリーの作成

`/etc/symlink.translations` ファイルを編集することで、Widelink エントリーを作成することができます。

1. 編集のために `/etc/symlink.translations` ファイルを開きます。

2. 次のフォーマットを使用して、ファイルに 1 行以上入力します。Widelink
template [*@qtree*] *result*

パラメーター	説明
<i>template</i>	UNIX パス名
<i>result</i>	CIFS UNC パス名
<i>qtree</i>	異なる qtree にある複数のエントリーが同一のテンプレート値を持つことを許可するために、任意で指定することができます

注: Map エントリーと異なり、円記号 (¥) エスケープ文字を先頭につけずに、ファイル・パスにスペースおよびシャープ (#) 文字を指定することができます。実際、Widelink エントリーでは、円記号 (¥) 文字は汎用命名規則に合致する標準的なファイル・パス文字です。

例

以下の例では、*result* が分離文字として円記号 (¥) を持つ CIFS パス名構文を使用しており、スペースの組み込みを許可しています。テンプレート・パス名のワイルドカード文字 (*) は、円記号 (¥) 文字を含めて 0 個以上の文字を表しています。*result* パス名で、ワイルドカード文字はテンプレート・パス名の対応するマッチングからのテキストを表しています。

```
Widelink /eng/proj/* @/vol/vol2 ¥¥filer¥hw¥proj¥*
```

```
Widelink /eng/proj/* ¥¥filer¥sw¥proj¥*
```

ストレージ・システムによる Map エントリーおよび Widelink エントリーの使用方法

CIFS クライアントが絶対シンボリック・リンクに従うことを許可するために、ストレージ・システムは `etc/symlink.translations` ファイル内のエントリーを、マッチング・エントリーが見つかるか検索が失敗するまで順次に検索します。

ストレージ・システムは、最初に見つけたマッチング・エントリーを使用して宛先へのパスを生成します。そのため、早期のマッピング・エラーを防ぐために、最も限定的なエントリーを最初に置くことが重要です。

この例では、Map エントリーのリスト方法を示しています。`/u/home/*` は `/u/*` よりも限定されています。

```
Map /u/home/* /vol/vol2/home/*
```

```
Map /u/* /vol/vol0/*
```

この例では、Widelink エントリーのリスト方法を示しています。

```
Widelink /u/docs/* ¥¥filer¥engr¥tech pubs¥*
```

```
Widelink /u/* ¥¥filer¥engr¥*
```

CIFS クライアントのための NFS ディレクトリー・アクセスの最適化

CIFS クライアントあるいは NFS クライアントのいずれかがディレクトリーにアクセスして Unicode フォーマットのディレクトリーのみを作成するときに、Data ONTAP が非 Unicode のディレクトリーを Unicode フォーマットに変換するように構成することで、NFS ディレクトリーへの CIFS クライアント・アクセスを最適化することができます。それによって、フォーマットを変換する必要を除去します。

このタスクについて

注: CIFS および NFS クライアントの間でファイルを共有する場合は、Data ONTAP をインストール直後に Unicode フォーマットでディレクトリーを作成するように構成します。これにより、すべての新規ディレクトリーは確実に Unicode フォーマットで作成されるようになります。

最初に Data ONTAP をインストールするときには、NFS クライアントによって作成されたディレクトリーは非 Unicode フォーマットで作成されており、CIFS クライアントによって作成されたディレクトリーは Unicode フォーマットで作成されています。これが原因で、CIFS ディレクトリーは NFS クライアントからアクセス可能ですが、NFS ディレクトリーは CIFS クライアントからアクセス可能ではありません。CIFS クライアントに NFS ディレクトリーへのアクセス権を提供するには、まずストレージ・システムが NFS ディレクトリーを Unicode フォーマットに変換する必要があります。これは、ストレージ・システムがアクセス要求を受信したときに自動的に (稼動中に) 実行されます。含まれるデータの量によって、Unicode 変換は時間を要し、ストレージ・システムのリソースを消費します。

Unicode フォーマットのディレクトリーの作成

`vol options` コマンドを使用すると、Data ONTAP はすべてのディレクトリーを Unicode フォーマットで作成します。

次のコマンドを入力してください。 `vol options volume_name create_unicode on`

Unicode フォーマットへの変換

デフォルトでは、Data ONTAP は CIFS クライアントがアクセスを要求したときのみ、ディレクトリーの Unicode 変換を実行します。ディレクトリーごとのエントリーを 50,000 より少なく制限することで、Unicode 変換に必要な時間を削減することができます。

このタスクについて

既に大容量のディレクトリーを持っている場合、以下の手順に記載しているように大容量のディレクトリーの Unicode 変換を先に強制することで、Unicode 変換のパフォーマンスへの影響を最小化することができます。

大容量ディレクトリーの Unicode 変換を強制し、また CIFS および NFS クライアントの両方からアクセスされたときにディレクトリーを Unicode フォーマットに変換するには、以下の手順を完了します。

1. 50,000 を超えるファイルを含むディレクトリーがある場合、変換したいディレクトリーと同じ `qtree` 内の同じボリュームに、Windows クライアントから新規の

CIFS ディレクトリーを作成し、作成したディレクトリーに `NFS mv` コマンドを使用してファイルを移動させ、状況に応じて古いディレクトリーを削除してその名前を新規のディレクトリーに割り当てます。

2. 次のコマンドを入力します。 `vol options volume_name convert_ucode on`
Unicode 変換は、NFS クライアントがファイルにアクセスしたときに実行されず。

注: 50,000 を超えるファイルを含むディレクトリーがある場合は、`convert_ucode` オプションを有効にしないでください。

CIFS クライアントの大文字ファイル名の作成の防止

`cifs.save_case` オプションを `off` に設定することで、CIFS クライアントが大文字のファイル名を作成することを防止することができます。

このタスクについて

古い 16 ビット CIFS クライアントは、ファイルをオープンあるいは保存するときに、小文字あるいは大/小文字混合をすべて大文字に変更することでファイル名を変更します。Data ONTAP が小文字を使用して CIFS ファイル名を保管するように強制することで、これらの大文字のファイル名を防止します。

次のコマンドを入力します。 `options cifs.save_case off`

NFS クライアントから CIFS ファイルへのアクセス

Data ONTAP は、Windows NT ファイル・システム (NTFS) セキュリティー・セマンティクスを使用して、NFS クライアントの UNIX ユーザーが混合あるいは NTFS qtree のファイルへのアクセス権を持っているかどうかを判別します。

このタスクについて

Data ONTAP は、ユーザーの UNIX ユーザー ID (UID) を CIFS 資格情報に変換することでこれを行い、次に、CIFS 資格情報を使用してユーザーがファイルへのアクセス権を持っているかを検証します。CIFS 資格情報は、プライマリーのセキュリティー ID (SID)、通常はユーザーの Windows ユーザー名、およびユーザーがメンバーになっている Windows グループに対応する 1 つ以上のグループ SID から構成されています。

Data ONTAP が UNIX UID を CIFS 資格情報に変換するのに要する時間は、プロセスがドメイン・コントローラーへのコンタクトを必要とするため、数 10 ミリ秒から数 100 ミリ秒です。Data ONTAP は、UID を CIFS 資格情報にマッピングし、変換による検証時間を削減するためにマッピングを WAFL 資格情報キャッシュに入力します。Data ONTAP が権限を検証するのに要する時間をさらに削減できるように、WAFL 資格情報キャッシュをコントロールすることができます。また、どの CIFS 資格情報が現在 WAFL 資格情報キャッシュに入っているかを確認するのに助けるために、WAFL 資格情報キャッシュの統計を監視することができます。

WAFL 資格情報キャッシュへのマッピング・エントリーの追加

マッピング・エントリーを、いつでも WAFL 資格情報キャッシュに追加することができます。通常は、ストレージ・システムがアクセスされたときに自動的にエントリーが作成されるため、この作業は必要ありません。

始める前に

WAFL 資格情報キャッシュに追加したいエントリーの名前と IP アドレスが必要です。

このタスクについて

エントリーを追加する最善の方法は、ブート時に WAFL 資格情報キャッシュをエントリーと一緒に読み込むスクリプトに入れることです。これは、Data ONTAP がファイルへのアクセス経路にエントリーを作成するのを待つより、すぐにエントリーを WAFL 資格情報キャッシュに置きます。

注: キャッシュは 10,000 エントリーに制限されています。この制限を超えると、古いエントリーは削除されます。

次のコマンドを入力します。 `wcc -a -u uname -i ipaddress`

パラメーター	説明
<i>uname</i>	ユーザーの UNIX 名
<i>ipaddress</i>	ユーザーがいるホストの IP アドレス

WAFL 資格情報キャッシュからのマッピング・エントリーの削除

マッピング・エントリーを、いつでも WAFL 資格情報キャッシュから削除することができます。セキュリティーの変更を実施した後、確実にその変更がすぐに有効になるように、エントリーを削除することをお勧めします。

始める前に

WAFL 資格情報キャッシュから削除したいエントリー名を把握している必要があります。さらに選択を絞り込むために、任意で IP アドレスを指定することができます。

このタスクについて

セキュリティー変更は、ユーザーの権限を変更した場合はすぐには有効になりません。例えば、WAFL 資格情報キャッシュに既に存在しているユーザーをグループから削除したり、そのユーザーのマッピングを削除した場合、WAFL 資格情報キャッシュのエントリーが自動的にタイムアウトになるまでは、ユーザーはそのグループのファイル・アクセス権を所有し続けます。デフォルトの資格情報キャッシュのタイムアウト期間は 20 分です。

コマンド `wcc -x name` を入力します。 *name* は、次の指定の 1 つです。 `-s` には、CIFS 資格情報で検出された Windows ユーザー名またはグループ名が続き、あるいは `-u` には、CIFS 資格情報で検出された UNIX 名が続きます。

注: `name` がグループ名の場合、この手順は WAFL 資格情報キャッシュからそのグループのすべてのメンバーを削除します。

後にそのユーザーがいるホストの IP アドレスが続く `-i` を追加することで、さらにユーザーの指定を絞り込むことができます。 `name` を指定しない場合、すべてのエントリーが削除されます。

タスクの結果

例

```
wcc -x -u jdoe -i 10.100.4.41
```

マッピング・エントリーが有効な期間の設定

Data ONTAP による更新後に、CIFS 資格情報が WAFL 資格情報キャッシュに残る時間を増やすことで、パフォーマンスが改善されます。 Data ONTAP がファイルへのアクセスを検証するために CIFS 資格情報を作成するための時間を消費する必要がないため、パフォーマンスが改善されます。

このタスクについて

CIFS 資格情報が WAFL 資格情報キャッシュに残る時間を増やすことの欠点は、ユーザーのアクセス権を変更した場合に、Data ONTAP が WAFL 資格情報キャッシュを更新するまでその変更が有効にならないことです。この場合、アクセスを拒否したばかりのファイルへのアクセス権を、ユーザーが一時的に保持している可能性があります。

このタイプの問題を望まない場合は、資格情報エントリーが有効な時間を減らすことができます。アクセス権の変更を行ったときにすぐに更新される必要があり、パフォーマンスの低下が問題ではない場合は、デフォルトより小さい値を使用することができます。

コマンド `options wafl.wcc_minutes_valid n` を入力します。 *n* は、各エントリーを有効にしたい分数です。 1 から 20,160 の範囲で指定できます。デフォルト値は 20 です。

WAFL 資格情報キャッシュ統計の監視

WAFL 資格情報キャッシュ統計の監視により、どのエントリーが現在キャッシュされているか、および UNIX UID-to-CIFS マッピングを表示することができます。この情報は、どのエントリーが WAFL 資格情報キャッシュにあるか、あるいはエントリーにリストされているユーザーのアクセス権は何かを知りたいときに役に立ちます。

コマンド `wcc -d uname` を入力します。 *uname* は、ユーザーの UNIX 名です。 WAFL 資格情報キャッシュのすべての資格情報エントリーをリストするには、 *uname* を省略します。コマンド行に `-v` を追加することで、より詳細な情報を取得することができます。コマンドごとに、 `-v` オプションを最大 3 つのインスタンスまで (`-vvv`) 持つことができます。各インスタンスは詳細のレベルの増加を表します。

出力例

以下の例は、-d オプションを使用した場合の統計の出力を示しています。

wcc -d

tday (UID 10350) from 10.121.4.41 => NT-DOMAIN\tday*

Total WCC entries: 3; oldest is 127 sec.

Total Administrator-privileged entries: 1

* indicates members of "BUILTIN\Administrators" group

以下の例は、-v オプションを 2 つ使用した場合の統計の出力を示しています。

wcc -dvv

jdoe (UID 1321) from 10.121.4.41 => NT-DOMAIN\jdoe

UNIX uid = 1321

NT membership

NT-DOMAIN\jdoe

NT-DOMAIN\Domain Users

NT-DOMAIN\SU Users

NT-DOMAIN\Installers

NT-DOMAIN\tglob

NT-DOMAIN\Engineering

BUILTIN\Users

User is also a member of Everyone, Network Users,

Authenticated Users

tday (UID 10350) from 10.121.4.41 => NT-DOMAIN¥tday*

UNIX uid = 10350

NT membership

NT-DOMAIN¥tday

NT-DOMAIN¥Domain Users

NT-DOMAIN¥Domain Admins

NT-DOMAIN¥SU Users

NT-DOMAIN¥Installers

BUILTIN¥Users

BUILTIN¥Administrators

User is also a member of Everyone, Network Users,

Authenticated Users

bday (UID 1219) from 10.121.4.41 => NT-DOMAIN¥bday

UNIX uid = 1219

NT membership

NT-DOMAIN¥bday

NT-DOMAIN¥Domain Users

NT-DOMAIN¥Installers

NT-DOMAIN\SU Users

BUILTIN\Users

User is also a member of Everyone, Network Users,

Authenticated Users

Total WCC entries: 3; oldest is 156 sec.

Total Administrator-privileged entries: 1

* indicates members of "BUILTIN\Administrators" group

マッピング不整合の管理

いくつかのタスクを実行することで、マッピング不整合を管理することができます。

このタスクについて

アクセス可能なはずのファイルにユーザーがアクセスできない場合、以下のようないくつかの理由が考えられます。

- 最近アクセスを許可したが、WAFL 資格情報キャッシュが新しいマッピング・エントリを持っていません。最近認可したアクセス権と WAFL 資格情報キャッシュの間のマッピング不整合を、CIFS 資格情報マッピングを比較することで判別することができます。ユーザーの UNIX 名あるいはユーザーの Windows 名に関するマッピングの結果を表示することができます。
 - NFS クライアントは、CIFS 資格情報を入手することができません。NFS クライアントが CIFS ログインをトレースすることで、ストレージ・システムへのログインを実行できるかを判別することができます。
 - NFS クライアントによっては、CIFS 資格情報を有効にするための変更前に NFS 属性キャッシュがタイムアウトになるのを待つ必要がある場合があります。
1. 次のコマンドを入力して、UNIX 名の現在の CIFS 資格情報マッピングを表示することができます。wcc -s uname ここで uname は、Windows ユーザー名です。後にそのユーザーがいるホストの IP アドレスが続く -i を追加することで、さらにユーザーの指定を絞り込むことができます。コマンド行に -v を追加することで、より詳細な情報を取得することができます。コマンドごとに、-v オプションを最大 3 つのインスタンスまで (-vvv) 持つことができます。各インスタンスは詳細のレベルの増加を表します。
 2. CIFS 資格情報をメモします。
 3. すべての接続ユーザーの情報を表示するには、次のコマンドを入力します。cifs sessions -s 出力内のユーザーの情報を見つけます。

4. 2 つの CIFS 資格情報マッピングを比較します。
5. CIFS 資格情報マッピングが異なっていた場合、次のコマンドを入力してクライアントを切断します。cifs terminate workstation クライアントが再接続すると、CIFS 資格情報マッピングは修正されています。

CIFS ログインのトレース

CIFS 資格情報を取得するための NFS クライアントによるあらゆる試行を監視することで、CIFS ログインをトレースすることができます。

このタスクについて

注: CIFS ログイン・トレースはすべての CIFS ログインを報告するため、慎重に使用してください。永続的な使用によって、システム・パフォーマンスに影響する過度のコンソールおよびログのメッセージを引き起こす可能性があります。

cifs.trace_login オプションは診断目的でのみオンにするべきで、その他のときはオフのままにしておくことが推奨されます (デフォルトはオフです)。

次のコマンドを入力します。options cifs.trace_login on | off CIFS ログイン・トレースを有効にするために on を、無効にするために off を使用します。

ドメイン・コントローラー接続のトレース

ドメイン・コントローラー接続を改善しようと数分ごとに試みるたびに、Data ONTAP がコンソールにメッセージを送信するように構成することができます。

このタスクについて

注: トレース機能は多くのメッセージをコンソールおよびシステム・ログに送信するため、このオプションを長時間有効にしないようにしてください。

次のコマンドを入力します。options cifs.trace_dc_connection on | off デフォルトは off です。

UNIX の「実行」アクセス権がない場合でも、.dll および .exe ファイルを実行するための、CIFS クライアントへ暗黙的アクセス権の提供

cifs.grant_implicit_exe_perm オプションを on に設定し、UNIX 実行可能ビットが設定されていない場合でも CIFS クライアントが .dll および .exe ファイルを実行することを許可できます。

次のコマンドを入力します。options cifs.grant_implicit_exe_perm on

タスクの結果

UNIX の「読み取り」アクセス権のみでの実行可能権限は、CIFS クライアントからの実行時に暗黙的に認可される実行許可です。

FTP を使用したファイル・アクセス

Windows および UNIX の FTP クライアントのユーザーが、ご使用のストレージ・システム上のファイルにアクセスすることを許可するために、インターネット・ファイル転送プロトコル (FTP) サーバーを有効に設定し構成することができます。

FTP サーバーの有効化あるいは無効化

FTP サーバーを有効にするには、`ftpd.enable` オプションを `on` に設定し、FTP サーバーを無効にするには、`ftpd.enable` オプションを `off` に設定します。デフォルトでは、このオプションは `off` です。

以下を実施したい場合、	以下を実行してください。
FTP サーバーを有効にする	次のコマンドを入力します。options <code>ftpd.enable on</code> これにより、FTP サーバーが標準の FTP ポート 21 で FTP 要求の <code>listen</code> を始めます。
FTP サーバーを無効にする	次のコマンドを入力します。options <code>ftpd.enable off</code>

FTP 認証スタイルの指定

FTP サーバーを UNIX、Windows、あるいは両方の認証スタイルを使用するように構成するには、`ftpd.auth_style` オプションをそれぞれ、`unix`、`ntlm` あるいは `mixed` に設定します。デフォルトでは、このオプションは `mixed` です。

このタスクについて

UNIX 認証スタイルを指定した場合、FTP サーバーは `/etc/passwd` ファイルあるいはネットワーク情報サービス (NIS) サーバーを使用してユーザーを認証します。

NTLM 認証スタイルを指定した場合、FTP サーバーは Windows ドメイン・コントローラーを使用してユーザーを認証します。NTLM 認証スタイルは暗号化されたユーザー名およびパスワードを使用するため、UNIX 認証スタイルよりセキュアです。

混合認証スタイルを指定した場合は、FTP サーバーは円記号 (¥) あるいはアットマーク ("@") 文字を含む名前のユーザーには UNIX 認証スタイルを使用し、他のすべてのユーザーには NTLM 認証スタイルを使用します。

1. コマンド `options ftpd.auth_style style` を入力します。*style* は、`unix`、`ntlm`、あるいは `mixed` です。
2. ステップ 1 で `ntlm` を指定した場合は、`/etc/cifs_homedir.cfg` ファイルで CIFS ホーム・ディレクトリーを指定し、次にコマンド `cifs homedir load` を入力します。ユーザーのホーム・ディレクトリーは、`/etc/cifs_homedir.cfg` で指定したパスとユーザーのユーザー ID の組み合わせです。`/etc/cifs_homedir.cfg` で指定するパスは大/小文字の区別をします。ただし、ユーザー ID は大/小文字の区別を

しません。例えば、パスが `¥home` でユーザー名が `JOHN` の場合、そのユーザーのホーム・ディレクトリーは `¥home¥john` です。

次のタスク

`ftpd.auth_style` オプションを `unix` に設定し、以前に `NIS` を有効にしていた場合 (`nis.enable` オプションが `on` の場合)、`/etc/nsswitch` ファイルに適切な `passwd` エントリーを追加する必要があります。

- `/etc/passwd` ファイルのみを使用してユーザーを認証するには、次のエントリーを追加します。`passwd: files`
- `NIS` のみを使用してユーザーを認証するには、次のエントリーを追加します。`passwd: nis`
- `/etc/passwd` ファイルと `NIS` の両方を使用してユーザーを認証するには、次のエントリーを追加します。`passwd: files nis`

NTLM 認証スタイルの制限

NTLM 認証スタイルにはいくつかの制限があります。

- ユーザーのホーム・ディレクトリーは、小文字の名前のみが許可されます。ユーザー名を大文字で指定した場合でも、ユーザーのホーム・ディレクトリーには小文字の名前を指定する必要があります。さもないと、ユーザーはログイン後にファイルにアクセスすることができません。
- NTLMv2 は、ストレージ・システム上にはないドメイン・コントローラー・ベースのサービスに依存しています。このため、ワークグループ・モードで作動しているストレージ・システムに接続するには、NTLMv1 以前のみが使用できます。
- NTLM 認証を使用するワークグループ・ストレージ・システム Windows クライアントは、「LAN マネージャー認証レベル」を「NTLMv2 のみ」以外に設定する必要があります。このオプションの設定は、「LMCompatibilitylevel」に関するレジストリー値を 0、1、または 2 に変更します。これらは、ワークグループ環境についてストレージ・システムがサポートする唯一の NTLM 設定です。
- Active Directory 環境のドメイン・ベースのクライアントは、(要求がストレージ・システムからドメイン・コントローラーに受け渡されるため) NTLMv2 を使用して認証することが可能ですが、ローカル・ストレージ・システムのアカウントに関する接続情報は、ドメイン・コントローラーでは使用できません。これにより、ローカル・ストレージ・システムのアカウントは、このような環境にあるストレージ・システムへの接続を試行している間は、認証に失敗します。

FTP 全探索チェックのバイパスの有効化あるいは無効化

`ftpd.bypass_traverse_checking` オプションを `on` あるいは `off` に設定することで、FTP 全探索チェックのバイパスをそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは `off` に設定されています。

このタスクについて

`ftpd.bypass_traverse_checking` オプションが `off` に設定されている場合、ユーザーが FTP プロトコルを使用してファイルにアクセスしようと試みると、Data ONTAP はファイルへのパスにあるすべてのディレクトリーについて (実行) 権限の全探索をチ

エックします。いずれかの中間ディレクトリーに X (実行権限) がない場合は、Data ONTAP はファイルへのアクセスを拒否します。 `ftpd.bypass_traverse_checking` オプションが `on` に設定されている場合、ユーザーがファイルへのアクセスを試みたときに、Data ONTAP はファイルへのアクセスを認可するか拒否するかを判断するのに、中間ディレクトリーのアクセス権の全探索チェックを行いません。

FTP 全探索チェックのバイパスを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
FTP 全探索チェックのバイパスを有効にする	次のコマンドを入力します。options <code>ftpd.bypass_traverse_checking on</code>
FTP 全探索チェックのバイパスを無効にする	次のコマンドを入力します。options <code>ftpd.bypass_traverse_checking off</code>

匿名 FTP アクセスの管理

匿名 FTP アクセスの有効化あるいは無効化、および匿名ユーザーのためのホーム・ディレクトリーおよびユーザー名の指定によって、匿名 FTP アクセスを管理することができます。

匿名 FTP アクセスの有効化あるいは無効化

匿名 FTP アクセスを有効あるいは無効にするには、`ftpd.anonymous.enable` オプションをそれぞれ `on` あるいは `off` に設定します。デフォルトでは、このオプションは `off` です。

以下を実施したい場合、	以下を実行してください。
匿名 FTP アクセスを有効にする	次のコマンドを入力します。options <code>ftpd.anonymous.enable on</code>
匿名 FTP アクセスを無効にする	次のコマンドを入力します。options <code>ftpd.anonymous.enable off</code>

次のタスク

匿名 FTP アクセスを有効にする場合、以下のタスクを実行する必要があります。

- 匿名 FTP ユーザー用のユーザー名を指定する。
- 匿名 FTP ユーザー用のホーム・ディレクトリーを指定する。

匿名 FTP ユーザーのためのユーザー名の指定

匿名 FTP ユーザーのためのユーザー名を指定するには、`ftpd.anonymous.name` オプションを設定します。デフォルトでは、匿名 FTP ユーザーのためのユーザー名は「anonymous」です。

このタスクについて

FTP 認証スタイルが `unix` の場合、このオプションを使用して指定したユーザー名は、`/etc/passwd` ファイルで `ftp` ユーザーのために指定したユーザー名をオーバーライドします。

コマンド `options ftpd.anonymous.name username` を入力します。*username* は、匿名ユーザーの名前です。

匿名 FTP ユーザーのためのホーム・ディレクトリーの指定

匿名 FTP ユーザーのためのホーム・ディレクトリー (匿名 FTP ユーザーがアクセス権を持っている唯一のディレクトリー)を指定するには、`ftpd.anonymous.home_dir` オプションを使用します。

このタスクについて

FTP 認証スタイルが `unix` の場合、このオプションで指定したホーム・ディレクトリーは、`/etc/passwd` ファイルあるいは `NIS` で `ftp` ユーザーのために指定したホーム・ディレクトリーをオーバーライドします。

1. 匿名 FTP ユーザーのためのホーム・ディレクトリーを作成します。
2. 次のコマンドを入力します。`options ftpd.anonymous.home_dir homedir`
homedir は、匿名 FTP ユーザーのためのホーム・ディレクトリーの名前です。

次のタスク

ステップ 1 で作成したディレクトリーに対して、匿名 FTP ユーザーが読み取り権限を持っていることを確認してください。詳細情報については、「*Data ONTAP ストレージ管理ガイド*」を参照してください。

注: FTP サーバーが `NTLM` 認証スタイルで匿名 FTP ユーザーを認証する場合は、FTP ユーザーは `null` ユーザーと同じアクセス権を持っています。

FTP アクセスの制限

FTP ユーザーのブロック、および特定のディレクトリー (ユーザーのホーム・ディレクトリーあるいはデフォルト・ディレクトリーのいずれか) への FTP ユーザーの制限によって、FTP アクセスを制限することができます。

特定の FTP ユーザーのブロック

特定のユーザーがストレージ・システムにアクセスすることを防ぐためには、そのユーザーを `/etc/ftpusers` ファイルに追加します。

1. `NFS` あるいは `CIFS` クライアントからストレージ・システムのデフォルト・ボリューム (デフォルトでは `/vol/vol0`) の `/etc` ディレクトリーにアクセスします。
2. `/etc/ftpusers` ファイルをテキスト・エディターで開きます。(ファイルがない場合は作成します。)
3. アクセスを拒否したいユーザーのユーザー名を追加します (1 行につき 1 ユーザー名)。 `NTLM` 認証では、以下のフォーマットのいずれかを使用してユーザー名を指定する必要があります。
 - `Domain\username`
 - `Username@domain`

注: 前者のフォーマットでは、正確なドメイン名を指定する必要があります。そうしない場合、FTP サーバーはユーザーに対してアクセスを拒否しません。例えば、ドメイン名が「.com」接尾部を含んでいる場合、その接尾部まで含んだドメイン名を指定する必要があります。

4. /etc/ftpusers ファイルを保存します。

特定のディレクトリーへの FTP ユーザーの制限

FTP ユーザーを特定のディレクトリーに制限するには、`ftpd.dir.restriction` オプションを `on` に設定します。あるいは、FTP ユーザーがストレージ・システム全体にアクセスすることを許可するには、`ftpd.dir.restriction` オプションを `off` に設定します。デフォルトでは、このオプションは `on` です。

FTP ユーザーをホーム・ディレクトリーに制限する、あるいはストレージ・システム全体へのアクセスを許可します。

以下を実施したい場合、	以下を実行してください。
FTP ユーザーを、ホーム・ディレクトリーあるいはデフォルト・ディレクトリーに制限する	次のコマンドを入力します。options <code>ftpd.dir.restriction on</code>
FTP ユーザーのストレージ・システム全体へのアクセスを許可する	次のコマンドを入力します。options <code>ftpd.dir.restriction off</code>

次のタスク

`ftpd.dir.restriction` オプションを `on` に設定した場合、`ftpd.dir.override` オプションを使用して、FTP ユーザーがホーム・ディレクトリーあるいはデフォルト・にアクセスできるかを指定することができます。

ユーザーのホーム・ディレクトリーあるいはデフォルト・ディレクトリーへの FTP ユーザーの制限

デフォルト・ディレクトリーへの FTP ユーザーを制限するには、`ftpd.dir.override` オプションを設定します。あるいは、ホーム・ディレクトリーへの FTP ユーザーを制限するには、`ftpd.dir.override` オプションを消去します。デフォルトでは、このオプションは消去されています。

始める前に

`ftpd.dir.override` オプションを設定する前に、`ftpd.dir.restrictions` オプションを `on` に設定する必要があります。

このタスクについて

以下を実施したい場合、	以下を実行してください。
ホーム・ディレクトリーへの FTP ユーザーの制限	次のコマンドを入力します。options <code>ftpd.dir.override ""</code>
デフォルト・ディレクトリーへの FTP ユーザーの制限	次のコマンドを入力します。options <code>ftpd.dir.override <i>directory</i></code> ここで <i>directory</i> は、FTP ユーザーを制限したいデフォルト・ディレクトリーの名前です。

次のタスク

ステップ 1 で作成したディレクトリーに対して、FTP ユーザーが読み取り権限を持っていることを確認してください。詳細情報については、「Data ONTAP ストレージ管理ガイド」を参照してください。

FTP ログ・ファイルの管理

FTP ログ・ファイルの表示、FTP ログ・ファイルの最大数の指定、および現行の FTP ログ・ファイルの最大サイズの指定によって、FTP ログ・ファイルを管理することができます。

FTP サーバーのログ・ファイル管理方法

Data ONTAP は、すべての FTP サーバーの要求を `/etc/log/ftp.cmd` ファイルに記録し、すべてのファイル転送を `/etc/log/ftp.xfer` ファイルに記録します。

Data ONTAP は、FTP ログ・ファイルが最大サイズに達するまで、FTP ログ・ファイル (`/etc/log/ftp.cmd` または `/etc/log/ftp.xfer` ファイル) にデータを書き込みます。その後、Data ONTAP は以下のタスクを実行します。

1. FTP ログ・ファイルの総数が FTP ログ・ファイルの最大数と等しい場合、最も古い FTP ログ・ファイルを削除します。
2. 古い FTP ログ・ファイルの接尾部を増やします。
3. .1 接尾部を現在の FTP ログ・ファイルに追加し、それにより古い FTP ログ・ファイルにします。
4. 新規の FTP ログ・ファイルを作成します。

例

ログ・ファイルの最大数を 6 と仮定した場合、`/etc/log/ftp.xfer` ログ・ファイルが最大サイズに達すると、Data ONTAP は以下のタスクを実行します。

1. `/etc/log/ftp.xfer.5` ファイルが存在する場合、削除します。
2. `/etc/log/ftp.xfer.4` を `/etc/log/ftp.xfer.5` に、`/etc/log/ftp.xfer.3` を `/etc/log/ftp.xfer.4` に、というように順に名前変更します。
3. `/etc/log/ftp.xfer` を `/etc/log/ftp.xfer.1` に名前変更します。
4. 新規の `/etc/log/ftp.xfer` ログ・ファイルを作成します。

`/etc/log/ftp.xfer` ログ・ファイルのフォーマット

`/etc/log/ftp.xfer` ファイルは、FTP サーバーが転送するすべてのファイルの情報を含みます。

以下の表は、`/etc/log/ftp.xfer` ファイル内のフィールドを示しています。

フィールド	説明
timestamp	ログ・レコードのタイム・スタンプ
xferTime	秒単位でのファイル転送の所要時間

フィールド	説明
clientIP	FTP クライアントの IP アドレス
xferCount	転送ファイルのバイト数
filename	転送ファイルのファイル名
xferType	「a」(ASCII)、「e」(EBCDIC)、または「b」(バイナリー)
xferDirection	「o」(アウトバウンド) あるいは「i」(インバウンド)
accessType	「a」(匿名)、「r」(実ユーザー)、あるいは「g」(ゲスト)

/etc/log/ftp.cmd ログ・ファイルのフォーマット

/etc/log/ftp.cmd ファイルは、FTP サーバーが受信するすべてのコマンドの情報を含みます。

以下の表は、/etc/log/ftp.cmd ファイル内のフィールドを示しています。

フィールド	説明
timestamp	ログ・レコードのタイム・スタンプ
serialNo	FTP 接続のシリアル番号
command	FTP コマンド

FTP ログ・ファイルの表示

FTP ログ・ファイルを表示するには、テキスト・エディターあるいはビューアーでそのファイルを開きます。

このタスクについて

FTP サーバーは次の 2 つのログ・ファイルを保持します。

- /etc/log/ftp.cmd ファイルは、FTP サーバーが受信するすべてのコマンドの情報を含みます。
 - /etc/log/ftp.xfer ファイルは、FTP サーバーが転送するすべてのファイルの情報を含みます。
1. ストレージ・システムのデフォルト・ボリューム (デフォルトでは /vol/vol0) 上の /etc/log ディレクトリーに、NFS あるいは CIFS クライアントからアクセスします。
 2. ログ・ファイルをテキスト・エディターあるいはビューアーで開きます。

FTP ログ・ファイルの最大数の指定

FTP ログ・ファイルの最大数を指定するには、ftpd.log.nfiles オプションを設定します。デフォルトでは、FTP ログ・ファイルの最大数は 6 です。

コマンド `options ftpd.log.nfiles n` を入力します。*n* は、ログ・ファイルの最大数です。詳細情報については、na_options(1) のマニュアル・ページを参照してください。

現行の FTP ログ・ファイルの最大サイズの指定

現行の FTP ログ・ファイル (the /etc/log/ftp.cmd および /etc/log/ftp.xfer ログ・ファイル) の最大サイズを指定するには、`ftpd.log.filesize` オプションを設定します。デフォルトでは、現行の FTP ログ・ファイルの最大サイズは 512 KB です。

コマンド `options ftpd.log.filesize filesize` を入力します。*filesize* は、後に K または k (KB の場合)、あるいは G または g (GB の場合) が付く整数です。詳細情報については、`na_options(1)` のマニュアル・ページを参照してください。

タスクの結果

現行の FTP ログ・ファイルの最大サイズを 1 GB に設定

現行の FTP ログ・ファイルの最大サイズを 1 GB に設定するには、次のコマンドを入力します。

```
options ftpd.log.filesize 1G
```

FTP サーバーが生成する SNMP トラップの表示

FTP サーバーが生成する SNMP トラップを表示するには、ストレージ・システム上で SNMP を開始および構成して、UNIX クライアント上で SNMP トラップを表示します。

FTP サーバーが生成する SNMP トラップ

FTP サーバーはいくつかの SNMP トラップを生成します。

FTP サーバーは、以下のイベントが発生すると SNMP トラップを生成します。

- 同時接続数が `ftpd.max_connections_threshold` に到達した場合。
- 同時接続数が `ftpd.max_connections` に到達した場合。
- FTP デーモン・プロセスがエラーによって停止した場合。

SNMP に関する詳細情報については、「*Network Management Guide*」を参照してください。

ストレージ・システム上の SNMP の開始および構成

ストレージ・システム上で SNMP を開始するには、`snmp` コマンドを使用します。

1. 次のコマンドを入力します。`snmp init 1`
2. 次のコマンドを入力します。`snmp traphost add hostname` ここで *hostname* は、FTP サーバーが生成した SNMP トラップを受信する UNIX クライアントのホスト名です。

次のタスク

ステップ 2 で指定した UNIX クライアントで SNMP トラップを有効に設定する必要があります。

UNIX クライアント上での SNMP トラップの表示

UNIX クライアント上で SNMP トラップを表示するには、`snmptrapd -P` コマンドを入力します。

始める前に

UNIX クライアント上で SNMP トラップが表示可能になる前に、ストレージ・システム上で SNMP を開始して構成する必要があります。

次のコマンドを入力します。`snmptrapd -P`

FTP 統計の表示

FTP 統計を表示するには、`ftp stat` コマンドを入力します。

次のコマンドを入力します。`ftp stat`

タスクの結果

`ftp stat` コマンドは、以下の統計を表示します。

- 現在の FTP 接続の数
- FTP 同時接続の最大数
- FTP 統計がリセットされて以降の FTP 接続の総数

FTP 統計のリセット

FTP 統計をリセットするには、`ftp stat -z` コマンドを入力します。

FTP 接続の最大数の指定

FTP サーバーが許可する FTP 接続の最大数を指定するには、`ftpd.max_connections` オプションを使用します。デフォルトでは、FTP 接続の最大数は 500 です。

コマンド `options ftpd.max_connections n` を入力します。*n* は、FTP サーバーが許可する FTP 接続の最大数です。

タスクの結果

`ftpd.max_connections` オプションを現行の FTP 接続の数より小さい値に設定すると、FTP サーバーは接続数が新しく設定した最大値を下回るまで、新規の接続を拒否します。FTP サーバーは既存の FTP 接続を中断しません。

アクティブ/アクティブ構成では、ストレージ・システムがテークオーバー・モードの場合は FTP 接続の最大数が自動的に 2 倍になります。

FTP 接続しきい値の設定

FTP 接続数がどの程度まで最大数に近づくと、FTP サーバーがエントリーをシステム・ログに追加し、(オプションで) SNMP トラップを起動するかを指定するには、`ftpd.max_connections_threshold` オプションを設定します。デフォルトでは、このオプションは 0 (off) です。

コマンド `options ftpd.max_connections_threshold n` を入力します。*n* は、`ftpd.max_connections` の値のパーセンテージ (0 から 99) です。

FTP 操作のための TCP ウィンドウ・サイズの指定

FTP 操作のための TCP ウィンドウ・サイズを指定するには、`ftpd.tcp_window_size` オプションを使用します。デフォルトでは、FTP 操作のための TCP ウィンドウ・サイズは 28,960 です。

始める前に

FTP 操作のための TCP ウィンドウ・サイズは、ネットワーク構成が変更を要求したときのみ変更します。変更は、FTP パフォーマンスに大きく影響します。

コマンド `options ftpd.tcp_window_size n` を入力します。*n* は、FTP 操作のための新規の TCP ウィンドウ・サイズです。

FTP ファイル・ロックの有効化あるいは無効化

FTP サーバーが転送中のファイルをユーザーが編集することを防ぐために、FTP ファイル・ロックを有効にすることができます。あるいは、FTP ファイル・ロックを無効にすることができます。デフォルトでは、FTP ファイル・ロックは無効に設定されています。

以下を実施したい場合、	以下を実行してください。
削除および名前変更について FTP ファイル・ロックを有効にする	次のコマンドを入力します。options ftpd.locking delete
削除、名前変更、および書き込みについて FTP ファイル・ロックを有効にする	次のコマンドを入力します。options ftpd.locking write
FTP ファイル・ロックを無効にする	次のコマンドを入力します。options ftpd.locking none

FTP アイドルのタイムアウト値の指定

FTP アイドルのタイムアウト値 (FTP サーバーが終了させる前に、FTP 接続がアイドル状態であることができる時間)を指定するには、`ftpd.idle_timeout` オプションを設定します。デフォルトでは、FTP アイドルのタイムアウト値は 900 秒です。

コマンド `options ftpd.idle_timeout n s | m | h` を入力します。*n* は、新規のタイムアウト値です。文字 *s*、*m*、あるいは *h* を付加して、*n* がそれぞれ秒、分、あるいは時間を表すことを指定します。

FTP over IPv6

Data ONTAP 7.3.1 から、ご使用のストレージ・システム上のファイルに FTP クライアントが IPv6 上でアクセスすることを許可することができます。

FTP over IPv6 の有効化あるいは無効化

FTP over IPv6 を、`ftpd.ipv6.enable` オプションを `on` あるいは `off` に設定することで、それぞれ有効あるいは無効にすることができます。

始める前に

`ip.v6.enable` オプションを `on` に設定することで、ストレージ・システム の IPv6 を有効にする必要があります。ストレージ・システム での IPv6 の有効化に関する詳細情報については、「*Data ONTAP Network Management Guide*」を参照してください。

このタスクについて

- FTP over IPv6 を有効にし、次に `ip.v6.enable` オプションを `off` に設定することで IPv6 をストレージ・システム で無効にする場合、FTP over IPv6 は自動的に無効になります。
- IPv6 グローバル・オプションの再始動の後、FTP over IPv6 を再始動する必要はありません。FTP over IPv6 がストレージ・システム 上で有効になっている場合、そして IPv6 グローバル・オプションを無効化および再有効化した場合、FTP over IPv6 ソケットが IPv6 アドレスを `listen` するために自動的に作成されます。

以下を実施したい場合、	以下を実行してください。
FTP over IPv6 を有効にする	次のコマンドを入力します。options <code>ftpd.ipv6.enable on</code>
FTP over IPv6 を無効にする	次のコマンドを入力します。options <code>ftpd.ipv6.enable off</code>

FTP over IPv4 および IPv6 接続のリスト表示

`ftpstat` コマンドを使用して、すべての FTP over IPv4 および IPv6 接続を表示することができます。

次のコマンドを入力します。ftp stat 例:

```
ftp stat
Current connections: 0
Maximum concurrent connections: 0
Total connections: 0

Current IPv4 connections: 0
Maximum IPv4 concurrent connections: 0
Total IPv4 connections: 0

Current IPv6 connections: 0
Maximum IPv6 concurrent connections: 0
Total IPv6 connections: 0
```

HTTP を使用したファイル・アクセス

HTTP クライアント (Web ブラウザー) がご使用のストレージ・システム上のファイルにアクセスすることを許可するために、Data ONTAP の組み込み Hypertext Transfer Protocol (HTTP) サーバーを有効にして構成することができます。あるいは、サード・パーティーの HTTP サーバーを購入し、ご使用のストレージ・システムに接続する方法も可能です。

Data ONTAP の組み込み HTTP サーバーの管理

Data ONTAP の組み込み HTTP サーバーの管理は、いくつかのタスクを含みます。

Data ONTAP の組み込み HTTP サーバーの有効化あるいは無効化

Data ONTAP の組み込み HTTP サーバーを有効あるいは無効にするには、`httpd.enable` オプションをそれぞれ `on` あるいは `off` に設定します。デフォルトでは、このオプションは `off` です。

以下を実施したい場合、	以下を実行してください。
HTTP を有効にする	次のコマンドを入力します。options <code>httpd.enable on</code>
HTTP を無効にする	次のコマンドを入力します。options <code>httpd.enable off</code>

次のタスク

HTTP ライセンスを購入すると、Web ブラウザーは HTTP サーバーのルート・ディレクトリーにあるすべてのファイルにアクセスできます。そうでない場合は、Web ブラウザーはマニュアル・ページおよび FilerView にのみアクセスできます。

HTTP 全探索チェックのバイパスの有効化あるいは無効化

`httpd.bypass_traverse_checking` オプションを `on` あるいは `off` に設定することで、HTTP 全探索チェックのバイパスをそれぞれ有効あるいは無効にすることができます。デフォルトでは、このオプションは `off` に設定されています。

このタスクについて

`httpd.bypass_traverse_checking` オプションが `off` に設定されている場合、ユーザーが HTTP プロトコルを使用してファイルにアクセスしようと試みると、Data ONTAP はファイルへのパスにあるすべてのディレクトリーについて (実行) 権限の全探索をチェックします。いずれかの中間ディレクトリーに X (実行権限) がない場合は、Data ONTAP はファイルへのアクセスを拒否します。 `httpd.bypass_traverse_checking` オプションが `on` に設定されている場合、ユーザーがファイルへのアクセスを試みたときに、Data ONTAP はファイルへのアクセスを認可するか拒否するかを判別するのに、中間ディレクトリーのアクセス権の全探索チェックを行いません。

HTTP 全探索チェックのバイパスを有効あるいは無効にします。

以下を実施したい場合、	以下を実行してください。
HTTP 全探索チェックのバイパスを有効にする	次のコマンドを入力します。options httpd.bypass_traverse_checking on
HTTP 全探索チェックのバイパスを無効にする	次のコマンドを入力します。options httpd.bypass_traverse_checking off

Data ONTAP の組み込み HTTP サーバーのルート・ディレクトリーの指定

Data ONTAP の組み込み HTTP サーバーのルート・ディレクトリー (HTTP クライアントがアクセス可能なすべてのファイルを含むディレクトリー) を指定するには、httpd.rootdir オプションを設定します。

コマンド options httpd.rootdir *directory* を入力します。*directory* は、HTTP サーバーのルート・ディレクトリーへの絶対パスです。

HTTP サーバーのルート・ディレクトリーを /vol0/home/users/pages に設定

HTTP サーバーのルート・ディレクトリーを /vol0/home/users/pages に設定するには、次のコマンドを入力します。options httpd.rootdir /vol0/home/users/pages

Data ONTAP の組み込み HTTP サーバーのログ・ファイルの最大サイズの指定

Data ONTAP の組み込み HTTP サーバーのログ・ファイル (/etc/log/httpd.log) の最大サイズを指定するには、ftpd.log.filesize オプションを設定します。(このオプションは、ftp.cmd、ftp.xfer、および httpd.log ファイルを含む /etc/log ディレクトリー内の HTTP および FTP ログ・ファイルの最大サイズを指定します。) デフォルトでは、このオプションは 512 キロバイトに設定されています。

次のコマンドを入力します。options ftpd.log.filesize *bytes* ここで、*bytes* は HTTP サーバーのログ・ファイルの新規の最大サイズです。

Data ONTAP の組み込み HTTP サーバーのテスト

Data ONTAP の組み込み HTTP サーバーが動作していることを確認するには、HTML ファイルを HTTP サーバーのルート・ディレクトリーにコピーして、Web ブラウザーからそのファイルにアクセスします。HTTP サーバーのルート・ディレクトリー (あるいは HTTP サーバーのルート・ディレクトリーのサブディレクトリー) に Web ブラウザーから直接アクセスすることができます。

1. HTML ファイルを HTTP サーバーのルート・ディレクトリーにコピーします。
2. 別のシステム上で稼働している Web ブラウザーから、HTTP サーバーのルート・ディレクトリーにコピーしたファイルにアクセスします。URL は `http://www.hostname.com/myfile.html` で、ここで *hostname* はストレージ・システムのホスト名で、*myfile.html* は、HTTP サーバーのルート・ディレクトリーにコピーしたファイルの名前です。ファイルの内容を参照することができます。

3. 任意で、HTTP サーバーのルート・ディレクトリー (あるいは HTTP サーバーのルート・ディレクトリーのサブディレクトリー) に、別のクライアントで稼働している Web ブラウザーから直接アクセスします。URL は `http://www.hostname.com` で、ここで `hostname` は、ストレージ・システムのホスト名です。

HTTP サーバーは、指定したディレクトリー内で以下の順番で以下のファイルを探します。

- a. `index.html`
- b. `default.htm`
- c. `index.htm`
- d. `default.html`

これらのファイルが存在しない場合、ストレージ・システムは自動的にそのディレクトリーをリスト表示する HTML バージョンのディレクトリーを生成する (`httpd.autoindex.enable` オプションが `on` の場合) か、あるいは「403」(forbidden) エラー・コードで応答します (`httpd.autoindex.enable` オプションが `off` の場合)。`httpd.autoindex.enable` オプションに関する詳細情報については、`na_options(1)` のマニュアル・ページを参照してください。

Data ONTAP の組み込み HTTP サーバーが MIME コンテンツ・タイプをファイル名拡張子にマッピングする方法の指定

Data ONTAP の組み込み HTTP サーバーがどのように Multipurpose Internet Mail Extensions (MIME) コンテンツ・タイプをファイル名拡張子にマッピングするかを指定するには、`/etc/httpd.mimetypes` ファイルを作成あるいは編集します。`/etc/httpd.mimetypes` ファイルが存在しない場合、HTTP サーバーは `/etc/httpd.mimetypes.sample` ファイルにあるマッピングを使用します。詳細情報については、`na_httpd.mimetypes(5)` のマニュアル・ページを参照してください。

このタスクについて

Web ブラウザーは、MIME コンテンツ・タイプによってファイルを解釈します。例えば、ファイルの MIME コンテンツ・タイプがイメージ・タイプの場合、Web ブラウザーはグラフィックス・プログラムを使用したイメージとしてファイルをレンダリングします。

注: MIME に関する詳細情報については、RFC 1521 を参照してください。

`/etc/httpd.mimetypes` ファイルのエントリーは、以下のフォーマットです。

```
# An optional comment. (任意指定のコメント。)
```

```
suffix Content-Type
```

suffix は、MIME コンテンツ・タイプをマッピングしたいファイル名拡張子で、*Content-Type* は MIME コンテンツ・タイプです。MIME コンテンツ・タイプの最初のフィールドは、ファイルに含まれている一般的なデータのタイプを表し、2 番目のフィールドはデータが保管されている特定のフォーマットを示すデータ・サブタイプを表しています。

シャープ (#) の後のテキストは、コメントです。ファイル名の接尾部は、大/小文字の区別はありません。

/image/pict MIME コンテンツ・タイプの .pct および .pict ファイル名拡張子を持つファイルへのマッピング

/image/pict MIME コンテンツ・タイプを .pct および .pict ファイル名拡張子を持つファイルにマッピングするには、以下のエントリーを /etc/httpd.mimetypes ファイルに追加します。

```
# My clients' browsers can now use (クライアントのブラウザーは現在使用可能です)
```

```
# PICT graphics files. (PICT グラフィックス・ファイル)
```

```
pct image/pict
```

```
pict image/pict
```

ここで、適切に構成されていると Web ブラウザーはグラフィックス・プログラムをヘルパー・アプリケーションとして開始し、ユーザーがグラフィックス・ファイルとして .pct および .pict ファイルを表示することを許可します。

Data ONTAP の組み込み HTTP サーバーが HTTP 要求を変換する方法の指定

Data ONTAP の組み込み HTTP サーバーが HTTP 要求に対してどのように応答するかを指定するには、/etc/httpd.translations 構成ファイルに map、redirect、pass、あるいは fail 変換規則を追加します。

Data ONTAP の組み込み HTTP サーバー変換ファイルの処理方法

Data ONTAP の組み込み HTTP サーバーは、/etc/httpd.translations ファイルにリストされている順に規則を処理し、規則は URL がテンプレートに一致した場合に適用されます。最初のマッチング成功の後、HTTP サーバーは残りの規則の処理を停止します。

アスタリスク (*) をワイルドカード文字として、マッピングの *template* と *result* フィールド、および /etc/httpd.translations ファイルに追加する転送規則および受け渡し規則で 사용할 ことができます。

template フィールドでは、ワイルドカード文字はスラッシュ (/) 文字を含めて 0 以上の文字とマッチングします。

result フィールドでは、ワイルドカード文字はテンプレート・フィールドでのマッチングから展開されたテキストを表します。結果フィールドでは、テンプレート・フィールドでワイルドカード文字を使用した場合のみ、ワイルドカード文字を含めることができます。

複数のワイルドカード文字を使用する場合は、結果フィールドの最初のワイルドカード文字がテンプレート・フィールドの最初のワイルドカード文字に、結果フィールドの 2 番目のワイルドカード文字がテンプレート・フィールドの 2 番目のワイルドカード文字に、というように一致します。

マッピング規則の追加

HTTP サーバーが URL を別の場所にマッピングするように指定するために、`/etc/httpd.translations` ファイルにマッピング規則を追加することができます。

1. `/etc/httpd.translations` ファイルをテキスト・エディターで開きます。
2. 次の規則を追加します。`map template result` ここで *template* は、別の場所にマッピングしたい URL のコンポーネント (例えば、`/image-bin/graphics/`) で、*result* は新しい場所です。
3. このファイルを保存します。

タスクの結果

/image-bin コンポーネントを含む URL の `/usr/local/http/images` ディレクトリーへのマッピング

`/image-bin` コンポーネントを含む URL を `/usr/local/http/images` ディレクトリーにマッピングするには、`/etc/httpd.translations` ファイルに次のマッピング規則を追加します。`map /image-bin/* /usr/local/http/images/*`

リダイレクト規則の追加

HTTP サーバーが特定のコンポーネントを含む URL を新しい場所にリダイレクトするように指定するために、`/etc/httpd.translations` ファイルにリダイレクト規則を追加することができます。

1. `/etc/httpd.translations` ファイルをテキスト・エディターで開きます。
2. 次のエントリーを追加します。`redirect template result` ここで *template* は、リダイレクトする URL のコンポーネントで、*result* は新しい場所です。

注: リダイレクト規則の結果フィールドを、`http://` およびホスト名で始まる完全な URL として指定する必要があります。

3. このファイルを保存します。

cgi-host と命名された HTTP サーバーへの CGI 要求のリダイレクト

コモン・ゲートウェイ・インターフェース (CGI) 要求を、`cgi-host` と命名された HTTP サーバーにリダイレクトするには、`/etc/httpd.translations` ファイルに以下のエントリーを追加します。`redirect /cgi-bin/* http://cgi-host/*`

パス規則の追加

HTTP サーバーが他の規則を無視して、規則をそのまま処理するように指定するには、`/etc/httpd.translations` ファイルにパス・エントリーを追加します。

1. `/etc/httpd.translations` ファイルをテキスト・エディターで開きます。
2. 次のエントリーを追加します。`pass template [result]`

template は URL のコンポーネントです。

result は、HTTP サーバーが URL をリダイレクトする任意指定の場所です。

3. このファイルを保存します。

/image-bin を含む URL に関する要求をそのまま処理する

/image-bin を含む URL に関する要求をそのまま処理するには、`/etc/httpd.translations` ファイルに以下のエントリーを追加します。pass /image-bin/*

失敗規則の追加

特定のコンポーネントを含む URL へのアクセスを HTTP サーバーが拒否するように指定するために、`/etc/httpd.translations` ファイルに失敗規則を追加します。

1. `/etc/httpd.translations` ファイルをテキスト・エディターで開きます。
2. 次のエントリーを追加します。fail *template* ここで *template* は、HTTP サーバーがアクセスを拒否すべき URL コンポーネントです。
3. このファイルを保存します。

/user/forbidden ディレクトリーへのアクセスの拒否

/user/forbidden ディレクトリーへのアクセスを拒否するには、次のエントリーを `/etc/httpd.translations` ファイルに追加します。fail /usr/forbidden/*

MIME コンテンツ・タイプ値の構成

例えば、`/etc/httpd.mimetypes` ファイルの情報によって .gif、.html、あるいは .mpg のようなファイル名の接尾部をマッピングすることで、受信したクライアントからの要求への各応答で適切な MIME コンテンツ・タイプ値を送信するように、ストレージ・システムを構成することができます。

このタスクについて

ファイルの MIME (Multipurpose Internet Mail Extensions) コンテンツ・タイプ値は、クライアント上のブラウザでどのようにファイルを解釈するかを示します。例えば、MIME コンテンツ・タイプ値が、ファイルは画像ファイルであることを示し、クライアントが適切に構成されている場合、ブラウザはグラフィックス・プログラムを使用して画像を表示することができます。

MIME に関する詳細情報については、RFC 1521 を参照してください。

`/etc/httpd.mimetypes` ファイルのエントリーを編集します。

エントリーは以下のフォーマットです。

An optional comment. (任意指定のコメント。)

suffix Content-Type

記号が先頭にある行はコメントです。ファイル名の接尾部は、大/小文字の区別はありません。

例

以下はサンプルのエントリーです。

```
# My clients' browsers can now use
```

```
# PICT graphics files.
```


pct	image/pict
-----	------------

pict	image/pict
------	------------

サンプルのエントリーでは、名前の最後が .pct あるいは .pict のファイルは、image/pict の MIME コンテンツ・タイプ値にマッピングされています。コンテンツ・タイプ値の最初のフィールドは、ファイルに含まれている一般的なデータのタイプを表し、2 番目のフィールドはデータが保管されている特定のフォーマットを示すデータ・サブタイプを表しています。クライアント上のブラウザがヘルパー・アプリケーションとしてグラフィックス・プログラムを開始するように構成されている場合、ユーザーは file.pict と命名されたファイルをグラフィックス・ファイルとしてクライアント上で表示することができます。

Data ONTAP の組み込み HTTP サーバーのセキュリティの維持

アクセスを制限するための HTTP オプションの使用、HTTP 仮想ファイアウォールの使用、ユーザー認証による Web ページの保護、HTTP TRACE 方式のサポートの無効化、および Data ONTAP がアイドル状態の HTTP 接続をオープンのまま保持する期間を指定することによって、Data ONTAP の組み込み HTTP サーバーのセキュリティを維持することができます。

アクセス制限のための HTTP オプションの使用

HTTP オプションは、特定のホストおよび特定のインターフェースからの HTTP サービスへのアクセスを制限します。

このタスクについて

HTTP アクセスを制限するために、以下のオプションが使用可能です。

- httpd.access — HTTP サービスへのアクセスを制限します。
- httpd.admin.access — HTTP (FilerView) 経由でのストレージ・システム管理へのアクセスを制限します。

1 つ以上のホスト上、あるいはネットワーク・インターフェース上のアクセスを制限することができます。これらのオプションに関する詳細情報については、options(1) のマニュアル・ページを参照してください。

注: httpd.admin.access オプションが設定されると、trusted.hosts オプションは HTTP 管理に関しては無視されます。

- httpd.method.trace.enable — HTTP TRACE メソッドのサポートを有効あるいは無効にします。

デフォルトでは、このオプションは off です。HTTP TRACE メソッドによって、HTTP クライアントはデバッグ目的で要求の相手が何を受信しているかを見ることができます。(詳細情報については、RFC 2616 を参照してください。) ただし、アタッカーはクロスドメイン・ブラウザが持つサード・パーティーのドメインからの重要ヘッダー情報を読み取るためのぜい弱性と連動して、HTTP TRACE メソッドを利用することができます。詳細情報については、

<http://www.cert.org/> にある United States Computer Emergency Readiness Team (US-CERT) の Vulnerability Notes Database で Vulnerability Note 867593 を検索してください。

- `httpd.admin.top-page.authentication` — 最上位の FilerView 管理 Web ページがユーザー認証のためのプロンプトを出すかを指定します。

デフォルトでは、このオプションは `on` です。

例

以下の例では、ホスト `Host1` のみが、インターフェース `e3` から ストレージ・システム `Filer1` 上の HTTP サービスにアクセスすることを許可されます。

```
Filer1> options httpd.access host=Host1 AND if=e3
```

以下の例では、ホスト `Host1` がストレージ・システム `Filer1` への FilerView アクセスを拒否されます。

```
Filer1> options httpd.admin.access host!=Host1
```

HTTP 仮想ファイアウォールの使用

HTTP 仮想ファイアウォールは、HTTP 要求が到着するサブネット・インターフェースからの HTTP アクセスを制限することで、ストレージ・システム上にセキュリティを提供します。

このタスクについて

サブネット・インターフェースを信頼できないとマーク付けすることで、HTTP アクセスを制限します。信頼できないサブネット・インターフェースは、ストレージ・システムに対して読み取り専用の HTTP アクセスのみを提供します。デフォルトでは、サブネット・インターフェースは信頼されています。

以下のすべての条件に当てはまる場合は、サブネット・インターフェースを信頼できないとマーク付けします。

- HTTP 要求をそのインターフェース上で保守するつもりである。
- HTTP 以外のプロトコルからの要求を許可したくない。
- そのインターフェースからのストレージ・システムへのアクセスを、読み取り専用アクセスに制限したい

次のコマンドを入力します。 `ifconfig interface_name [trusted | untrusted]` `interface_name` は、「信頼できる」または「信頼できない」と設定する特定のインターフェースです。 `untrusted` を使用して HTTP アクセスを制限し、あるいは `trusted` を使用して完全 HTTP アクセスを許可します。

例

この例では、`f0` インターフェースを信頼できないとマーク付けします。

```
ifconfig f0 untrusted
```

Web ページの保護

許可されていないユーザーによる Web ページへのアクセスを防ぐことで、HTTP アクセスを制限し、それによって Web ページを保護することができます。この方法では、指定されたユーザーあるいはグループのみが Web ページを含むディレクトリーにアクセスできます。

このタスクについて

Data ONTAP は、HTTP アクセスのために以下の 2 つの認証方式を提供します。

- Basic
- NTLM

使用する認証方式を `/etc/httpd.access` ファイルで指定します。両方の認証方式はストレージ・システム上で共存することができますが、HTTP サブツリーのディレクトリーごとに 1 つの認証方式のみを指定することができます。

基本 (Basic) 認証:

以下の 3 つの構成ファイルを使用して HTTP サービスに関する認証をセットアップします。`/etc/httpd.access`、`/etc/httpd.passwd`、および `/etc/httpd.group`

`/etc/httpd.access` ファイルは、認証の方式、アクセスを制限したいディレクトリー、およびそれらのディレクトリーにアクセスを許可されたユーザーとグループのリストを含みます。

`/etc/httpd.passwd` ファイルは、`/etc/httpd.access` ファイルで指定されたユーザーが `/etc/httpd.access` ファイルで指定されたディレクトリーにアクセス権を取得するために使用する、暗号化された書式のパスワードを含みます。`/etc/httpd.passwd` ファイルは `/etc/passwd` ファイルが使用しているものと同じ書式を使用します。

`/etc/httpd.group` ファイルは、`/etc/httpd.access` ファイルで指定されたディレクトリーへのアクセスを許可された各グループのメンバーのグループおよびユーザー ID を含みます。`/etc/httpd.group` ファイルは `/etc/group` ファイルが使用しているものと同じ書式を使用します。

NTLM 認証:

ディレクトリーの基本認証の代わりに Windows ドメイン認証を使用することができます。Data ONTAP は、Web ページを含めたディレクトリーへのユーザーのアクセス認証にドメイン・コントローラー (DC) を使用します。

ドメイン・コントローラーにユーザー認証をさせたいディレクトリーを `/etc/httpd.access` ファイルで指定する必要があります。

NTLM 認証がセットアップされたディレクトリーへアクセスするユーザーは、ユーザー名と一緒にドメインを指定する必要があります。ドメインが指定されていない場合、ストレージ・システムのドメインはデフォルトと仮定されます。ユーザーは、以下のフォーマットのいずれかでドメインを指定することができます。

- `user_name@domain_name`
- `domain_name¥user_name`

注: HTTP アクセスに関して NTLM 認証を使用するには、ご使用のストレージ・システム上で CIFS が稼働している必要があります。

/etc/http.passwd および /etc/http.group ファイルの情報を維持するような、ユーザー管理の集中化を行う必要はありません。また、ブラウザとして Internet Explorer (IE) を使用する場合、NTLM 認証は、ユーザー名とパスワードが非暗号化テキストで送信されないため、よりセキュアなユーザー認証方式です。

注: Netscape ブラウザーは、ユーザー名とパスワードを非暗号化テキストで送信するため、NTLM のセキュリティの利点が提供されません。

/etc/httpd.access ファイルの編集:

/etc/httpd.access ファイルは、各ディレクトリーへのアクセス権および各ディレクトリーの出現を管理するオプションを含んでいます。

このタスクについて

ストレージ・システムは、以下のオプションをサポートします。

- **Directory** — 保護したいディレクトリーを指定します。 **directory** オプションは他のすべてのオプションを囲んでいます。
- **AuthName** — ユーザーがディレクトリーへのアクセスを試みるときに、ブラウザのパスワード・ダイアログ・ボックスでディレクトリー名の代わりに表示されるディレクトリーのエイリアスを指定します。
- **require user** — ディレクトリーにアクセス可能なユーザーを指定します。
- **require group** — ディレクトリーにアクセス可能なグループを指定します。

注: オプション **require user** および **require group** のみが、基本認証で要求されます。

/etc/httpd.access ファイルにある各ディレクトリーのオプション情報は、以下のフォーマットで提供されます。

```
<Directory directory>
```

```
option ...
```

```
</Directory>
```

directory は、許可されたアクセスを有効にしたい特定のディレクトリー・ツリー名です。

1. 編集のために、/etc/httpd.access ファイルを開きます。
2. 次の行で、保護したいディレクトリー・ツリーを指定します。<Directory *directory*> ここで、*directory* は保護したい特定のディレクトリー・ツリー名です。
3. /etc/httpd.passwd および /etc/httpd.group ファイルを使用して基本認証を構成している場合、次の行でディレクトリーのエイリアスを指定します。AuthName *title_phrase* ここで *title_phrase* は、ユーザーがディレクトリーへのアクセスを試みるときに、ブラウザのパスワード・ダイアログ・ボックスでディレクトリ

一名の代わりに表示されるように指定する文字列です。この名前はスペースを含むことができます。例: AuthName Secured Area

4. あるいは、NTLM 認証を構成している場合は、以下を示すように正確に指定します。AuthName Windows(tm) Authentication
5. 次の行で、ディレクトリーにアクセス可能なユーザーを指定します。require user user_id[, user_id, ...] ここで user_id は、ディレクトリーへのアクセス権を持つ各ユーザーの固有のユーザー ID です。
6. 次の行で、ディレクトリーにアクセス可能なグループを指定します。require group group_id[, group_id, ...] ここで group_id は、ディレクトリーへのアクセス権を持つ各グループの固有のグループ ID です。
7. 次の行を使用して、オプションあるいは指定されたディレクトリーのオプションのリストを終了します。</Directory>
8. このファイルを保存します。

例

以下の例は、ストレージ・システム上で基本認証あるいは NTLM 認証のいずれかを指定するための /etc/httpd.access ファイル内の、複数の Directory オプションの用途について示しています。

```
<Directory /vol/vol0/web1>
AuthName Windows(tm) Authentication
</Directory>
<Directory /vol/vol0/web2>
AuthName Web2 directory
require user test1
require group testg1
</Directory>
<Directory /vol/vol0/web3>
AuthName Windows(tm) Authentication
</Directory>
<Directory /vol/vol0/web4>
AuthName Web4 directory
require user test2
</Directory>
```

この例では、web1 および web3 は NTLM 認証を使用し、web2 および web4 は基本認証を使用しています。web2 へのアクセスは、ユーザー test1 およびグループ testg1 のメンバーに制限されており、web4 へのアクセスは、ユーザー test2 に制限されています。

httpd.passwd ファイルの作成および編集:

/etc/httpd.passwd ファイルは、/etc/httpd.access ファイルにリストされているユーザーの暗号化されたパスワードを含んでいます。このファイルは、ユーザーの認証に基本認証を使用している場合にのみ必要です。

このタスクについて

ユーザーの認証にユーザー名およびパスワード方式を使用している HTTP サーバーがある場合、そのサーバーからユーザー ID および暗号化されたパスワードをコピーすることができます。アクセス権を与えたくなくユーザーを削除するために、/etc/httpd.passwd ファイルを編集する必要があります。

HTTP サーバーが使用可能ではない場合、UNIX サーバーから既存の `/etc/passwd` ファイルをコピーして、ストレージ・システム上で `/etc/httpd.passwd` ファイルとして保存することが可能です。

1. `/etc/httpd.passwd` ファイルを開きます。
2. `/etc/httpd.access` ファイルで指定したディレクトリーへのアクセス権を与えたくないユーザーの、ユーザー ID および暗号化されたパスワードを削除します。
3. 編集を保存します。

httpd.group ファイルの作成および編集:

`/etc/httpd.group` ファイルは、グループ名およびそのグループに属するユーザーを含んでいます。このファイルは、ユーザーの認証に基本認証を使用している場合にのみ必要です。

このタスクについて

ユーザーのグループを認証する HTTP サーバーがある場合、そのサーバーからグループ名およびユーザー ID をコピーすることができます。アクセス権を与えたくなくグループを削除するために、`/etc/httpd.group` ファイルを編集する必要があります。

HTTP サーバーが使用可能ではない場合、UNIX サーバーから既存の `/etc/group` ファイルをコピーして、ストレージ・システム上で `/etc/httpd.group` ファイルとして保存することが可能です。

1. `/etc/httpd.group` ファイルで、次の行を編集します。 `group_id:user_id [, user_id, ...]` リストは、同様のリストを持つサーバーからコピーされます。
2. グループおよびユーザーを追加または削除します。グループおよびユーザーの情報は、次のフォーマットでリストされています。 `group_id: user_id[user_id ...]` ここで `group_id` は、グループ名で、`user_id` はそのグループに属する各ユーザーの名前です。
3. このファイルを保存します。

仮想ホスティングの使用

仮想ホスティングによって、1 つの物理インターフェースのみを使用して複数の IP アドレスをホストするようにストレージ・システムを構成することができます。例えば、インターネット・プロバイダーがいくつかの Web サイト をホストしたいが物理インターフェースが 1 つしかないような場合に、仮想ホスティングが便利です。

このタスクについて

仮想ホスティングが有効にされると、HTTP サーバーは仮想ホストに属する HTTP ページを含むディレクトリーを検出するために、HTTP 着信要求によってポイントされた IP アドレスを使用します。

仮想ホスティングを有効にするには、以下のタスクを実行します。

- `/etc/httpd.hostprefixes` ファイルを編集して仮想ホスティングをセットアップする
- `ifconfig` コマンドを使用して、仮想ホストのアドレスを `vh` インターフェースにマッピングする

Data ONTAP は HTTP 要求をサブディレクトリーおよび `/etc/httpd.hostprefixes` ファイルにリストされたホストあるいはアドレスに転送します。

vh インターフェースに関する詳細情報については、`ifconfig(1)` のマニュアル・ページを参照してください。

1. 編集のために、`/etc/httpd.hostprefixes` ファイルを開きます。
2. サブディレクトリーと、ホストあるいはアドレスのエントリーを次のフォーマットで入力します。prefix [*host_name_or_address ...*]

パラメーター	説明
<i>prefix</i>	HTTP サーバーのルート・ディレクトリーにあるサブディレクトリーで、options <code>httpd.rootdir</code> コマンドで定義されます。
<i>host_name_or_address</i>	HTTP のホスト名あるいは IP アドレス。複数のホスト名および IP アドレスを持つことができます。

3. 編集を保存します。

仮想ホスティングの例

次のエントリーを `/etc/httpd.hostprefixes` ファイルに追加すると仮定します。

```
/customer 192.225.37.102
```

```
/customer www.customer.com
```

HTTP サーバーがその仮想ホストの IP アドレス の 1 つ、192.225.37.102 に向かう HTTP 要求を受信すると、その IP アドレスは仮想ホストのルート・ディレクトリーである `/customer` ディレクトリーを `/etc/httpd.hostprefixes` ファイルから選択するために使用されます。HTTP 1.1 ホストを使用した HTTP 要求では、`www.customer.com` を指定するヘッダーは `/customer` ディレクトリーに誘導されます。いずれの場合も、要求側は `/customer` ディレクトリーの外部のファイルを取得することはできません。

仮想ホスト・アドレスのマッピング:

仮想ホスティングをサポートするために、仮想ホスト・アドレスを vh インターフェースにマッピングすることができます。

新規の仮想ホスト IP アドレスのマッピングを追加するには、コマンド `ifconfig vh -wins [alias | -alias] address` を入力します。*address* は、追加あるいは削除したい IP アドレスです。*alias* を使用して、仮想ホスト・アドレスをマッピングします。`-alias` を使用して、仮想ホスト・アドレスのマッピングを削除します。

タスクの結果

注: 多くの連続するアドレスを使用して仮想サブネットを作成する必要がある場合は、IP アドレスはサブネット・アドレスを使用することができます。

vh インターフェースは、IP 別名アドレスではなく、仮想ホスト・アドレスをネットワーク・インターフェースに追加していることを示します。

Data ONTAP の組み込み HTTP サーバーに関する統計の表示

httpstat コマンドを使用して、Data ONTAP の組み込み HTTP サーバーに関する 5 つのタイプの統計を表示することができます。

このタスクについて

これらの 5 つのタイプは以下のとおりです。

- 要求
- 詳細
- エラー
- サービス
- タイムアウト

次のコマンドを入力します。httpstat [-dersta]

オプション	表示される情報
-d	詳細な統計
-e	エラー統計
-r	要求統計
-s	サービス統計
-t	タイムアウト統計
-a	すべての HTTP 統計

引数を使用しない場合、httpstat は HTTP 要求統計を表示します。

httpstat コマンドに関する詳細情報については、httpstat(1) のマニュアル・ページを参照してください。

要求統計

要求統計を指示すると、Data ONTAP は以下の統計を表示します。

統計のラベル	説明
Accept	ストレージ・システムによって承認された新規接続の数
Reuse	既存の接続で受信した新規要求の数
Response	送信された応答数
InBytes	すべての着信要求について受信したバイト数
OutBytes	すべての HTTP ヘッダーを含む (ただし、サブレットによって生成されたデータは含まない) 送信されたバイト数

詳細な統計

詳細な統計を指示すると、Data ONTAP は以下の統計を表示します。

統計のラベル	説明
Get	受信したファイルに関する要求の数

統計のラベル	説明
Head	受信したファイル情報に関する要求の数
Redirect	別のファイルにリダイレクトされた要求の数
NotMod	クライアント（ブラウザ）が、要求されたファイルは変更されていないと伝えられた回数
Post	受信した POST 要求の数
Put	受信した PUT 要求の数
Servlet	受信したサーブレット要求の数

エラー統計

エラー統計を指示すると、Data ONTAP は以下の統計を表示します。

統計のラベル	説明
エラー	リターンされた HTTP プロトコルのエラー応答の数
BadReq	受信した未認識な要求の数
LogDiscard	ログがフルになったために廃棄されたログ項目の数
UnAuth	権限の欠如により拒否された要求の数
RcvErr	入力ソケットでのエラーにより異常終了した要求の数

サービス統計

サービス統計を指示すると、Data ONTAP は以下の統計を表示します。

統計のラベル	説明
Open	現在オープンされている接続数
Peak	過去に達した接続の最大数
Waits	現在接続が承認済みで接続構成を待っている数

タイムアウト統計

タイムアウト統計を指示すると、Data ONTAP は以下の統計を表示します。

統計のラベル	説明
Pending	ネットワーク接続が開始した後、ストレージ・システムヘデータを送信する前にレクラメーション処理された接続構成の数
Active	ネットワーク接続が開始した後、一部の要求が送信されたが完全に要求が到達する前にレクラメーション処理された接続構成の数
Idle	要求を完了した後、開いた接続が別の要求を受信する前にレクラメーション処理された接続の数

Data ONTAP の組み込み HTTP サーバーに関する統計のリセット

httpstat -z コマンドを使用して、Data ONTAP の組み込み HTTP サーバーに関する統計をリセットすることができます。

次のコマンドを入力します。httpstat -z[derta]

オプション	リセットする統計
-zd	詳細な統計
-ze	エラー統計
-zr	要求統計
-zt	タイムアウト統計
-za	サービス統計を除くすべての HTTP 統計

注: サービス統計をリセットすることはできません。

httpstat コマンドに関する詳細情報については、httpstat(1) のマニュアル・ページを参照してください。

Data ONTAP の組み込み HTTP サーバーに関する接続情報の表示

Data ONTAP の組み込み HTTP サーバーによって確立された各接続に関して、/etc/log/httpd.log ファイルにある多くのタイプの情報を表示することができます。

1. ストレージ・システムのデフォルト・ディレクトリー上の /etc/log ディレクトリーに、NFS あるいは CIFS クライアントからアクセスします。
2. テキスト・ビューアーあるいはテキスト・エディターを使用して、httpd.log ファイルを開いて表示します。
3. 見終われば、ログ・ファイルをクローズします。

タスクの結果

Data ONTAP は、以下のタイプの情報を表示します。

- HTTP クライアントの IP アドレス
- 要求を送信している許可されたユーザーの名前 (ページが保護されている場合、Data ONTAP は /etc/httpd.passwd ファイルから取得した許可された名前をリストします。ページが保護されていない場合は、名前の代わりにダッシュが表示されます)
- 接続の時間 — グリニッジ標準時 (GMT) dd/mm/yy:hh:mm:ss フォーマット
- 接続ホストからの要求ライン (例えば、get /my_company.html)
- サーバーによって返された (HTTP 1.0 の規格で定義されている) 状況コード
- ストレージ・システムによる応答で送信された総バイト数 (MIME ヘッダーは含みません)

例

```
192.9.77.2 - - [26/Aug/2003:16:45:50] "GET /top.html" 200 1189
192.9.77.2 - - [26/Aug/2003:16:45:50] "GET /header.html" 200 531
192.7.15.6 - - [26/Aug/2003:16:45:51] "GET /logo.gif" 200 1763
198.9.200.2 - - [26/Aug/2003:16:45:57] "GET /task/top.html" 200 334
192.9.20.5 authuser [26/Aug/2003:16:45:57] "GET /task/head.html" 200 519
```

/etc/log/httpd.log ファイルのフォーマットの変更

/etc/log/httpd.log ファイルのデフォルトのフォーマットは、HTTP クライアントの IP アドレスおよびアクセスの HTTP パスを表示しますが、どの仮想ホストがアクセスされているかは表示しません。httpd.log.format オプションを設定することで /etc/log/httpd.log ファイルのフォーマットを変更し、仮想ホストによる HTTP メッセージを区別することが可能です。

次のコマンドを入力します。options httpd.log.format alt1 ログのフォーマットの設定を戻すには、このオプションを alt1 からデフォルト値 common に変更します。

サード・パーティー HTTP サーバーの購入およびストレージ・システムへの接続

Data ONTAP 組み込み HTTP サーバーの制限を、サード・パーティー HTTP サーバーを購入してストレージ・システムに接続することで解決することができます。

このタスクについて

Data ONTAP 組み込み HTTP サーバーには以下の制限があります。

- セキュア HTTP (HTTPS) のサポートはありません。
 - 複数の HTTP ルート・ディレクトリーのサポートはありません。
 - スクリプトのサポートはありません (HTTP は、ファイル・サービス提供のみサポートします)。
 - 大規模な数の小さなファイルで大規模な数のファイル操作がある場合に、スケラビリティおよびパフォーマンス上の問題があります。
1. サード・パーティー HTTP サーバーを購入します。
 2. サード・パーティー HTTP サーバーを、NFS プロトコルを使用してストレージ・システムに接続します。 詳細情報については、サード・パーティー HTTP サーバーに付属の資料を参照してください。

HTTP over IPv6 および HTTPS over IPv6

Data ONTAP 7.3.1 から、ご使用のストレージ・システム上のファイルに HTTP クライアントが IPv6 上でアクセスすることを許可することができます。また、ストレージ・システムへのセキュアな管理のアクセスのために HTTPS を有効にすることもできます。

ご使用のストレージ・システムからのファイル・アクセスにのみ、HTTP over IPv6 が使用できます。FilerView およびセキュア FilerView には、IPv6 での HTTP を使用することはできません。

注: FilerView およびセキュア FilerView は、IPv6 上では使用できません。

HTTP over IPv6 および HTTPS over IPv6の有効化あるいは無効化

HTTP over IPv6 および HTTPS over IPv6を、`httpd.ipv6.enable` オプションを `on` あるいは `off` に設定することで、それぞれ有効あるいは無効にすることができます。

始める前に

`ip.v6.enable` オプションを `on` に設定することで、ストレージ・システムの IPv6 を有効にする必要があります。ストレージ・システムでの IPv6 の有効化に関する詳細情報については、「*Data ONTAP Network Management Guide*」を参照してください。

このタスクについて

- HTTP および HTTPS over IPv6 を有効にしており、次に `ip.v6.enable` オプションを `off` に設定することで IPv6 をストレージ・システムで無効にする場合、HTTP および HTTPS over IPv6 は自動的に無効になります。
- IPv6 グローバル・オプションの再始動の後、HTTP および HTTPS over IPv6 を再始動する必要はありません。HTTP および HTTPS over IPv6 がストレージ・システム上で有効になっている場合、そして IPv6 グローバル・オプションを無効化して再有効化した場合、HTTP および HTTPS over IPv6 ソケットが IPv6 アドレスを `listen` するために自動的に作成されます。

以下を実施したい場合、	以下を実行してください。
HTTP および HTTPS over IPv6 を有効にする	次のコマンドを入力します。options <code>httpd.ipv6.enable on</code>
HTTP および HTTPS over IPv6 を無効にする	次のコマンドを入力します。options <code>httpd.ipv6.enable off</code>

HTTP over IPv4 および IPv6 接続のリスト表示

`httpstat` コマンドを使用して、すべての HTTP over IPv4 および IPv6 接続を表示することができます。また、`httpstat` コマンドと一緒に `-i` オプションを使用することで、HTTP over IPv4 接続のみ、あるいは HTTP over IPv6 接続のみを表示することができます。

以下を実施したい場合、	以下を実行してください。
すべての HTTP 接続をリストする	次のコマンドを入力します。httpstat 例: <pre> httpstat Requests Accept Reuse Response InBytes OutBytes Total Stats: 73 0 39 27620 7247 IPv4 Stats: 43 0 10 9460 9 IPv6 Stats: 30 0 29 18160 7238 </pre>
HTTP over IPv4 接続をリストする	次のコマンドを入力します。httpstat -i ipv4 例: <pre> httpstat -i ipv4 Requests Accept Reuse Response InBytes OutBytes 43 0 10 9460 9 </pre>
HTTP over IPv6 接続をリストする	次のコマンドを入力します。httpstat -i ipv6 例: <pre> httpstat -i ipv6 Requests Accept Reuse Response InBytes OutBytes 30 0 29 18160 7238 </pre>

WebDAV を使用したファイル・アクセス

ユーザーに WebDAV で相互運用が可能な共同アプリケーションの使用を許可するために、WebDAV (Web ベースの分散オーサリングおよびバージョン管理) プロトコルを既存の HTTP サービスに追加することができます。あるいは、サード・パーティーの WebDAV サーバーを購入し、ご使用のストレージ・システムに接続する方法も可能です。

注: HTTP に関するライセンスを購入した場合に限り、ご使用のストレージ・システムで HTTP の拡張機能として WebDAV プロトコルをご使用になれます。Data ONTAP の今後のバージョンでは、WebDAV を HTTP と使用するための WebDAV ライセンス・キーの使用が必要になる可能性があります。

WebDAV の理解

WebDAV プロトコルは、ユーザーが必要とするサポートを行うと同時に、広範囲に相互接続するために配布された Web オーサリング・ツールを有効にする HTTP 拡張機能を定義します。WebDAV によって、HTTP ディレクトリーの作成が可能になります。

WebDAV プロトコルは、広範囲な共同アプリケーションを通じて、リモート・ソフトウェア開発チームのサポートを提供します。WebDAV は HTTP の成功を活用し、広範囲なストレージ・リポジトリの標準的なアクセス・レイヤーとしての役割を果たします。HTTP は読み取りアクセスを提供し、WebDAV は書き込みアクセスを提供します。

このプロトコルの主要機能は以下を含みます。

- ロック。長期間に及ぶ排他的書き込みロックおよび共有書き込みロックによって、2 人以上のコラボレーターが最初のマージ変更なしで同じリソースに書き込みを行うことを防ぎます。インターネット規模の堅固なコラボレーションを達成するために、ネットワーク接続が任意におよびスケラビリティのために切断されている場合、それぞれのオープン接続がサーバー・リソースを消費するため、DAV ロックの継続期間は個々のネットワーク接続から独立しています。
- プロパティー。XML プロパティーは、Web リソースの作成者のリストのような、任意のメタデータをストレージに提供します。これらのプロパティーは、DAV プロトコルを使用して、効率的に設定、削除、および取り出しを行うことができます。DASL (DAV Searching and Locating) プロトコルは、XML プロパティーの値に基づく Web リソースの検索を提供します。
- 名前空間操作。リソースは、Web の進化に伴ってコピーあるいは移動が必要な場合があるため、DAV はコピーおよび移動操作をサポートします。ファイル・システム・ディレクトリーと同様の集合を作成およびリストすることが可能です。
- HTTP 機能のサポート。Data ONTAP の WebDAV 実装環境は、リダイレクト規則、認証、およびアクセス制限などの HTTP 構成設定をサポートします。WebDAV を使用するには、HTTP サービスを有効にし、構成している必要があります。

- CIFS 機能のサポート。Data ONTAP の WebDAV 実装環境は、有効な CIFS および HTTP ライセンスを持っていて、WebDAV を有効にしている場合、CIFS ホーム・ディレクトリーをサポートします。

Data ONTAP の組み込み WebDAV サーバーの管理

Data ONTAP の組み込み WebDAV サーバーの管理は、WebDAV プロトコルを有効あるいは無効にするタスク、および WebDAV クライアントをホーム・ディレクトリーにポイントするタスクを含みます。

Data ONTAP の組み込み WebDAV サーバーの有効化あるいは無効化

Data ONTAP の組み込み WebDAV サーバーを有効あるいは無効にするには、`webdav.enable` オプションをそれぞれ `on` あるいは `off` に設定します。デフォルトでは、このオプションは `off` です。

始める前に

Data ONTAP の組み込み WebDAV サーバーを有効にする前に、Data ONTAP の組み込み HTTP サーバーを有効にする必要があります。Data ONTAP の組み込み WebDAV サーバーは、リダイレクト規則、認証、およびアクセス制限のようなご使用の HTTP 構成の設定をサポートします。

さらに、Data ONTAP の組み込み WebDAV サーバーは、有効な CIFS ライセンスを持ち、CIFS ホーム・ディレクトリーを有効に設定して構成している場合、CIFS ホーム・ディレクトリーをサポートします。

以下を実施したい場合、	以下を実行してください。
WebDAV を有効にする	次のコマンドを入力します。 <code>options webdav.enable on</code>
WebDAV を無効にする	次のコマンドを入力します。 <code>options webdav.enable off</code>

WebDAV クライアントのホーム・ディレクトリーへのポインティング

WebDAV クライアントのナビゲーション・フィールドに入力する URL にチルド (~) 文字を追加することで、WebDAV クライアントをホーム・ディレクトリーにポイントすることができます。

WebDAV クライアントのナビゲーション (あるいはデフォルト・ディレクトリー) フィールドで、次の構文で URL を入力します。`http://host[:port]/~`
`host` は、ストレージ・システムのホスト名あるいは IP アドレスです。
`port` は、ストレージ・システムへのアクセスに使用したいポートです。チルド (~) 文字は、ユーザーのホーム・ディレクトリーを示します。

タスクの結果

有効な WebDAV ホーム・ディレクトリー URL の例

`http://eng_filer.lab.company.com/~`

`http://10.120.83.104:80/~`

サード・パーティー WebDAV サーバーの購入およびストレージ・システムへの接続

Data ONTAP 組み込み WebDAV サーバーの制限を、サード・パーティー WebDAV サーバーを購入してストレージ・システムに接続することで解決することができます。

このタスクについて

Data ONTAP 組み込み WebDAV サーバーには以下の制限があります。

- 2 バイト Unicode 文字を含む値のみをサポートします。Data ONTAP は、大容量の Unicode 文字を正確に記録しません。
 - WebDAV のコア・プロトコルのみをサポートします。Data ONTAP は、WebDAV のセカンダリー・プロトコルをサポートしません。
 - 仮想 IP アドレスのためのホーム・ディレクトリー機能をサポートしません。ホストとして仮想 IP アドレスを指定する URL は解決されません。
1. サード・パーティー WebDAV サーバーを購入します。
 2. サード・パーティー WebDAV サーバーを、NFS プロトコル経由でご使用のストレージ・システムに接続します。詳細情報については、サード・パーティー WebDAV サーバーに付属の資料を参照してください。

システム・メモリーによる CIFS リソースの制限

ストレージ・システム・モデルによる CIFS リソースの制限は、システム・メモリーに基づく上限です。ただし、これらの制限は理論上の制限です。実用上の制限は、理論上の制限より低くなり、またご使用の環境でのシステム構成により変化します。

注: 以下の表にある数量を、ご使用のシステムのストレージ・リソースのサイズ変更には使用しないでください。ご使用のストレージ・システムがこれらのカテゴリで十分なリソースを得ることができない場合は、技術サポートにお問い合わせください。

ストレージ・システムは、CIFS リソースについて最大値を割り当てるために、6 GB を超えるシステム・メモリーを使用することはありません。例えば、32 GB のメモリーを持つストレージ・システムは、8 GB のメモリーを持つストレージ・システムより非常に良いパフォーマンスを示しますが、CIFS リソースにおける制限はどちらも同じです。この方法で CIFS リソースの制限を計算することにより、ストレージ容量および他のシステム・リソースのスケーリングにシステム・メモリーを確実に使用できるようにします。

ストレージ・システム上のすべての vFiler ユニットは、CIFS リソースの同一の有限なプールを利用しています。そのため、ストレージ・システム上のすべての vFiler ユニットによって消費されているこれらのリソースの合計は、システムのリソースの制限を超えることはできません。

N7000 シリーズ のストレージ・システムの制限

以下の表は、N7000 シリーズ シリーズのストレージ・システムのアクセス制限を示しています。

ストレージ・システム・メモリーによる CIFS 制限	8 GB N7600	32 GB N7800
接続の最大数	96,000	96,000
共有の最大数	192,000	192,000
共有接続の最大数	384,000	384,000
オープン・ファイルの最大数	1,920,000	1,920,000
ロック・ファイルの最大数	2,116,608	2,116,608
ロックの最大数	4,233,216	4,233,216

N5000 シリーズ および N6000 シリーズ のストレージ・システムの制限

以下の表は、N5000 シリーズ および N6000 シリーズ のストレージ・システムのアクセス制限を示しています。

ストレージ・システム・メモリーによる CIFS 制限	2 GB N5200	4 GB N5300、N5500、および N6040	8 GB N5600 および N6060
接続の最大数	32,000	64,000	96,000
共有の最大数	64,000	128,000	192,000
共有接続の最大数	128,000	256,000	384,000
オープン・ファイルの最大数	640,000	1,280,000	1,920,000
ロック・ファイルの最大数	705,536	1,411,072	2,116,608
ロックの最大数	1,411,072	2,822,144	4,233,216

イベント・ログおよび監査ポリシーのマッピング

イベント・ログおよび監査のグループ・ポリシーは、Data ONTAP によって Windows システムとは別に適用される場合があります。

グループ・ポリシー・オブジェクト (GPO) のサポートがストレージ・システムで有効になっている場合、Data ONTAP はすべての関連する GPO を処理および適用します。関連するほとんどのグループ・ポリシー設定は、Data ONTAP および Windows システムが稼働しているストレージ・システム上で一様に適用されます。

しかし、イベント・ログと監査 (ローカル・ポリシー) の 2 つのタイプのポリシーは、根本的なロギングおよび監査のテクノロジーが異なるため、ストレージ・システム上で別に適用されます。イベント・ログおよび監査の GPO は、対応する Data ONTAP オプションのマッピングおよび設定によってストレージ・システムに適用されます。これらのオプションのマッピングの効果は、イベント・ログおよび監査ポリシーの設定と似ていますが、同一ではありません。

以下の表は、対応する GPO が適用された際に設定された Data ONTAP オプションを示しています。これらのオプションに関する詳細については、options(1) のマニュアル・ページを参照してください。

イベント・ログ・マッピング値

以下の表の各行について、右の列は左の列のイベント・ログ・ポリシー (および設定と該当する場合は例) が適用された際に設定される Data ONTAP オプションを示しています。

ポリシー名	設定	Data ONTAP オプション
最大セキュリティ・ログ・サイズ	n/a	cifs.audit.logsize
セキュリティ・ログの保存方式	日単位でイベントを上書き (例: 7 日)	cifs.audit.autosave.file.extension timestamp cifs.audit.autosave.file.limit 0 cifs.audit.autosave.onsize.threshold 100 cifs.audit.autosave.onsize.enable on cifs.audit.autosave.ontime.interval 7d cifs.audit.autosave.ontime.enable on cifs.audit.saveas /etc/log/adtlog.evt cifs.audit.enable on

ポリシー名	設定	Data ONTAP オプション
セキュリティ・ログの保存方式	必要に応じてイベントを上書き	cifs.audit.autosave.file.extension timestamp cifs.audit.autosave.file.limit 1 cifs.audit.autosave.onsize.threshold 100 cifs.audit.autosave.onsize.enable on cifs.audit.autosave.ontime.enable off cifs.audit.saveas /etc/log/adtlog.evt cifs.audit.enable on
セキュリティ・ログの保存方式	イベントを上書きしない (手動でログを消去する)	cifs.audit.autosave.file.extension timestamp cifs.audit.autosave.file.limit 0 cifs.audit.autosave.onsize.threshold 100 cifs.audit.autosave.onsize.enable on cifs.audit.autosave.ontime.enable off cifs.audit.saveas /etc/log/adtlog.evt cifs.audit.enable on

監査マッピング値

以下の表の各行について、右の列は左の列の監査ポリシー（および設定と該当する場合は例）が適用された際に設定される Data ONTAP オプションを示しています。

ポリシー名	設定	Data ONTAP オプション
監査アカウント・ログオン・イベント 監査ログオン・イベント	両方のポリシーが定義されているが、どちらも監査計画が設定されていない。	cifs.audit.logon_events.enable off
監査アカウント・ログオン・イベント 監査ログオン・イベント	両方のポリシーが定義されており、監査計画が「Success」、 「Failure」、あるいは 「Success & Failure」に設定されている。	cifs.audit.enable on cifs.audit.logon_events.enable on
監査ディレクトリー・サービス・アクセス 監査オブジェクト・アクセス	両方のポリシーが定義されているが、どちらも監査計画が設定されていない。	cifs.audit.file_access_events.enable off

ポリシー名	設定	Data ONTAP オプション
監査ディレクトリ・サービス・アクセス 監査オブジェクト・アクセス	両方のポリシーが定義されており、監査計画が「Success」、 「Failure」、あるいは「Success & Failure」に設定されている。	cifs.audit.enable on cifs.audit.file_access_events.enable on
他の監査ポリシーおよび設定	マッピング・アクションは実行されません。	

用語集

以下の用語は、ファイル・アクセスおよびプロトコル管理のコンテキストで頻繁に使用されます。

アクティブ/アクティブ構成 一方が動作していない場合に他方がそれを検出し、そのような場合に障害が発生しているシステムのデータを供給することができるように接続されたストレージ・システムのペア。Data ONTAP の資料およびその他の情報リソースでは、アクティブ/アクティブ構成はクラスターあるいはアクティブ/アクティブ・ペアとして参照される場合もあります。

アダプター・カード 拡張スロットに差し込む SCSI カード、ネットワーク・カード、ホット・スワップ・アダプター・カード、シリアル・アダプター・カード、あるいは VGA アダプター。

アドレス解決 LAN あるいは WAN の宛先のアドレスに対応するメディア・アクセス制御 (MAC) アドレスを決定する手順。

アプライアンス 明確に定義された機能を実行し、インストールおよび操作が容易なデバイス。

イーサネット・アダプター イーサネット・インターフェース・カード。

エージェント 状況および診断情報を収集し、NMS に転送する Data ONTAP プロセス。

エミュレートされたストレージ・システム テークオーバー・ストレージ・システムによってホスティングされた障害のあるストレージ・システムのソフトウェア・コピー。エミュレートされたストレージ・システムは、ユーザーあるいは管理者には障害のあるストレージ・システムの機能バージョンのように見えます。例えば、エミュレートされたストレージ・システムは、障害のあるストレージ・システムと同じ名前を持ちます。

拡張カード ストレージ・システムの拡張スロットに差し込む SCSI カード、NVRAM カード、ネットワーク・カード、ホット・スワップ・カード、あるいはコンソール・カード。

拡張スロット 拡張カードを挿入する、システム・ボード上のスロット。

管理ホスト システム・セットアップ中にストレージ・システムを管理するために指定したクライアント。セットアップ・プログラムは、自動的にこのクライアントからの Telnet および rsh 接続を承認するように、このクライアントに / および /home ディレクトリーをマウントするアクセス権を与えるように、そして AutoSupport E メール・メッセージを送信するメール・ホストとしてこのクライアントを使用するように、ストレージ・システムを構成します。セットアップ・プログラムを実行した後はいつでも、管理ホストと同じように他のクライアントでもストレージ・システムが動作するように構成することができます。

ギブバック 仮想ストレージ・システムから障害のあるストレージ・システムに識別情報が戻り、その結果、正常の運用に戻ることに。テークオーバーの逆。

共有 ネットワーク・ユーザーに使用可能で、CIFS クライアントのドライブ名にマッピングすることができる、ストレージ・システムのディレクトリーあるいはディレクトリー構造。

クライアント ストレージ・システム上のファイルを共有するコンピューター。

クラスター・モニター アクティブ/アクティブ構成のストレージ・システムの関係を `cf` コマンドで管理するソフトウェア。

クラスター相互接続 アクティブ/アクティブ構成の 2 つのストレージ・システムを接続し、両方のシステムが稼働しているときにハートビートおよび WAFL ログ情報を伝送するためのケーブルおよびアダプター。

グループ ストレージ・システムの `/etc/group` ファイルで定義されたユーザーのグループ。

コピー・オン・ライト 過剰なディスク・スペースを消費することなくスナップショット・コピーを作成する技法。

コミュニティ ストレージ・システム・エージェントと通信するために SNMP マネージャーによってパスワードとして使用される名前。

コンソール ストレージ・システムのシリアル・ポートに接続され、ストレージ・システムの操作を監視および管理するための端末。

システム・ボード ストレージ・システムの CPU、拡張バス・スロット、およびシステム・メモリーを含んだプリント回路ボード。

障害のあるストレージ・システム 動作が停止している物理ストレージ・システム。ギブバックが成功するまで、障害のあるストレージ・システムのままです。

シリアル・アダプター いくつかのストレージ・システム・モデルでコンソールとして端末を接続するための拡張カード。

シリアル・コンソール ストレージ・システムのシリアル・ポートに接続された ASCII あるいは ANSI 端末。ストレージ・システム運用の監視および管理に使用します。

スナップショット・コピー ファイル内容の複製なしでの予定外のファイル削除や変更から保護するための、ファイル・システム全体のオンラインでの読み取り専用コピー。スナップショット・コピーによって、ユーザーはシステムの使用中にファイルの復元およびテープへのストレージ・システムのバックアップが可能になります。

通常モード アクティブ/アクティブ構成でテークオーバーが発生していないときのストレージ・システムの状態。

ツリー quota quota qtree コマンドで作成されたディレクトリーのディスク使用量を制限するディスク quota のタイプ。指定された UID あるいは GID でのファイルによるディスク使用量の制限である、ユーザーおよびグループ quota とは異なります。

テークオーバー アクティブ/アクティブ構成でのテークオーバー・ストレージ・システムによる、障害が発生したストレージ・システムの識別情報のエミュレーション。ギブバックの反対。

テークオーバー・ストレージ・システム 他方のストレージ・システムが動作を停止した後も運用を続け、障害が発生したストレージ・システム・ディスク・シェルフおよびネットワーク接続へのアクセスを管理する仮想ストレージ・システムを提供するストレージ・システム。テークオーバー・ストレージ・システムは、自身の識別情報を維持し、仮想ストレージ・システムは障害が発生したストレージ・システムの識別情報を維持します。

テークオーバー・モード パートナーを引き継いでいる間の、ストレージ・システムとの対話方式。ストレージ・システムがテークオーバー・モードになる場合は、コンソール・プロンプトが指示します。

低下モード RAID アレイからディスクが欠落したり、あるいは NVRAM カードのバッテリー残量が少ない場合のストレージ・システムの動作モード。

ディスク ID 番号 ストレージ・システムが起動時にディスクを精査し、それぞれのディスクに割り当てた番号。

ディスク・シェルフ ディスク・ドライブを含み、ストレージ・システムに取り付けられているシェルフ。

トラップ SNMP エージェントから SNMP マネージャーに送信される、ストレージ・システムにイベントが発生したことを示す非同期の非送信請求メッセージ。

認証 ストレージ・システムのドメインのためのドメイン・コントローラー、あるいはストレージ・システムそのものによって /etc/passwd ファイルを使用して実行されるセキュリティー手順。

ネットワーク・アダプター イーサネット、FDDI、あるいは非同期伝送モード (ATM) アダプター。

ネットワーク管理ステーション NMS を参照。

パートナー ローカル・ストレージ・システムの視点から、アクティブ/アクティブ構成における他方のストレージ・システム。

パートナー・モード テークオーバー中にコマンド行インターフェースから仮想ストレージ・システムと通信するために使用する方式。

ハートビート システムが運用中であることを示すために、1 つのストレージ・システムから他のストレージ・システムに送信される繰り返し信号。ハートビート情報はディスクにも保管されます。

パニック ストレージ・システムの停止を引き起こす深刻なエラー状況。 Windows システム環境でのソフトウェア異常終了に似た状況。

パリティ・ディスク RAID-4 ディスク・ドライブ・アレイで、パリティ情報が保管されているディスク。障害のあるディスク・ブロック内または障害のあるディスク上のデータを再構成するのに使用します。

ビッグ・エンディアン 最上位ビットまたはバイトが最初にくる、保管および伝送のためのバイナリー・データ・フォーマット。

保守モード ストレージ・システムをシステム・ブート・ディスクからブートするときのオプション。保守モードは、ハードウェアおよび構成のトラブルシューティングに関する特別なコマンドを提供します。

ホット・スペア・ディスク 障害が起こったディスクの代替用に使用できる、ストレージ・システムにインストールされているディスク。ディスク障害の前は、ホット・スペア・ディスクは RAID ディスク・アレイの一部ではありません。

ホット・スワップ ストレージ・システムが稼働中に、ディスクを追加、取り外し、あるいは交換するプロセス。

ホット・スワップ・アダプター ファイル・システム活動への最小限の割り込みで、ハード・ディスクの追加、または取り外しを可能にする拡張カード。

ボリューム ファイル・システム。

マジック・ディレクトリー 名前によってアクセス可能だが、ディレクトリー・リストには表示されないディレクトリー。スナップショット・コピー・ディレクトリーは、マウント・ポイントにあるものあるいは共有のルートにあるものを除いて、マジック・ディレクトリーです。

メール・ホスト 特定のストレージ・システム・イベントが発生したときに、技術サポートに自動的に E メールを送信するのに関与するクライアント・ホスト。

メールボックス・ディスク システムのアクティブ/アクティブ構成状況の情報を保管するのに使用される、それぞれのストレージ・システムが所有するディスクのセットの 1 つ。ストレージ・システムが運用を停止すると、テークオーバー・システムは仮想ストレージ・システムの構築においてメールボックス・ディスク内の情報を使用します。メールボックス・ディスクは、ファイル・システム・ディスクとしても使用されます。

ローカル・ストレージ・システム ユーザーがログインしているストレージ・システム。

ワークグループ 表示および共有のためにグループ化された Windows NT あるいは Windows for Workgroups が稼働しているコンピューターの集合。

割り込みスイッチ デバッグを目的に使用する、いくつかのストレージ・システムのフロント・パネルにあるスイッチ。

ACL アクセス制御リスト (Access control list)。ユーザーあるいはグループの、各共有へのアクセス権を含むリスト。

ATM 非同期伝送モード (Asynchronous Transfer Mode)。セル切り替え機能と多重化機能を結合して、信頼できる効率的なネットワーク・サービスを提供するネットワーク・テクノロジー。ATM は、ワークステーションやルーターなどのデバイスとネットワークの間のインターフェースを提供します。

AutoSupport 潜在的なストレージ・システムの問題がある場合に、お客様のサイトから技術サポートあるいは他の指定した E メール 受信者に E メール・メッセージを起動するためのストレージ・システム・デーモン。

CIFS 共通インターネット・ファイル・システム (Common Internet File System)。ネットワーク用 PC 用のプロトコル。

FDDI アダプター 光ファイバー分散データ・インターフェース (FDDI) のインターフェース・カード。

FDDI ファイバー 光ファイバー・ケーブルをサポートする FDDI アダプター。

FDDI-TP 対より線ケーブルをサポートする FDDI アダプター。

FPolicy ファイル・タイプのようなファイル・プロパティに基づくアクセス許可をコントロールする能力を提供する、Data ONTAP の所有ファイル・ポリシー機能。

GID グループ ID。

inode ストレージ・システム上、および UNIX ファイル・システムのファイルに関する情報を含んだデータ構造。

LAN エミュレーション (LANE) 基本的なネットワーク・トポロジとして ATM を使用してエミュレートされた LAN を作成するアーキテクチャー、プロトコル、およびサービス。LANE によって、ATM 接続された終端システムは、他の LAN ベースのシステムと通信可能になります。

MIB 管理情報ベース (Management Information Base)。エージェントが NMS に転送する情報を記載した ASCII ファイル。

MIME Multipurpose Internet Mail Extensions。インターネット・メッセージ本体のフォーマットを指定および記述するためのメカニズムを定義した規格。MIME コンテンツ・タイプのヘッダーを含む HTTP 応答は、HTTP クライアントが受信したデータにとって適切なアプリケーションを開始することを許可します。

MultiStore ネットワーク上で複数のストレージ・システムとして現れるように、単一のストレージ・システムのストレージおよびネットワーク・リソースをパーティションで区切ることを可能にする、オプションのストレージ・システム・ソフトウェア製品。

NDMP Network Data Management Protocol。ストレージ・システムがバックアップ・アプリケーションと通信することを許可し、複数のテープ・バックアップ装置のロボット装置をコントロールする機能を提供するプロトコル。

NMS ネットワーク管理ステーション。ストレージ・システムに関する状況および診断情報を処理するための、サード・パーティーのネットワーク管理アプリケーション (SNMP マネージャー) を使用するネットワークのホスト。

NULL ユーザー リモート・データにアクセスするためにアプリケーションが使用する Windows NT マシンのアカウント。

NVRAM カード ストレージ・システムの NVRAM キャッシュを含んだアダプター・カード。

NVRAM キャッシュ 着信書き込みデータおよび NFS 要求を記録するために使用する、ストレージ・システム内の不揮発性 (Nonvolatile) RAM。システム・パフォーマンスを向上させ、ストレージ・システムあるいは電源の障害の場合のデータのロスを防ぎます。

NVRAM ミラー パートナーのストレージ・システム上に保持された、ストレージ・システム NVRAM (不揮発性ランダム・アクセス・メモリー) の内容を同期的に更新したコピー。

PCI Peripheral Component Interconnect。新しいストレージ・システム・モデルで使われているバス・アーキテクチャー。

pcnfsd PC がストレージ・システムのファイル・システムをマウントすることを許可するストレージ・システム・デーモン。対応する PC クライアント・ソフトウェアは、PC-NFS と呼ばれます。

PDC 1 次ドメイン・コントローラー (Primary Domain Controller)。ドメインのプライマリー認証サーバーになるように交渉された、あるいはそのように割り当てられたドメイン・コントローラー。

POST パワーオン自己診断テスト (Power-on self-tests)。電源をオンにした後、ストレージ・システムによって実行されるテスト。

PVC パーマネント・バーチャル・サーキット (Permanent Virtual Circuit)。通常は手動セットアップで前もって定義された、静的ルートによるリンク。

qtree 特別な属性を持った仮想サブボリュームとして活動するボリュームのルートの特別なサブディレクトリー。

RAID 新磁気ディスク制御機構 (Redundant array of independent disks)。アレイ内のすべてのディスクの内容に基づくパリティ情報を計算することで、ディスク障害から保護する技法。ストレージ・システムは、すべてのパリティ情報を単一のディスクに保管する RAID レベル 4 を使用しています。

RAID ディスク修正 システムが RAID グループの各ディスクを読み取って、他のディスク領域にデータを再書き込みすることでメディア・エラーを修正することを試みる処理。

SCSI ID SCSI チェーン上のディスク・ドライブの番号 (0 から 6)。

SCSI アダプター SCSI ディスク・ドライブおよび磁気テープ・ドライブをサポートする拡張カード。

SCSI アドレス ディスクの SCSI アダプター番号およびディスクの SCSI ID で構成されているディスクのフル・アドレス (例えば 9a.1)。

SID セキュリティー ID。

SVC スイッチド・バーチャル・サーキット (Switched Virtual Circuit)。信号方式によって確立された接続。ユーザーは呼び出しが開始されたときにエンドポイントを定義します。

UID ユーザー ID。

Unicode 16 ビット文字セット規格。非営利コンソーシアムの Unicode Inc. によって設計され保守されています。

VCI 仮想チャネル識別子 (Virtual Channel Identifier)。セルが移動する仮想チャネルを識別する ATM セル・ヘッダー内の 16 ビット・フィールドによって定義される固有の数値タグ。

vFiler ユニット ネットワーク上で複数のストレージ・システムとして現れるように、単一のストレージ・システムのストレージおよびネットワーク・リソースをパーティションで区切ることを可能にする、MultiStore を使用して作成した仮想ストレージ・システム

VGA アダプター コンソールとして VGA 端末を接続するための拡張カード。

VPI 仮想パス ID (Virtual Path Identifier)。セルが通るべき仮想パスを示す ATM セル・ヘッダー内の 8 ビット・フィールド。

WAFL Write Anywhere File Layout。WAFL ファイル・システムは、Data ONTAP が稼働しているストレージ・システムで書き込みパフォーマンスを最適化するために設計されました。

WINS Windows インターネット・ネーム・サービス (Windows Internet Name Service)。



Printed in Japan

GC88-8107-00



日本アイ・ビー・エム株式会社
〒106-8711 東京都港区六本木3-2-12