

ホワイトペーパーシリーズ:

Windows Server IoT 2019 for Storage で構築する企業向け最新ファイルサーバー

- 1. インフラ編
- 2. 運用管理編
- 3. 集中管理編
- 4. ハイブリッドクラウド編

2019年6月30日

内容

1	概要	토 2
	1.1	このガイドについて 2
	1.2	ファイルサーバーとしての運用管理について2
	1.3	実施環境について 4
2	標準	きのリモート管理環境の準備
	2.1	リモートデスクトップ接続
	2.2	リモートサーバー管理ツール(RSAT)6
	2.3	サーバーマネージャーによるファイルサーバーの管理11
3	ファ	ァイルサーバーリソースマネージャーの活用14
	3.1	フォルダーの使用法(分類プロパティ)14
	3.2	クォータの管理15
	3.3	ファイルスクリーンの管理18
	3.4	ファイル管理タスク 20
	3.5	記憶域レポートの管理 22
仚	録	外部メールサービスを利用したメール通知の実現

本文書は、株式会社アイ・オー・データ機器(以下、「アイ・オー・データ」とします。)が、アイ・オー・ データの特定の商品に関する機能・性能や技術についての説明を記述した参考資料となります。当該商品の 利用という目的の範囲内で自由に使用、複製をしていただけますが、アイ・オー・データの事前の書面によ る承諾なしに、改変、掲示、転載等の行為は禁止されます。また、あくまで参考資料として提供いたします ので、内容については一切保証を致しかねます。アイ・オー・データサポートセンターでは内容に関するお 問い合わせは承っておりません。以下の内容をご了承いただいた場合のみご利用ください。(1)アイ・オー・ データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるもの ではありません。(2)アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のい かなる保証をするものではありません。(3)アイ・オー・データは、本文書を利用したこと、または利用しな かったことにより生じるいかなる損害についても責任を負うものではありません。(4)アイ・オー・データ は、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報について は、https://www.iodata.jp/をご覧ください。

1 概要

1.1 このガイドについて

このガイドは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z シリーズの NAS デバイスを新規に導入するにあたり、ファイルサーバーとしての運用管理の基本 的な環境の整備、および Windows Server の便利なファイルサーバー機能の活用について解説します。

1.2 ファイルサーバーとしての運用管理について

Windows Server IoT 2019 for Storage のファイルサーバー機能は、Windows Server 2019 とその多く が共通しており、同じ管理操作で運用管理することができます。このガイドでは、Windows またはその他 の OS を実行する管理用端末から、Windows Server IoT 2019 for Storage 搭載の LAN DISK Z をリモー ト管理する環境を準備し、運用管理の一例としてファイルサーバーリソースマネージャーのいくつかの機能 の活用例を示します。

- リモートデスクトップ接続
- リモートサーバー管理ツール(RSAT)
- ファイルサーバーリソースマネージャー

リモートデスクトップ接続

リモートデスクトップ接続は、Windows Server が標準でサポートするリモートデスクトッププロトコル (RDP)を使用するリモート管理環境です。Windows Server は、リモートデスクトップサービス (RDS) の役割を追加することなく、RDP 対応クライアントから管理目的でのリモートでストップ接続をサポート します。RDP 対応クライアントから LAN DISK Z の Windows Server IoT 2019 for Storage のセッショ ンにリモート接続した後は、Windows Server 2019 が備えるのと共通の管理ツール、例えば、[設定] ア プリや [コントロールパネル]、[サーバーマネージャー] やその他の MMC (Microsoft 管理コンソール) ス ナップインの管理ツールを使用して、Windows Server のシステム設定や更新管理、運用管理、ファイルサ ーバー機能の管理が可能です。

Windows クライアントおよびデスクトップエクスペリエンスが有効な Windows Server は、標準の RDP 接続クライアントとして [リモートデスクトップ接続] デスクトップアプリ (mstsc.exe) を備えています。 Windows 8.1 および Windows 10 向けには、ストア (Windows ストア、Microsoft ストア)を通じて [リ モートデスクトップ] アプリが無料提供されており、標準の [リモートデスクトップ接続] デスクトップア プリの代わりにこちらを利用することもできます。

Android や iOS、macOS に対しては、それぞれのデバイスのストアを通じて[Microsoft Remote Desktop] アプリが無料提供されています。Linux についても、FreeRDP (<u>http://www.freerdp.com/</u>) や Remmina (<u>https://remmina.org/</u>) といった無料のオープンソースソフトウェアを RDP 対応クライアントとして利 用できます。この他、このガイドのシリーズの『3.集中管理編』で説明する Windows Admin Center を 導入すると、HTML5 対応ブラウザーだけでリモートデスクトップ接続を行うことができます。

マイクロソフト純正の Android、iOS、macOS 向け RDP 対応クライアント

マイクロソフトは、Windows 以外の Android、iOS、macOS に対しても、 最新の RDP 対応クライアントをそ れぞれのデバイスのストアを通じて 無料提供しています。これらのアプ リを利用すれば、Windows 端末がな くても、AndriodやiPadのタブレッ ト端末から LAN DISK Z をリモート 管理できます。

Android 向け Microsoft Remote Desktop (Google Play)



https://play.google.com/store/apps/details?id=com.microsoft.rdc.android&hl=ja

iOS 向け Microsoft リモートデスクトップ(App Store) https://itunes.apple.com/jp/app/microsoft-remote-desktop/id714464092?mt=8

macOS 向け Microsoft Remote Desktop 10 (Mac App Store) https://itunes.apple.com/us/app/microsoft-remote-desktop/id1295203466?mt=12

リモートサーバー管理ツール(RSAT)

Windows クライアントと Windows Server の標準的な管理ツールは共通であり、Windows 10 のローカ ルの管理ツールを管理対象にリモート接続して管理することができます。 ただし、 Windows Server のサー バーの役割や機能に対応した管理ツールについては、Windows クライアントには標準では搭載されていま せん。

Windows 10(ただし、Home エディションを除く)を利用できる場合は、Windows 10 に「リモートサー バー管理ツール(Remote Server Administrative Tool:RSAT)」を追加することで、[サーバーマネージ ャー]やその他の MMC スナップイン管理ツールを LAN DISK Z の Windows Server IoT 2019 for Storage にリモート接続して管理することができます。

ファイルサーバーリソースマネージャー

ファイルサーバーにファイルサーバーリソースマネージャーの役割サービスを追加すると、クォータの管理、 ファイルスクリーンの管理、ファイル分類管理、ファイル管理タスク、記憶域レポートといった、高度なフ アイルサーバー機能を活用することができます。

ファイルサーバーリソースマネージャーのすべての機能を利用するには、リテール製品またはボリュームラ

イセンス製品の Windows Server で構築した Active Directory ドメイン環境や Windows Server クライ アントアクセスライセンス (CAL)、その他の CAL (Active Directory Rights Management サービスによ る暗号化のための RMS CAL など)、および社内のメールシステム環境が必要です。このガイドでは、ワー クグループ環境でも比較的簡単に導入して利用できる機能について説明します。

1.3 実施環境について

このガイドの内容は、LAN DISK Z (HDL4-Z19SCA-4) と管理用端末を同じネットワークスイッチに接続 した、ワークグループ環境で実施しました。ディスクのパーティションは、既定の構成(OS C: 100GB ミ ラー、データ D: 約 2.4TB RAID-5) は変更せず、管理用端末の環境のセットアップと、ファイルサーバ ーリソースマネージャーの役割サービスのインストールと利用手順について説明します。ファイルサーバー リソースマネージャーの機能の検証は、管理用の Windows 10 端末で兼用して行いました。



リモートデスクトップ接続のリモート管理環境は、サーバーに対する TCP および UDP ポート 3389 の接続 のみで利用できるのに対して、リモートサーバー管理ツール(RSAT)のリモート接続には、Windows Remote Management (TCP ポート 5589)、ファイル共有ポート(TCP ポート 445)、RPC(TCP ポート 135 おび動的ポート)など、広範囲のポートを使用するため、クライアントとサーバーの Windows Defender ファイアウォールや経路上のファイアウォールでブロックされることがあることに留意してください。

2 標準のリモート管理環境の準備

はじめに、リモートデスクトップ接続またはリモートサーバー管理ツール(RSAT)を使用した LAN DISK Zの NAS デバイスのためのリモート管理環境を準備する手順を説明します。

2.1 リモートデスクトップ接続

「1.2 ファイルサーバーとしての運用管理について」で説明したように、RDP 対応クライアントを使用したリモートデスクトップ接続は、Windows クライアントでは標準で利用できますが、Windows 以外の OS

においてもマイクロソフト純正の RDP クライアントアプリや、オープンソースの RDP 対応クライアントア プリを利用できます。そのため、リモートデスクトップ接続を使用する方法は、クライアントの OS を問わ ない、マルチプラットフォーム対応のリモート管理環境と言えます。ここでは、Windows クライアント標 準の [リモートデスクトップ接続] デスクトプアプリ(Mstsc.exe)を使用する方法で説明します。

Windows 10 の場合は、タスクバーの検索ボックス(Cortana)に"**リモートデスクトップ接続**"と入力し、 検索結果に表示された[リモートデスクトップ接続]をクリックします。Windows 10 およびそれ以前の Windows バージョンでは、[ファイル名を指定して実行]や[コマンドプロンプト]などから"**mstsc.exe**" を実行することで、[リモートデスクトップ接続] デスクトプアプリを開始することができます。

	すべて アブリ ドキュメント 設定 ウェブ その他 ▼	フィードバック …
ŵ	最も一致する検索結果	
	設定 (3) ストア (1) リモート デスクトップ 接続 コンビューター(C): HDL-Z19 ユーザー名: 指定われていません 接続時時には責格情報を要求されます。	Windows ゼキュリティ × 資格情報を入力してください これらの資格情報は、HDL-Z19 への接続に使用されます。 HDL-Z19¥administrator
ନ୍ ଞ ∎	 オブションの表示(Q) 	
		h 🗘 🖈 🛃 💼 🚍

[リモートデスクトップ接続] デスクトップアプリのウィンドウが開いたら、[コンピューター] のテキス トボックスに接続先のコンピューター名または IP アドレスを入力し、ローカル管理者の資格情報(既定は <コンピューター名>¥Administrator とそのパスワード)を入力して[接続] をクリックします。

💽 🛅 サーバー マネージャー		HDL-Z19	_ 8 ×	- 🗆 X
ごみ苑 р サーバー マネージャー Windows Admin Center でのサード	ー管理を試してみる	×	• 🕄 🚩 管理(M)	ツ−ル(T) 表示(V) ヘルプ(H)
Windows Admin Center を使用する ス アプリにまとめることができます。これ ンス以外に追加の料金は発生しませ	と、新機能や使い慣れた標能を、1 つのブラウザー ベ はサーバーまたは PC 上で実行でき、Windows ライ† ん。	2		
I-O DA aka.me/WindowsAdminCenter で話 口 今後、このメッセージを表示しない	<u>編8支見る</u> (D)	ル サーバーの構成		
	2 役 3 管 4 サ- 5 乙の 詳細情報(!)	割と機能の追加 理するサーバーの追加 -バー グルーブの作成 Dサーバーをクラウド サービスに接続	₫Ğ	非表示
	役割とサーバーグループ 役割の数2 サーバーグループの数1 サーバ ⑦ ファイル サービスと記憶域 1 ・ 1 ・ 管理状態 イベント サービス パフォーマンス	(-0合計数:1 ・ 印刷サービス 1 ・ 管理状態 イベント サービス パワオーマンス	 ローカルサーバー 管理状態 イベント サービス パワネーマンス 	
🖬 🔎 🛱 🏉 🔚 🧮				へ 記 (か) S 9:05 2019/05/21 レ

LAN DISK Z に初めて接続する場合は MagicalFinder が便利

LAN DISK Z を設置したばかりで、 そのコンピューター名や IP アドレ スが不明の場合は、アイ・オー・デ ータが Windows および macOS 向 けに無料ダウンロード提供してい る MagicalFinder アプリを利用し てください。MagicalFinder アプリ を実行すると、ネットワーク上のデ バイスが検出され、LAN DISK Z の 場合は MagicalFinder アプリから

□ I I I I マ I ファイル ホーム 共有 表示	Ø Magical Finder デバイス情報		-		×
← → ✓ ↑ → mfinder401 名前 Manual Manual		HDL-Z19 WORKGROUP			
MagicalFinder.ini	MACアドレス IPv4 情報	34:76:c5:			
r401	IPアドレス割当設定	DHCP有効			
	IPv4アドレス	192.168.10.42			
	サブネットマスク	255.255.255.0			
	デフォルトゲートウェイ	192.168.10.1			
		リモートデスクトップを開く			
3 個の項目 1 個の項目を選択 512 Ki		し <u>。</u> ネットワーク設定を変更]	
	ヘルプ	端末悟報	バージ	ia)/	

直接にリモートデスクトップ接続を開始できます。

MagicalFinder のダウンロード(Windows および macOS 用) https://www.iodata.jp/lib/product/m/3022.htm

ネットワークレベル認証(NLA)の無効化について(非推奨)

リモートデスクトップ接続のサーバー側の設定では、RDP セッションを確立する前にユーザー認証を 要求するネットワークレベル認証 (NLA) が有効になっていることが推奨されます。NLA が有効になっ ている場合、古いバージョンの RDP 対応クライアントやセキュリティパッチ (例、CVE-2018-0886 の CredSSP の脆弱性) が不足している RDP 対応クライアントからの接続は拒否されます。

セキュリティ上の問題があることを理解した上でセキュリティ設定を一時的に緩和して接続可能にす るには(非推奨)、[設定] アプリの [システム] – [リモートデスクトップ] – [詳細設定] を開き、 [コンピューターの接続にネットワークレベル認証の使用を求める(推奨)] をオフにします。または、 コントロールパネルの [システムとセキュリティ] – [システム] – [リモートアクセスの許可] から [システムのプロパティ] の [リモート] タブを開き、[ネットワークレベル認証でリモートデスクト ップを実行しているコンピューターからのみ接続を許可する(推奨)] をオフにします。

2.2 リモートサーバー管理ツール (RSAT)

管理用端末として Windows 10 コンピューターを利用できる場合は、Windows 10 に「リモートサーバー 管理ツール (RSAT)」を追加することで、Windows Server 標準の管理ツールから直接リモートのサーバー を管理することができます。Windows 10 バージョン 1809(October 2018 Update)以降を実行してい る場合は、[設定] アプリの [アプリ] – [オプション機能の管理]を開き、[+機能の追加] をクリックし て RSAT のツールを個別に追加できます。Windows Server IoT 2019 for Storage を搭載する LAN DISK Z の管理のためには、以下の RSAT ツールを追加すればよいでしょう。

- RSAT: BitLocker ドライブ暗号化管理ユーティリティ
- RSAT : サーバーマネージャー
- RSAT:ファイルサービスツール

Micros	÷	設定				_	×	
WIETOS	命	機能の追加						
	<)	RSAT: サーバー マネージャー サーバー マネージャーには、Windo サーバー マネージャー コンソールおよ	vs Server をリモート び PowerShell ツーJ	6.47 MB で管理するための いと、Windows				
		Server とヘスト ノラクナイス アノラ 構成するためのツールが含まれてし	1 リーエの NIC テー: はす。	インストール				
	<	RSAT: シールドされた VM のツール		16.9 MB			ľ	
	<(RSAT: ストレージ移行サービス管理	ツール	108 KB				
	<	RSAT: データ センター ブリッジング	LLDP ツール	30.7 KB				
	<3	RSAT: ネットワーク コントローラー管	理ツール	172 KB				
-	0 22	に入力して検索	Q Ħ	е н	S 🕹			

Windows 10 バージョン 1803(April 2018 Update)以前の RSAT

「リモートサーバー管理ツール (RSAT)」が Windows 10 のオプションの機能(オンデマンド機能) になったのは Windows 10 バージョン 1809(October 2019 Update)からであり、Windows 10 バ ージョン 1809 には Windows Server 2019 と同じバージョンのツールが含まれます。Windows 10 バージョン 1803(April 2018 Update)以前については、RSAT が以下の URL からダウンロード提供 されています。ダウンロード提供されている RSAT は、Windows Server, version 1803、Windows Server, version 1709、または Windows Server 2016 バージョンに対応するものですが、Windows Server 2019 のリモート管理にも使用できます。ただし、古いバージョンの管理ツールは、Windows Server 2019 からの新機能の管理には対応していない場合があることに注意してください。

Windows 10 用のリモートサーバー管理ツール https://www.microsoft.com/ja-jp/download/details.aspx?id=45520

TrustedHostsの構成(ワークグループ環境のみ)

Active Directory ドメインに参加していないワークグループ環境の場合は、RSAT のツールを使用する Windows クライアント側で Windows リモート管理(WinRM)で NTLM 認証を使用するために TrustedHostsの構成が必要です。それには、Windows クライアントの Windows PowerShell を管理者と して開き、次のいずれかのコマンドラインを実行します。管理対象が複数ある場合は"*"を使用するか、"<

A

管理対象1>,<管理対象2>"のようにカンマで区切って指定してください。

Set-Item WSMan:¥localhost¥Client¥TrustedHosts "<管理対象のサーバー名または IP アドレ ス>" -Force

または

Set-Item WSMan:¥localhost¥Client¥TrustedHosts "*" -Force

この手順は Windows リモート管理(WinRM) に Kerberos 認証が使用される Active Directory ドメイン 環境では不要です。

追加のファイアウォール規則の許可

RSAT のツールおよび Windows 10 にもともと含まれる MMC スナップインのツールをリモート管理に使用するには、サーバー側の [セキュリティが強化された Windows Defender ファイアウォール] で [受信の規則] の許可設定が必要なものがあります。ただしその前に、大前提としてサーバー側の現在のネットワークプロファイルを確認してください。

サーバー側 (サーバーにリモートデスクトップ接続して) で、[設定] アプリの [ネットワークとインターネット] を開き、現在のネットワークプロファイルを確認します。ネットワークプロファイルが [ドメインネットワーク] (Active Directory ドメインに参加している場合) または [プライベートネットワーク] と認識されている場合は問題ありません。[パブリックネットワーク] と認識されている場合は、ほとんどの受信トラフィックがファイアウォールでブロックされる状態であり、リモート管理に影響する場合があります。そのため、[設定] アプリの [ネットワーク] – [イーサネット] を開き、ネットワーク名をクリックして[ネットワークプロファイル] を [パブリック] から [プライベート] に変更してください。

易 HDL-Z19 - リモート デスクトップ接続		퉋 HDL-Z19 - リモート デスクトップ接続		
← 設定	- 0	← 設定		
命 赤-ム	状態	☆ ネットワーク		
設定の検索の	ネットワークの状態	ネットワーク プロファイル		
ネットワークとインターネット 伊 状態	<u>Мумс Геат</u> (Луэр жэн5-2	○ パブリック お使いの PC は、ネットワーク上のその他のデバイスから隠され、ブリンターやファイル の共有に使用できません。		
 マ イーサネット デ ダイヤルアップ 	インターネットに接続されています 制限付きのデータ通信プランをお使いの場合は、このネットワークを 金接続に設定するか、またはその他のプロパティを変更できます。	ブライベート ホームネットワークまたは社内ネットワークなど、信頼するネットワーク向け。お使いの PCは発見可能になり、設定した場合はブリンターやファイルの共有に利用できます。		
% VPN	接続プロパティの変更	ッ。 ファイアウォールとセキュリティ設定の構成		
 プロキシ 	利用できるネットワークの表示 ネットワーク設定の変更	従量制課金接続		

次に、サーバー側で [スタート] メニューの [Windows 管理ツール] から [セキュリティが強化された Windows Defender ファイアウォール] を開き、[受信の規則] の以下の規則またはグループに含まれる規 則を有効化します。

● [COM+ネットワークアクセス (DCOM-受信)]の規則

- [リモートイベントログ管理] グループのすべての規則
- [リモートボリューム管理] グループのすべての規則

なお、[リモートボリューム管理] グループの規則は、接続元の Windows クライアント側の[セキュリティ が強化された Windows Defender ファイアウォール]の[受信の規則]でも有効化する必要があります。



管理対象のサーバーの追加

以上の事前準備ができたら、Windows 10 の [スタート] メニューに追加された [Server Manager] をク リックして [サーバーマネージャー] を開始します。[ダッシュボード] にある [①管理するサーバーの追 加] をクリックすると、[サーバーの追加] ダイアログボックスが開くので、[DNS] タブに切り替え、LAN DISK Z のコンピューター名または IP アドレスを検索し、[▶] をクリックして管理対象に追加して、[OK] をクリックします。



[サーバーマネージャー]は、Windows 10 のサインインに使用している資格情報を使用してリモートのサ ーバーに接続を試みます。しかし、管理対象のサーバーの資格情報(ユーザー名とパスワード)と一致しな いため、アクセスが拒否されて失敗するはずです。そこで、[サーバーマネージャー]の[すべてのサーバ ー]を開き、追加したサーバーを右クリックして[管理に使用する資格情報]をクリックし、サーバーの管 理者の資格情報(<コンピューター名>¥Administrator とそのパスワード)を入力し、[OK]をクリックし ます。

📠 サーバー マネージャー	– 🗆 X
●◎・ サーバー マネージャー・ すべてのサーバー	 ◆ ② ↓ ● 管理(M) ツール(T) 表示(V) ヘルブ(H)
■ ダッシュボード ■ すべてのサーバー すべてのサーバー 合計: 1 フィルター タ サーパー名 IPv4 アドレス 管理状態	
HDL-Z19 オンライン - アクセスオ 役割と機能の追加 サーバーの再起動 コンピューターの管理 リモート デスクトップ接続 Windows PowerShell NIC チーミングの構成 ビビーニングの構成 管理に使用する資格情報 イペン 受新の情報に更新 コピー アバークー アバークー ア サーバー名 ID 単一パー名 ID 単一パー名 ID	Windows セキュリティ × ユーザーアカウントとパスワードの入力 選択したサーバーに対するユーザー権利を持つアカウントの名前とパスワードを入力してください。 例: user、user@example.contoso.com、または domain¥user name。 ユーザー名とパスワードを空白にすると、キャッシュされた資格情報が削除されます。 HDL-Z19¥administrator ●●●● □ このアカウントを記憶する OK キャンセル

以上の設定により、アクセス拒否のエラーが解消され、[サーバーマネージャー] による管理や、[サーバー マネージャー] から起動する [コンピューターの管理] や [Windows PowerShell]、その他の操作を使用 したリモートサーバーの管理が可能になります。

リモート管理に利用できないツールは、リモートデスクトップ接続で代替 A

[コンピューターの管理] に含まれるほとんどのツールは、このガイドで説明した方法で利用できるはずです。ただし、[デバイスマネージャー] と [ディスクの管理] は、リモート管理に対応していないため使用できません。これらのツールを使用する場合は、リモートデスクトップ接続を利用してください。

また、管理ツールの中には、追加のファイアウォール許可設定やセキュリティ設定が必要な場合や、ド メイン管理者アカウント(またはサーバーのローカル管理者と同じ名前、同じパスワード)による Windows 10 へのサインインが要求されるものもあります。これらはリモートデスクトップ接続で完 全に代替できるため、個別のツールについては説明を省略します。

2.3 サーバーマネージャーによるファイルサーバーの管理

リモートデスクトップ接続から起動する [サーバーマネージャー]、または Windows 10 に追加した RSAT の [サーバーマネージャー] を使用すると、LAN DISK Z の Windows Server IoT 2019 for Storage が提 供するファイルサーバーの主要な機能を単一の GUI で管理することができます。

ファイルサービスと記憶域サービス

[サーバーマネージャー] にファイルサーバー機能を持つサーバーを管理対象として追加すると、[ファイルと記憶域サービス] にそのサーバーが分類され、ここからボリュームや共有、iSCSI ターゲットなどの管理ができるようになります。

🍐 サーバ	ーマネージャー		- 0	×
E	●	▼ (記)	「) 表示(V) ヘル	プ(H)
	サーバー ボリューム ディスク 記憶域プール 共有	サーバー すべてのサーバー 合計: 1 フィルター	<i>রিয়িয</i> ় ▼ ⊙ Windo	
	iscsi ワークフォルダー	HDL-Z19 192.168.10.121、192.168.10.13 オンライン - パフォーマンス ガウンターが開始されていません。2019/05/24 重複除去スケジュール iSCSI ターゲット設定 ファイル サーパー リソース マネージャー ファイル サーパー リソース マネージャー の設定 役割と機能の追加 サーパーの再起動 コンピューターの管理	<u>15;48:</u> 50 00429 	
		イベント オ〈てのイベント」合計:0 リモートデスクトップ接続 Windows PowerShell NIC チーミングの構成 フィルター ア サーバー名 ID 重大度 ソース ログ 日付と時刻 管理に使用する資格情報 パ(フォーマンスカウンターの開始 サーバーの削除 最新の情報に更新 コピー	∞	

ファイルサーバーリソースマネージャーの役割サービスの追加

このガイドの次に説明するファイルサーバーリソースマネージャーの役割サービスは、LAN DISK Z の Windows Server IoT 2019 for Storage には既定でインストールされていません。[サーバーマネージャ -]の[すべてのサーバー]で管理対象のサーバーを右クリックし、[役割と機能の追加]をクリックして [役割と機能の追加ウィザード]を開始して追加してください。[ファイルサーバーリソースマネージャー] の役割サービスは、[ファイルサービスと記憶域サービス] - [ファイルサービスおよび iSCSI サービス] の下にあります。この役割サービスとともに、関連する管理ツールをインストールします。インストールを 完了するために、通常、サーバーの再起動は求められません。

役割サービスを追加したら、ファイルサーバーリソースマネージャーのリモート管理を可能にするために、 [Windows Defender ファイアウォール]の[例外の規則]で以下のグループの規則を有効化します。

● [リモートファイルサーバーリソースマネージャー管理] グループのすべての規則



[ファイルサーバーリソースマネージャー] スナップインで使用される資格情報

Windows 10 に追加した RSAT の [サーバーマネージャー] から開始する [ファイルサーバーリソー スマネージャー] スナップインや、[ファイルサーバーリソースマネージャー] スナップインの [別の コンピューターに接続] によるリモートサーバーのファイルサーバーリソースマネージャーの接続に は、Windows 10 にサインイン中の資格情報(ローカルアカウント、Microsoft アカウント、または Active Directory ドメインアカウント)が使用されます。[サーバーマネージャー] に指定した別の資 格情報が使用されることはありません。

そのため、ファイルサーバーリソースマネージャーをリモートから管理するには、通常、サーバーの管理者アカウント(ローカル Administrators グループのメンバー)となっている、Active Directory ドメインアカウントでサインインしていることが前提となります。この要件は、Windows 10 のローカルアカウントして、サーバー側に作成したローカル管理者アカウントと同じ名前(Administrator の使用は非推奨)、同じパスワードのユーザーを作成し、そのユーザーでWindows 10 にサインインすることで回避することができます。

ファイルサーバーリソースマネージャーの全体設定

ファイルサーバーリソースマネージャーには、電子メールによる管理者やユーザーへの通知機能があります。 この通知機能を利用するためには、少なくとも SMTP ポート 25、匿名アクセスでメールの転送が可能な SMTP メールサーバーが社内ネットワーク上で利用できる必要があります。

転送用のメールサーバーを利用できる場合は、[サーバーマネージャー]の[ファイルサービスと記憶域サ ービス] – [サーバー] で管理対象のサーバーを右クリックして [ファイルサーバーリソースマネージャー の設定] をクリックし、[SMTP サーバー] にメールサーバーの FQDN または IP アドレスを設定します。ま

Α

た、[管理者の電子メール] に通知先となる管理者の電子メールアドレスを、[差出人の電子メールアドレス] に送信元となる電子メールアドレスを入力します。

📥 サーバーマ	ネージャー					-	- C) ×	×
¢¢	 ・・ ファイ 	′ル サービスと記憶域サービ	゚ス・サ−バ−	• ② 🖡	管理(M) >>	/ール(T) 表	表示(V)	∧ルプ(H)
	サーバー ポリューム ディスク 記憶域プール 共有 iSCSI ワークフォルダー	サーバー すべてのサーバー 合計: 1 アルター ク サーパー名 IPv4 アドレス HD-Z19 192.163.10.13 重視除去スケジュール iSCIS ターグット設定 ファイル サーバー リソース マネージャーのEP 役割と戦能の追加 ローカル サーバー リソース マネージャーのEP 役割と戦能の追加 ローカル サーバーのシャットダウン コンピューターの管理 リモート・デスストップ接続 Windows PowerShell NIC チーミングの構成 管理に使用する資格情報… パフォーマンス カウンターの開始 最新の语報に更新 コピー	 ▶ ファイル サーバー リソース マネージャーの設定 HDL-Z19 電子メールの通知 SMTP サーバー(S): 管理者の電子メール(E): 歴出人の電子メール(E): 			-	-	×	~
				(OK ŧ	ャンセル	適用	(<u>A</u>)	

上記の設定は、[ファイルサーバーリソースマネージャー] スナップインの [オプションの構成] の [電子メ ール] タブで設定することもできます。

ファイル(F) 操作(A) 表示(V) ヘルブ(H) ファイルスクリーンの話査 自動分類 Pクセス拒否アシスタンス ● ● □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
< >> OK キャンセル

SMTP ポート 25、匿名アクセスでメール転送を許可するようなメール環境は、マルウェアによって踏

み台に使用されるリスクがあるため、高いセキュリティが要求される現代のメール環境としては不適切 なものです。このセキュリティ上のリスクを理解した上で、必要な対策(転送元 IP アドレスや転送先 アドレスの制限など)を講じたメールサーバーを用意できる場合に限り、ファイルサーバーリソースマ ネージャーのメール通知環境をセットアップしてください。

ファイルサーバーリソースマネージャーのクォータの管理やファイルスクリーンの管理でユーザーごとの 通知を行う場合は、さらに Active Directory ドメイン環境が必要になります。ファイルサーバーリソースマ ネージャーは、通知先のユーザーのメールアドレスとして、Active Directory のドメインユーザーアカウン トの [電子メール (mail)] 属性を使用します。つまり、ユーザーごとの通知機能は、LAN DISK Z の NAS デバイスとクライアントの両方が Active Directory ドメインのメンバーとしてセットアップされており、 NAS デバイスの共有フォルダーへのアクセスが Active Directory のドメインユーザーアカウントで行われ る環境でのみ利用できます。

このガイドの「付録 外部メールサービスを利用したメール通知の実現」では、ファイルサーバーリソース マネージャーのメール通知機能を使用せずに、Outlook.com や Office 365 といった外部メールサービスを 使用して通知する方法について説明しています。ユーザーごとの通知には利用できませんが、管理者への固 定メッセージの通知に応用することができます。

3 ファイルサーバーリソースマネージャーの活用

ファイルサーバーリソースマネージャーの機能の一部は、[サーバーマネージャー]の[ファイルサービス と記憶域サービス]に統合されています。すべての機能は[ファイルサーバーリソースマネージャー]スナ ップインで管理できます。

3.1 フォルダーの使用法(分類プロパティ)

ファイルサーバーリソースマネージャーには分類プロパティという概念があります。既定では[フォルダーの使用法]というローカルプロパティに次の4つの値が設定済みで利用可能な状態になっています。共有フォルダーに対して[フォルダーの使用法]を設定しておくこと、ファイルサーバーリソースマネージャーの他の機能においてフォルダーの対象化のために利用できます。例えば、個別のフォルダーごとに指定する代わりに、[ユーザーファイル] ローカルプロパティが設定されたすべてのフォルダーを対象化できます。

- ユーザーファイル (User Files)
- グループファイル(Group Files)
- アプリケーションファイル (Application Files)
- バックアップおよびアーカイブファイル(Backup and Archival Files)

[フォルダーの使用法]は、[サーバーマネージャー]の[ファイルサービスと記憶域サービス] – [共有] から開始する[新しい共有ウィザード]でファイル共有プロファイル[SMB 共有 – 高度]を選択した際に、 [管理プロパティ]のページで選択できるようになっています。ファイル共有プロファイル [SMB 共有 – 簡 易]を選択した場合は、分類プロパティを設定する場面はありませんが、作成済みの共有のプロパティの[管 理プロパティ]を使用して後から選択することができます。

[フォルダーの使用法]の表示名と値

 ● Indiany 0.00/1 ● Indiany 0.00/1<th>🏊 サー/</th><th>ーマネージャー</th><th></th><th>Rausen of uter</th><th></th><th>X</th>	🏊 サー/	ーマネージャー		Rausen of uter		X
 ・サーバー ・パレューム ・パレター ・ピー ・レー ・ ・ ・	E	● ・ ファイル	,サービスと記憶域	Library		
		サーバー ボリューム ディスク 記信域ブール <mark>共有</mark> iSCSI ワークフォルダー	共有 すべての共有 会計・ 大市 ・ HDL-Z19 (3) Documents Library Users	全般 アクセス許可 設定 管理プロパティ	すべて表示 + + -	管理プロパテイ わんぷーの使用法、プロバティでは、フォルダーおよびそのフォルダーに保存されるファイル の準備の目的を指定します。またこのプロバマイは、分類規則などのテータ管理ポリジーで 使用されます。 コーガークフィル コーガーファイル プリルーファイル プリカージョンソフィル プリカージョンファイル フォルダー所有者の電子メール、プロバティでは、フォルダーへのアクセスを拒否された後 ユーザ・ガアシスタンスを要求するときに連絡する配布リストまたは電子メール アドレスを指 た。 フォルダー所有者の (セミコロンで区切られた) 電子メール アドレスを指定する(E)

[フォルダーの使用法] ローカルプロパティは、[ファイルサーバーリソースマネージャー] スナップインの [分類管理] – [分類プロパティ] で編集することができます。例えば、独自の値を追加することができます。また、[操作] メニューの [フォルダー管理プロパティの設定] を使用して、フォルダーに対してプロ パティを設定することもできます。

[サーバーマネージャー] や [ファイルサーバーリソースマネージャー] スナップインは、[フォルダ ーの使用法] ローカルプロパティが実際の値ではなく、ローカライズされた表示名(例:ユーザーファ イル)で表示します。[ファイルサーバーリソースマネージャー] スナップインを使用して [フォルダ ーの使用法] ローカルプロパティの編集画面を開くと、値を追加や変更をしなくても、日本語の表示名 から英字の値(例: User Files、Application Files)に変わってしまうことに注意してください。これ は表示上の問題であり、実際の分類に影響することはありません。

3.2 クォータの管理

▲

ファイルサーバーリソースマネージャーを使用すると、ファイルサーバーの共有フォルダーのディレクトリ パス内でユーザーが使用できるディスク領域に上限を設定することができます。クォータには、制限を超え てのファイルの保存を拒否する「ハードクォータ」と、使用量の計測だけ行い実際の制限は行わない「ソフ トクォータ」の2種類があり、制限値に対するしきい値を設定して、管理者やユーザーへの電子メールによ る警告の通知やイベントログへの記録、コマンドの実行などの処理を自動化することができます。Windows は標準で、NTFS ボリュームでディスククォータを作成することができますが(エクスプローラーでボリュ ームのプロパティを開き [クォータ] タブからクォータを作成できます)、これはディスク単位のクォータ 制限であり、ファイルサーバーリソースマネージャーのような高度な管理機能は備えていません。 [サーバーマネージャー]の[ファイルサービスと記憶域サービス] – [共有]から開始する[新しい共有 ウィザード]では、ファイル共有プロファイル[SMB共有 – 高度]を選択した場合に、[クォータ]ページ でクォータのテンプレートを選択できるようになっています。[ファイルサービスと記憶域サービス] – [共 有]で既存の共有フォルダーを右クリックして [クォータの構成]を開き、あとから設定または変更するこ ともできます。

ユーザーがクォータのしきい値を超えた場合

ユーザーが共有フォルダーにファイルを保存したときに、ハードまたはソフトクォータのしきい値を超えた 場合、しきい値に定義されている操作が自動実行され、管理者やユーザーへの通知やイベントログへの記録 が行われます。また、ファイルを保存する際にハードクォータの100%に達する場合は、空き領域不足で保 存はブロックされます。



クォータ設定でイベントログに記録するように設定した場合、サーバーの [Application] ログにソース [SRMSVC] からのイベントが記録されます。

🌆 コンピューターの管理					
ファイル(<u>F</u>) 操作(<u>A</u>) 表示(<u>V</u>) /	ヘルプ(<u>H</u>)				
🗢 🄿 🙍 🖬 👔 🖬					
ヨンピューターの管理(ローカル)	1×1	日付と時刻	ソース	ተሻንት ID	タスクのカテゴリ
	▲ 警告	2019/05/22 9:38:45	SRMSVC	12325	なし
	1 情報	2019/05/22 9:31:00	VSS	8224	なし
> 📑 h (2) - C_2 -	1 情報	2019/05/22 9:16:00	VSS	8224	なし
🗸 📫 Windows ログ	イベント 12325. SRMSV	с			×
Application	A 40.				
€ セキュリティ	全般詳細				
Setup					
ミング システム	ユーサー HDL-219¥	demouserU1ほ、サーハー HDI まート・トの地図(+ 10000 M	L-Z19 上() D:¥Shares¥D; ロフ: 理士 at as MD (書)	emo ()クォータ() と 田川 エムキー (中国)	35%(リクォータ
Forwarded Event	のしきい地を超えまし	パこ。クオーダ(J市)P氏(よ 100.00 M	B (1、現在 91.85 МВ 1要)	日内しいます。(制取	\$(J) 91%)
> 10 アプリケーションとサービ					
📑 サブスクリプション					
> 🕺 共有フォルダー					

クォータのテンプレートの編集

ファイルサーバーリソースマネージャーには既定でハードとソフトの12のクォータのテンプレートが定義 済みになっています。いずれもユーザー(Active Directoryドメイン環境が必要)や管理者への電子メール 通知が設定されています。そのため、メール環境が利用できない場合、既定のクォータのテンプレートをそ のまま利用することはできません(メール通知が機能しません)。メール環境が利用できない場合は、使用 するクォータのテンプレートの管理者やユーザーへの電子メール通知設定をオフにするか、電子メール通知 設定を含まない独自のクォータのテンプレートを作成して使用してください。

뭘 ファイル サーバー リソース マネージャー	10 GB の制限 のクォータ テンプレートの	85% のしきい値のプロパティ	×
ファイル(F) 操作(A) 表示(V) ヘルプ(H) (ティー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	クォータ テンプレートからのプロパティの 10 GB の制限	使用率 (%) がた(に達したら、通知を生成する(G): 85	-
 3 ファイルサ・バーリソースマネージ ・ダ クォータの音型 ・ターク 3 ファイル スクリーンの音理 ・図 クォータのテンブレート ・ロ 058 の制限 10.00 (2000) 10 TB ボリュームの使用 10.01 ・ロ 048 制限 100 MB 制用 100 MB ND 100 MB ND	設定 テンプレート名(N)× 10 GB の参照限 説明 (名略寺T)(D)× 空を結婚の参照限 参照死値(L)× 10000 GB ✓ の /\ード クォー欠(L): 参照死値を起 ○ ソフト クォー欠(S): 参照死値を起 ○ ソフト クォー欠(S): 参照死値を起 ○ ジフト クォー欠(S): 参照死値を起 ○ ジラト クォー欠(S): 参照衣(信を起 ○ ジョント クォーク(S): 参照衣(信を起 ○ ジョント クォーク(S): 参照衣(信を起 ○ ジョント クォーク(S): 参照衣(信を起 ○ ジョント クォーク(S): 参照衣(E)) ○ ごうか(A) - 編集(E) -	 電子メールメッセージ イベントログ コマンド レポート は次の管理者に電子メールを送信する(A): account@domain の形式で指定し、複数のアカウントはセミコレンで区切ってください。 レイン値を起えたユーザー(電子メールを送信する(U) マナメール メッセージ ドキと、シャレージで(開発するテキストを入力してください。 ホーム・シージー(電子メールを送信する(U) マナメール メッセージ ドキと、シャレージで(開発するテキストを入力してください。 現在の目の後期でのかったりまた。 (Accuta Threshold)% のクタータのしまい(値を起ぶました) メッセージネマ(M): コージー ESource is Owner! は、サーバー(Server! の [Quota Path] 上のクターダで) (Acuta Threshold)% のクタータのしまい(値を超ぶました) メッセージネマ(M): コージー ESource is Owner! は、サーバー(Server! の [Quota Path] 上のクターダン ((Acuta Threshold)% のクタータのしまい(値を超ぶました) メッセージネマ(M): コージー ESource is Owner! は、サーバー (Server! の [Quota Path] 上のクターダン ((Acuta Threshold)% のクタータのしまい(値を超ぶました) メッセージネマ(M): コージー ESource is Owner! は、サーバー (Server! の [Quota Path] 上のクターダン ((Acuta Threshold)% のクタータのしまい(値を超ぶました) メッセージネマ(M): コージー Source is Owner! は、サーバー (Server! の [Quota Path] 上のクターダン ((Acuta Threshold)% のクタータのしまい(値を超ぶました) メッセージネマ(M): コージー Source is Owner! (は、サーバー (Server!)) マージ マング (E): (Admine Threshold)% のクタータのしまい(マング (Acuta Used MB) MB! (利用) ロージャング (E): (Admine Threshold)% (Acuta Used MB) (Admine Threshold) (Admine Threshold) (Admine Threshold) (Admine T	
		UK FP/C	<i>ν</i>

電子メール通知の代替策について

電子メール通知の代替策について

電子メール通知機能を利用できる環境が無い場合、管理者はハードクォータに達したユーザーからのク

レームや、イベントログの監視、ソフトクォータと記憶域レポートの結果に基づいて、ユーザーに対し

て不要なファイルの削除の依頼を行ったり、クォータの制限を増やしたりといったマニュアルの対応で 運用できるでしょう。最も重要なことは、サーバーのストレージを使い果たしてしまう前に対処するこ とです。

管理者への固定メッセージの通知については、このガイドの「付録 外部メールサービスを利用したメ ール通知の実現」の方法をクォータのテンプレートのコマンド実行機能(しきい値のプロパティの[コ マンド]タブ)に応用することで実装可能です。

3.3 ファイルスクリーンの管理

ファイルサーバーリソースマネージャーのファイルスクリーンの管理は、ファイルの種類(拡張子)に基づいて、指定したディレクトリパスへの保存をブロック、または警告やイベントログへの記録で監視する機能を提供します。ファイルスクリーン処理には、該当するファイルの種類の保存を許可しない「アクティブ」と、監視のみで保存を許可する「パッシブ」の2種類あり、フォルダーに対するカスタム設定またはファイルスクリーンのテンプレートによる設定が可能です。

ファイルスクリーンの作成

ファイルスクリーンの管理は、[サーバーマネージャー]の[ファイルサービスと記憶域サービス]には統 合されていません。この機能を利用するには、[ファイルサーバーリソースマネージャー]スナップインの [ファイルスクリーンの管理] – [ファイルスクリーン]の[操作]ペインから[ファイルスクリーンの作 成]をクリックし、ディレクトリパス(例えば、共有フォルダーのローカルパス)に対してスクリーン処理 設定を作成します。



例えば、ドキュメント用の共有フォルダーに実行可能形式のファイル(.exe、.bat、.inf など)やシステム

ファイル(.dll、.sys など)が保存されるのをブロックするには、カスタム設定でファイルグループの[実 行形式ファイル]と[システムファイル]をチェックし、[アクティブスクリーン処理]を選択します。スク リーン処理が発生した際に通知やイベントログへの記録を行うには、[電子メールメッセージ] タブや[イ ベントログ] タブを設定します。

ファイルスクリーン処理

ユーザーがドキュメント用の共有フォルダーに実行可能形式やシステムファイルの種類のファイルを保存 しようとすると、アクセスが拒否されます。

ごみ箱	및 ☑ <mark>-</mark> マ Documents ファイル ホーム 共有 表示				× ~ ?
	← → · ↑ ▲ → *ットワーク > H	DL-Z19 > Documents	~ Ō	Documentsの検索	<i>م</i>
2	名前	更新日時 種類	サイズ		
	Manual WhitePapers	2019/05/14 18:02 ファイル フォルダ- 2010/05/14 18:02 ファイル フォルダ-			
Microsoft Edge	・ ドキュメント フリー表材	■■ 対象のフォルダーへのアクセスは拒否されました	: -	- 🗆 X	
	demo.txt	この操作を実行するアクセス許可が必要です			
procexp.exe	2	Documents			
	processgi <mark>+ Documents ∧⊐ピ</mark> -		再試行(<u>R</u>)	キャンセル	
		◇ 詳細情報			
	5 個の項目				

イベントログに記録するように設定した場合、サーバーの [Application] ログにソース [SRMSVC] からの イベントが記録されます。



ファイルスクリーンのテンプレートの編集

既定で以下の 4 つのファイルスクリーンのテンプレートが定義済みになっており、[ファイルサーバーリソ ースマネージャー] スナップインの [ファイルスクリーンの管理] – [ファイルスクリーンテンプレート] で確認および編集することができます。

- イメージファイルのブロック(アクティブ)
- オーディオとビデオのファイルのブロック(アクティブ)
- 実行形式とシステムのファイルの監視(パッシブ)
- 実行形式のファイルのブロック(アクティブ)

クォータのテンプレートと同様に、ファイルスクリーンのテンプレートにもユーザー(Active Directory ド メイン環境が必要)や管理者への電子メール通知が設定されています。そのため、メール環境が利用できな い場合、既定のクォータのテンプレートをそのまま利用することはできません(メール通知が機能しません)。 メール環境が利用できない場合は、使用するファイルスクリーンのテンプレートの管理者やユーザーへの電 子メール通知設定をオフにするか、電子メール通知設定を含まない独自のファイルスクリーンのテンプレー トを作成して使用してください。あるいは、その都度、カスタム設定を行います。

電子メール通知の代替策について

電子メール通知機能を利用できる環境が無い場合は、アクセスが拒否されたユーザーからのクレームや、イベントログの監視、記憶域レポートの結果に基づいて、ユーザーにマニュアルで対応することができるでしょう。

管理者への固定メッセージの通知については、このガイドの「付録 外部メールサービスを利用したメ ール通知の実現」の方法をファイルスクリーン処理のコマンド実行機能(プロパティの[コマンド]タ ブ)に応用することで実装可能です。

3.4 ファイル管理タスク

Ħ

ファイルサーバーリソースマネージャーの分類管理とファイル管理タスクは FCI (File Classification Infrastructure) とも呼ばれ、ファイルのアーカイブやセキュリティ(自動暗号化や動的アクセス制御)を 実現する柔軟なカスタマイズ機能を提供します。自動暗号化や動的アクセス制御は Active Directory ドメ イン環境が前提で、高度なカスタマイズは構成が複雑になり、正常性の監視やメンテナンス作業の負担が大 きくなってしまうでしょう。

ここでは、ファイルのアーカイブについての簡単な活用例を紹介します。ユーザーのドキュメント用フォル ダーに格納されていて長期間アクセスされていないファイルを、ファイル管理タスクのスケジュール実行を 使用してアーカイブ用のディレクトリに移動するという利用シナリオです。管理者は、事前にユーザーに対 して長期間アクセスのないファイルは自動的に特定の場所(アーカイブ用の共有フォルダーなど)に移動す る旨を事前に周知しておき、目的のファイルが見つからない場合はユーザー自身で移動先のパスから探して もらって、不要なファイルを削除する、あるいは元の場所に戻す(最終アクセス日が更新されます)など、 対処を要請することができます。

ファイル管理タスクの作成

ファイル管理タスクは、[ファイルサーバーリソースマネージャー] スナップインの[ファイル管理タスク] の[操作] ペインから [ファイル管理タスクの作成] をクリックして作成します。[ファイル管理タスクの作 成] ダイアログボックスの [全般] タブで [タスク名] に分かりやすい名前を指定したら、[スコープ] タブ に切り替えます。

🎝 ファイル サーバー リソース マネージャー			- 🗆 X
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
	ファイル管理タスクの作成	×	
ファイル サーバー リソース マネージャ タス タス タス マゥークの管理	全般 スコーブ アクション 通知 レポート 条件	スケジュール	操作
	タスク名(N):		ファイル管理タスク
● クォータのテンプレート □ ファイル スクリーンの答理 □	ADD 011 (1300 - 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	M 19X012 9 Q(E)	アイル管理タスクの作成…
	戎 月(<u></u>):		(4) 取新の情報に更新
IIII ファイル スクリーン テンプレ □ ファイル グループ			
■ 記憶域レポートの管理			
> 🛗 分類管理			
	ヘルフ(<u>H</u>)	OK キャンセル	

[スコープ] タブでは、「3.1 フォルダーの使用法(分類プロパティ)」で説明した分類プロパティに基づいて対象のフォルダーを選択させることができます。[追加] をクリックして個別のパスを指定することもできます。続いて [アクション] タブに切り替え、ドロップダウンリストボックスから [ファイルの有効期限] を選択し、[有効期限切れのディレクトリ] にファイルの移動先のパスを指定します。

ファイル管理タスクの作成	×	ファイル管理タスクの作成	×
全般 スコープ アクション 通知 レポート 条件 次の種類のデータを格納するすべてのフォルダーを含めます	スケジュール す:	全般 スコーブ アクション 通知 レポート 条件 スケジュール 種類(T): ファイルの有効期限 マ 有効期限切れのディレクトリ(E): 参照(B)	
□ アブリケーション ファイル □ グループ ファイル □ バックアップおよびアーカイブ ファイル ☑ ユーザー ファイル		D#Shares#OLDDATA	
このスコーフに含まれるフォルター: フォルダー フォル D¥shares¥demo¥ User D¥Shares¥Documents¥ User	ダーの使用法 Files Files		
フォルダー管理プロパティの設定。 フォルダー管理プロパティの設定。	カロ 肖耶奈 OK キャンセル	ヘルプ(H) OK キャンセル	ŀ

[条件] タブに切り替えると、[ファイルの作成からの日数]、[ファイルの最終変更からの日数]、[ファイルの最終アクセスからの日数]、またはこれらの組み合わせで有効期限を設定します。最後に [スケジュール] タブに切り替え、実行スケジュールを調整します。電子メール通知環境がある場合は、[通知] タブを構成してファイルの移動をユーザーに通知するように設定することもできます。

ファイル管理タスクの作成 ×	ファイル管理タスクの作成	×
全般 スコープ アクション 通知 レポート 条件 スケジュール プロパティの条件(P) プロパティ 演算子 値 オフセ	全般 スコープ アクション 通知 レポート 条件 スケジュール スケジュール 実行時期 23:00:00 ◆	
	 ● 毎週 ○ 毎月 □ 日曜日 □ 月曜日 □ 火曜日 □ 水曜日 □ 木曜日 ☑ 金曜日 	
送力(A) 編集(E) 前部(R)	□土曜日	
□ ファイルの作成からの日数(C): 0 🖕	□ 制/段 (B寺間弦文):	
 □ ファイルの最終変更からの日数(M): □ クァイルの最終アクセスからの日数(S): 3851 全 サーバーによって最終アクセス特別が管理されない場合、この条件は正しく 概能しないとびあります。 □ ファイルをのパターン: □ フィイルをつパターン: □ フィイルをつパターン: □ フィイルトード文字がサポートされます。複数入力する場合はセミコロン (.) で パターンを区切ります。 例! *docx*xlsx*financial** 	連続動作 □ 新しいファイルに対して連続実行する □ ログを有効にする 最大ログサイズ (KB): 1024 連続動作では、条件に分類プロパティを含むタスクで、新しく追加されたファイルのな 処理します。	¢€
ヘルプ(H) OK キャンセル	ヘルプ(H) OK キャン	セル

3.5 記憶域レポートの管理

ファイルサーバーリソースマネージャーは、以下に示す10種類の記憶域レポートの作成機能を持ちます。 これらのレポートは[ファイルサーバーリソースマネージャー]スナップインを使用してスケジュールまた は手動で作成することができます。また、クォータやファイルスクリーン処理、ファイル管理タスクと連動 してレポートを生成させることもできます。

- クォータの使用率
- ファイルグループごとのファイル
- ファイルスクリーン処理の監査
- プロパティごとのファイル
- プロパティ別フォルダー
- 最近アクセスされていないファイル
- 最近アクセスしたファイル
- 重複しているファイル
- 所有者ごとのファイル
- 大きいサイズのファイル

[ファイルスクリーン処理の監査] レポートについて

[ファイルスクリーン処理の監査]レポートを生成するには、ファイルサーバーリソースマネージャー の全体設定である [オプションの構成]の [ファイルスクリーンの監査] タブで [監査データベースに ファイルスクリーン処理の動作状況を記録する] をチェックしておく必要があります。

このオプションは既定で無効です。無効の場合、または有効であっても監査データベースが空の状態の 場合、[ファイルスクリーン処理の監査] レポートの生成はエラーで失敗します。このレポートを含む 同じスケジュールまたは手動タスクはエラーが発生すると途中でレポートの生成を停止するため、他の レポートの生成に影響することに注意してください。

スケジュール生成と今すぐ生成

▲

[ファイルサーバーリソースマネージャー] スナップインの [記憶域レポートの管理] の [操作] ペインで [新しいレポートのタスクのスケジュール] をクリックすると、記憶域レポートをスケジュールに従って自 動生成させることができます。[レポート名] を入力し、生成するレポートを選択したら、[スコープ] タブ で分類プロパティまたは個別のパス設定で対象のフォルダーを指定し、[スケジュール] タブでスケジュー ルを調整します。[設定] タブの [パラメーターの編集] では、各レポートでカスタマイズ可能なパラメータ - (最終アクセス日からの日数や、大きなファイルのサイズなど)を変更できます。

スケジュールタスクで生成されたレポートは、既定で C:¥Storage¥Reports¥Scheduled ディレクトリに DHTML 形式で格納されます。

🎝 ファイル サーバー リソース マネージャー		- 🗆 ×
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	記憶域レポート タスクのプロパティ ローン	
	設定 スコープ 配信 スケジュール	
🖾 ファイル サーバー リソース マネージャ 🛛 レオ		操作
> # クォータの管理 、 ◎ ファイル スクリーンの管理	レポート名:	記憶域レポートの管理 🔺
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	定期レポート	新しいレポートのタスクのスケジュール
> 📸 分類管理		レポートタスク用のレポートの追加と
ころ ファイル管理タスク	しポート データ	レポートを今すぐ生成する
	生成するレポートの選択(P):	る 最新の情報に更新
	✓ クォータの使用率 ヘ バラメーターの編集	表示
	☑ ファイル グループごとのファイル	パルプ
	は、レポートのラベルを 選択したレポートの表示(V)	選択した記憶域のレポート▲
		レポート タスクを今すぐ実行
	9 个 (の記憶域レホートの対象と9 るノアイルの最大数 最大数(M):	レポート タスクの取り消し
	1000	レポート タスクのプロパティの変更
		🗙 削除
< >	レポートの形式 「 DHTML(D)] HTML(M)] XML(X)] CSV(C)] テキスト(T) OK キャンセル	

[操作]ペインの [レポートを今すぐ生成する]をクリックすると、指定したレポートを即時に生成させ、 表示させることができます。この方法で生成したレポートは、C:¥Storage¥Reports¥Interactive ディレク トリに格納されます。

📙 🛃 📕 🖛 Interactive	2					- [) X
ファイル ホーム 共有	表示	(+))	C:¥St	orageReports¥Interactive¥Filesby(Owner32_201	9-05-22_11-34-	49.html
	2 # ^	🥌 C:¥Stora	geReports	¥Interacti × 📑			
▼ デスクトップ	1 = 100 DuplicateFiles31_2019-05-22_11-34-49_file			所有者ごとのファイルのし ^{生成日時: 2019/05/22 11:34:49}	ノボー ト		
置 ドキュメント	FilesbyOwner32_2019-05-22_11-34-49_file	レポートの	説明:	ファイルを所有するユーザー順にファイ	「ルを→覧表示	します。このレポ	 -トを使って、サ
■ ビクチャ	FilesByType28_2019-05-22_11-34-49_files	コンピュー	ター:	HDL-Z19			
📑 ビデオ	FileScreenAudit13_2019-05-22_11-28-28_f.	レポートフ	オルダー:	'User Files (D:\shares\demo D:\Sh	ares\Documen	ts\)'	
🎝 ミュージック	FileScreenAudit21_2019-05-22_11-31-38_f.						
🏪 ローカル ディスク (C	Largerlies33_2019-05-22_11-34-49_files	🔥 レポ	ートの基準	に一致したグループごとのファイルの最	大数を超えまし	た。次のファイル	グループ内の
I-O DATA	Ouotal leage? 2019-05-22 09-54-12 files	019-05-22_11. [] 19-54-12_files 所有者ごとのファイルのレポート 目次 11-34-49_files レポートの合計					
PerfLogs	Quotal/sage27_2019-05-22_05-04-12_Inics						
Program Files	最近アクヤスされていない29 2019-05-22 11-						
Program Files (DuplicateFiles31_2019-05-22_11-34-49.htm	 ファ・	<u>者ここの</u> 5 (ルグルー	<u>・コム</u> -ブごとのサイズ			
StorageReports	FilesbyOwner32_2019-05-22_11-34-49.htm	所有	者: HDL-Z	<u>19\demouser01の統計</u> 19\demouser02の統計			
Interactive	FilesByType28_2019-05-22_11-34-49.html	所有	者: HDL-Z	19\demouser03の統計			
Scheduled	🗿 LargeFiles33_2019-05-22_11-34-49.html			1 4-	1000		
Windows	MostRecentlyAccessed30_2019-05-22_11						
7_tf_	🕘 QuotaUsage2_2019-05-22_09-54-12.html		レホー	トに表示されるファイル	L	ボートの発件に-	*蚊するすべて
	QuotaUsage27_2019-05-22_11-34-49.html	所有者	ファイル	ディスク上の合計サイズ	所有者	ファイル	ディスクト
🚍 ローカル テイスク (C	● 最近アクセスされていない29_2019-05-22_11	3	229	7,298 MB	3	12487	7,
🥏 ネットワーク 🗸 🗸		現在のレポー	トの先頭	2			
18 個の項目 1 個の項目を	選択 188 KB	所有者	ことのサイ	ば			

付録 外部メールサービスを利用したメール通知の実現

ファイルサーバーリソースマネージャーが備える電子メール通知機能は、SMTP ポート 25、匿名アクセス が可能な、セキュアではない転送用の SMTP メールサーバーを必要とします。メールシステムに高いセキュ リティが求められる現代、そのようなメールサーバーの存在や設置はセキュリティ上のリスクになるため、 ファイルサーバーリソースマネージャーの電子メール通知機能のためにそのような環境を用意するのは推 奨される方法ではありません。

代替策として、Windows PowerShell の Send-MailMessage コマンドレットを利用した方法を紹介します。 Send-MailMessage コマンドレットは、現代のセキュアなメールシステム環境に対応できるオプション(ポ ート番号の設定、SMTP 認証、TLS/StartTLS の対応など)をサポートしています。オプションの詳細につ いては、以下の公式ドキュメントを参照してください。

Send-MailMessage

https://docs.microsoft.com/ja-jp/powershell/module/Microsoft.PowerShell.Utility/Send-MailMessage

例えば、Microsoft アカウント(Outlook.com)や Office 365 のメールアカウントを利用できる場合は、フ ァイルサーバーリソースマネージャーのクォータの管理やファイルスクリーンの管理、ファイル管理タスク が備えるコマンド実行機能で Send-MailMessage のコマンドラインを実行することで、特定のメールアド レス(管理者のメールアドレス)に固定メッセージを送信することが可能です。具体的には、該当する設定 の[コマンド] タブで次のように設定します。

コマンドまたはスクリプトの実行:

C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe

コマンド引数:

-Command "& {\$mailuser = メールアカウント名; \$mailpass = ConvertTo-SecureString メー ルアカウントのパスワード -asplaintext -force; \$mailcred = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList \$mailuser, \$mailpass; Send-MailMessage -From メールアカウントのメールアドレス -To 通知先のメールアドレス -Subject 件 名 -Body メッセージ本文 -Encoding ([System.Text.Encoding]::UTF8) -SmtpServer smtp.office365.com -Port 587 -Credential \$mailcred -UseSSL}"

Outlook.com および Office 365のメール送信設定は共通であり、SMTP サーバー「smtp.office365.com」、 SMTP ポート「587」、TLS/StartTLS「有効」、およびメールボックスの資格情報を指定することで、任意の 宛先にメール送信が可能です。これらの設定は、Send-MailMessage コマンドレットの-Port、-SmtpServer、 -UseSSL でそれぞれ対応することができます。その他の外部メールサービスにも応用できる場合がありま す。



