Systemwalker

FUJITSU

Systemwalker Centric Manager

カスタムイベントログ監視ガイド

UNIX/Windows(R)共通

J2X1-7519-01Z0(00)
2010年4月

まえがき

本書の目的

本書は、Windows Server 2008におけるカスタムイベントログを、Systemwalker Centric Managerを使用してイベントログ監視、監査ログ収集、および監査ログ分析する方法について説明します。

なお、本書は、Windows版/Solaris版/Linux版のSystemwalker Centric Manager V13.3.0以降を対象としています。

本書の読者

本書は、Systemwalker Centric Managerのシステム監視機能、監査ログ管理機能や監査ログ分析機能を使用しているシステムで、Windows Server 2008におけるカスタムイベントログを監視、収集や分析に使用する管理者ユーザを対象にしています。

本書を読む場合、OSやSystemwalker Centric Managerの一般的な操作、システム監視機能、監査ログ管理機能、および監査ログ分析機能の一般的な知識をご理解の上でお読みください。

本書の表記について

エディションによる固有記事について

本書では、標準仕様である“Systemwalker Centric Manager Standard Edition”の記事と区別するため、エディションによる固有記事に対して以下の記号をタイトル、または本文に付けています。

EE:

“Systemwalker Centric Manager Enterprise Edition”の固有記事

GEE:

“Systemwalker Centric Manager Global Enterprise Edition”の固有記事

EE/GEE:

“Systemwalker Centric Manager Enterprise Edition”、および“Systemwalker Centric Manager Global Enterprise Edition”の固有記事

固有記事の範囲は、タイトル、または本文に付いた場合で以下のように異なります。

タイトルに付いている場合

章/節/項などのタイトルに付いている場合、タイトルの説明部分全体が、固有記事であることを示します。この場合、タイトルに対して、オンラインマニュアルの場合は色付けされます。

本文に付いている場合

固有記事全体に対して、オンラインマニュアルの場合は色付けされます。

Windows版とUNIX版の固有記事について

本書は、Windows版、UNIX版共通に記事を掲載しています。Windows版のみの記事、UNIX版のみの記事は、以下のように記号をつけて共通の記事と区別しています。

タイトル【Windows版】

タイトル、小見出しの説明部分全体が、Windows版固有の記事です。

タイトル【UNIX版】

タイトル、小見出しの説明部分全体が、UNIX版固有の記事です。

本文中でWindows版とUNIX版の記載が分かれる場合は、“Windows版の場合は～”“UNIX版の場合は～”のように場合分けして説明しています。

記号について

[ ]記号

Systemwalker Centric Managerで提供している画面名、メニュー名、および画面項目名をこの記号で囲んでいます。

コマンドで使用する記号

コマンドで使用している記号について以下に説明します。

記述例

[PARA={a ｜b ｜c ｜… }]

記号の意味

記号	意味
[ ]	この記号で囲まれた項目を省略できることを示します。
{ }	この記号で囲まれた項目の中から、どれか1つを選択することを示します。
＿	省略可能記号“[ ]”内の項目をすべて省略したときの省略値が、下線で示された項目であることを示します。
｜	この記号を区切りとして並べられた項目の中から、どれか1つを選択することを示します。
…	この記号の直前の項目を繰り返して指定できることを示します。

マニュアルの記号について

マニュアルでは以下の記号を使用しています。

注意

特に注意が必要な事項を説明しています。

ポイント

知っておくと便利な情報を説明しています。

略語表記について

- 以下の製品すべてを示す場合は、“Windows 7”と表記します。
  - Windows(R) 7 Home Premium
  - Windows(R) 7 Professional
  - Windows(R) 7 Enterprise
  - Windows(R) 7 Ultimate
- 以下の製品すべてを示す場合は、“Windows Server 2008 R2”と表記します。
  - Microsoft(R) Windows Server(R) 2008 R2 Foundation
  - Microsoft(R) Windows Server(R) 2008 R2 Standard
  - Microsoft(R) Windows Server(R) 2008 R2 Enterprise
  - Microsoft(R) Windows Server(R) 2008 R2 Datacenter

- Microsoft(R) Windows Server(R) 2008 R2 Standard without Hyper-V(TM)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise without Hyper-V(TM)
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter without Hyper-V(TM)

・以下の製品すべてを示す場合は、“Windows Server 2008 Foundation”と表記します。

- Microsoft(R) Windows Server(R) 2008 R2 Foundation
- Microsoft(R) Windows Server(R) 2008 Foundation

・以下の製品すべてを示す場合は、“Windows Server 2008 Server Core”、または“Server Core”と表記します。

- Microsoft(R) Windows Server(R) 2008 Standard Server Core
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core
- Microsoft(R) Windows Server(R) 2008 Enterprise Server Core
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core
- Microsoft(R) Windows Server(R) 2008 Datacenter Server Core
- Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core

・以下の製品すべてを示す場合は、“Windows Server 2008 STD”と表記します。

- Microsoft(R) Windows Server(R) 2008 Standard
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM)

・以下の製品すべてを示す場合は、“Windows Server 2008 DTC”と表記します。

- Microsoft(R) Windows Server(R) 2008 Datacenter
- Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM)

・以下の製品すべてを示す場合は、“Windows Server 2008 EE”と表記します。

- Microsoft(R) Windows Server(R) 2008 Enterprise
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM)

・以下の製品すべてを示す場合は、“Windows Server 2003 STD”と表記します。

- Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
- Microsoft(R) Windows Server(R) 2003, Standard Edition

・以下の製品すべてを示す場合は、“Windows Server 2003 DTC”と表記します。

- Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition
- Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems
- Microsoft(R) Windows Server(R) 2003, Datacenter Edition

・以下の製品すべてを示す場合は、“Windows Server 2003 EE”と表記します。

- Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition

・以下の製品すべてを示す場合は、“Windows(R) 2000”と表記します。

- Microsoft(R) Windows(R) 2000 Professional operating system
- Microsoft(R) Windows(R) 2000 Server operating system
- Microsoft(R) Windows(R) 2000 Advanced Server operating system
- Microsoft(R) Windows(R) 2000 Datacenter Server operating system

- 以下の製品すべてを示す場合は、“Windows NT(R)”と表記します。
  - Microsoft(R) Windows NT(R) Server network operating system Version 4.0
  - Microsoft(R) Windows NT(R) Workstation operating system Version 4.0
  - Microsoft(R) Windows NT(R) Server network operating system Version 3.51
  - Microsoft(R) Windows NT(R) Workstation operating system Version 3.51
- 以下の製品すべてを示す場合は、“Windows(R) XP”と表記します。
  - Microsoft(R) Windows(R) XP Professional x64 Edition
  - Microsoft(R) Windows(R) XP Professional
  - Microsoft(R) Windows(R) XP Home Edition
- 以下の製品すべてを示す場合は、“Windows Vista”と表記します。
  - Microsoft(R) Windows Vista(R) Home Basic
  - Microsoft(R) Windows Vista(R) Home Premium
  - Microsoft(R) Windows Vista(R) Business
  - Microsoft(R) Windows Vista(R) Enterprise
  - Microsoft(R) Windows Vista(R) Ultimate
- Microsoft(R) Windows(R) Millennium Editionを“Windows(R) Me”と表記します。
- Microsoft(R) Windows(R) 98 operating system、Microsoft(R) Windows(R) 98 Second Editionを“Windows(R) 98”と表記します。
- Microsoft(R) Windows(R) 95 operating system、Microsoft(R) Windows(R) 95 Second Editionを“Windows(R) 95”と表記します。
- 以下の製品上で動作する固有記事を“Windows Server 2003 STD(x64)”と表記します。
  - Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
- 以下の製品上で動作する固有記事を“Windows Server 2003 DTC(x64)”と表記します。
  - Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition
- 以下の製品上で動作する固有記事を“Windows Server 2003 EE(x64)”と表記します。
  - Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
- 以下の製品上で動作する固有記事を“Windows(R) 2000 Server”と表記します。
  - Microsoft(R) Windows(R) 2000 Server operating system
- 以下の製品上で動作する固有記事を“Windows(R) XP x64”と表記します。
  - Microsoft(R) Windows(R) XP Professional x64 Edition
- Systemwalker Centric Manager Standard Editionを“SE版”と表記します。
- Systemwalker Centric Manager Enterprise Editionを“EE版”と表記します。
- Systemwalker Centric Manager Global Enterprise Editionを“GEE版”と表記します。
- Standard Editionを“SE”、Enterprise Editionを“EE”、Global Enterprise Editionを“GEE”と表記します。
- Windows上、Itaniumに対応したWindows上で動作するSystemwalker Centric Managerを“Windows版”と表記します。
- Itaniumに対応したWindows上で動作するSystemwalker Centric Managerの固有記事を“Windows for Itanium版”と表記します。
- Windows Server 2003 STD(x64)/Windows Server 2003 DTC(x64)/Windows Server 2003 EE(x64)に対応したWindows上で動作するSystemwalker Centric Managerの固有記事を“Windows x64版”と表記します。
- Solaris(TM) オペレーティングシステムを“Solaris”と表記します。
- Solarisで動作するSystemwalker Centric Managerを“Solaris版 Systemwalker Centric Manager”または“Solaris版”と表記します。

- HP-UX上で動作するSystemwalker Centric Managerを“HP-UX版Systemwalker Centric Manager”または“HP-UX版”と表記します。
- AIX上で動作するSystemwalker Centric Managerを“AIX版Systemwalker Centric Manager”または“AIX版”と表記します。
- Linux上、Itaniumに対応したLinux上で動作するSystemwalker Centric Managerを“Linux版Systemwalker Centric Manager”または“Linux版”と表記します。また、Itaniumに対応したLinux上で動作するSystemwalker Centric Managerの固有記事を“Linux for Itanium版”と表記します。
- Linux上、Linux for Intel64に対応したLinux上で動作するSystemwalker Centric Managerを“Linux版Systemwalker Centric Manager”または“Linux版”と表記します。また、Linux for Intel64に対応したLinux上で動作するSystemwalker Centric Managerの固有記事を“Linux for Intel64版”と表記します。
- Solaris、Linux、HP-UX、AIX上で動作するSystemwalker Centric Managerを、“UNIX版Systemwalker Centric Manager”または“UNIX版”と表記します。
- Microsoft(R) SQL Server(TM)を“SQL Server”と表記します。
- Microsoft(R) Visual C++を“Visual C++”と表記します。
- Microsoft(R) Cluster ServerおよびMicrosoft(R) Cluster Serviceを“MSCS”と表記します。

輸出管理規制について

本ドキュメントを輸出または提供する場合は、外国為替および外国貿易法および米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。

商標について

Apache、Tomcatは、The Apache Software Foundationの登録商標または商標です。

APC、PowerChuteは、American Power Conversion Corp.の登録商標です。

ARCserveは、米国CA, Inc.の登録商標です。

Citrix、MetaFrameは、Citrix Systems, Inc.の米国およびその他の国における登録商標です。

Ethernetは、富士ゼロックス株式会社の登録商標です。

HP-UXは、米国Hewlett-Packard社の登録商標です。

IBM、IBMロゴ、AIX、AIX 5L、HACMP、Power、PowerHAは、International Business Machines Corporationの米国およびその他の国における商標です。

Intel、Itaniumは、米国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。

JP1は、株式会社日立製作所の日本における商標または登録商標です。

LaLaVoiceは、株式会社東芝の商標です。

LANDeskは、米国およびその他の国におけるAvocent Corporationとその子会社の商標または登録商標です。

Laplinkは、米国Laplink Software, Inc.の米国およびその他の国における登録商標または商標です。

Linuxは、Linus Torvalds氏の米国およびその他の国における商標または登録商標です。

MC/ServiceGuardは、Hewlett-Packard Companyの製品であり、著作権で保護されています。

Microsoft、Windows、Windows NT、Windows Vista、Windows Serverまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Mozilla、Firefoxは、米国Mozilla Foundationの米国およびその他の国における商標または登録商標です。

NEC、SmartVoice、WinShareは、日本電気株式会社の商標または登録商標です。

Netscape、Netscape の N および操舵輪のロゴは、米国およびその他の国におけるNetscape Communications Corporationの登録商標です。

OpenLinuxは、The SCO Group, Inc.の米国ならびその他の国における登録商標あるいは商標です。

平成22年4月

改版履歴
平成22年 4月 初版

目　次

第1章 概要

Windows Server 2008のカスタム イベントログを、Systemwalker Centric Managerを使用してイベントログ監視、監査ログ収集、および監査ログ分析する方法について説明します。

1.1 イベントログの種類

Systemwalker Centric Managerでは、以下のイベントログをイベントログ監視、監査ログ収集、および監査ログ分析できます。

イベントログの種類	イベントログ監視	監査ログ収集、および監査ログ分析
アプリケーション	○	○
セキュリティ	○	○
システム	○	○
ファイル複製サービス	○	○
Directory Service	○	○
DFSレプリケーション	○	○
ハードウェア	○	○
DNS Server	○	○
Internet Explorer	○	×注1
Key Management Service	○	×注1
Media Center	○	×注1
転送された イベント	×	○
Microsoft-Windows-Hyper-V-Config-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Config-Operational	○	○ 注2
Microsoft-Windows-Hyper-V-High-Availability-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Hypervisor-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Hypervisor-Operational	○	○ 注2
Microsoft-Windows-Hyper-V-Image-Management-Service-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Image-Management-Service-Operational	○	○ 注2
Microsoft-Windows-Hyper-V-Integration-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Network-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Network-Operational	○	○ 注2
Microsoft-Windows-Hyper-V-SynthNic-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-SynthStor-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-SynthStor-Operational	○	○ 注2
Microsoft-Windows-Hyper-V-VMMS-Admin	○	○ 注2
Microsoft-Windows-Hyper-V-Worker-Admin	○	○ 注2
Virtual Server	○	× 注1

注1：本書に従って定義することで該当のイベントログの監査ログ収集や監査ログ分析を行えます。

注2：Systemwalker Centric Manager V13.4.0から該当のイベントログの監査ログ収集や監査ログ分析を行えます。

Systemwalker Centric Manager V13.3.0、およびV13.3.1では、本書に従って定義することで該当のイベントログの監査ログ収集や監査ログ分析を行えます。

なお、アプリケーションのインストール、またはユーザ作成のアプリケーションの追加により、異なる種類のイベントログ(カスタム イベントログ)が追加されることがあります。

本書に従って設定を行うことで、追加されたカスタム イベントログを監視/監査することができます。

なお、監視できるカスタム イベントログは、イベントの種類が“Admin”、または“Operational”のものです。

1.2 動作環境

カスタム イベントログのイベントログ監視、監査ログ収集を行う環境について説明します。

監査ログ分析については、Systemwalker Centric Manager V13.3.0以降の各バージョンレベルの“Systemwalker Centric Manager 解説書”の“ソフトウェア資源”を参照してください。

- 動作OS
- ソフトウェア条件

動作OS

以下のOSが対象のOSとなります。

Systemwalker Centric Manager V13.3.0

【Windows for Itanium版の場合】

インストール種別	動作OS	備考 (修正情報/パッチ番号)
運用管理サーバ 部門管理サーバ 業務サーバ	Microsoft(R) Windows Server(R) 2008 for Itanium-Based Systems	Service Pack 無/2

【Windows for Itanium以外のWindows版の場合】

インストール種別	動作OS	備考 (修正情報/パッチ番号)
運用管理サーバ	Microsoft(R) Windows Server(R) 2008 Standard(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x86)	Service Pack 無/2
部門管理サーバ 業務サーバ	Microsoft(R) Windows Server(R) 2008 Standard(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x86)	Service Pack 無/2

インストール種別	動作OS	備考 (修正情報/パッチ番号)
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard Server Core(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise Server Core(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能

Systemwalker Centric Manager V13.3.1 以降

【Windows for Itanium版の場合】

インストール種別	動作OS	備考 (修正情報/パッチ番号)
運用管理サーバ 部門管理サーバ 業務サーバ	Microsoft(R) Windows Server(R) 2008 for Itanium-Based Systems	Service Pack 無/2

【Windows for Itanium以外のWindows版の場合】

インストール種別	動作OS	備考 (修正情報/パッチ番号)
運用管理サーバ	Microsoft(R) Windows Server(R) 2008 Standard(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Foundation(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 R2 Foundation(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Standard(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Enterprise(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Datacenter(x64)	
部門管理サーバ /業務サーバ	Microsoft(R) Windows Server(R) 2008 Standard(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter(x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x86)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能

インストール種別	動作OS	備考 (修正情報/パッチ番号)
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core(x86)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Foundation(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter(x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (x64)	Service Pack 無/2
	Microsoft(R) Windows Server(R) 2008 Standard Server Core(x64) (注3)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core(x64)	Service Pack 無/2 業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 R2 Foundation(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Standard(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Enterprise(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Datacenter(x64)	
	Microsoft(R) Windows Server(R) 2008 R2 Standard Server Core(x64)	業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 R2 Enterprise Server Core(x64)	業務サーバだけ動作可能
	Microsoft(R) Windows Server(R) 2008 R2 Datacenter Server Core(x64)	業務サーバだけ動作可能

ソフトウェア条件

Systemwalker Centric Manager V13.3.0以降が必要です。

また、Systemwalker Centric Managerに以下の緊急修正を適用してください。

- Systemwalker Centric Manager V13.3.0,V13.3.1

  【Windows for Itanium版の場合】

  T001881IP-04を含む緊急修正

  【Windows for Itanium以外のWindows版の場合】

  T001846WP-04を含む緊急修正

- Systemwalker Centric Manager V13.4.0以降

  前提となる緊急修正はありません。

第2章 監視する

2.1 カスタム イベントログを監視する

Systemwalker Centric Managerのイベント監視機能でカスタ ムイベントログを監視する手順を説明します。

1. カスタム イベントログ名を確認する

カスタム イベントログの一覧を出力し、確認します。

2. イベント監視の定義をする

監視するカスタム イベントログ名をイベント監視に定義するための設定を行います。

2.2 カスタム イベントログを監視する方法

Systemwalker Centric Managerのイベント監視機能でカスタム イベントログを監視する設定方法を説明します。

1. カスタム イベントログ名を確認する

カスタム イベントログの監視を行いたいサーバ上で、カスタム イベントログ名を確認します。

1. [スタート]-[アクセサリ]-[コマンドプロンプト]を右クリックし、[管理者として実行]を選択します。

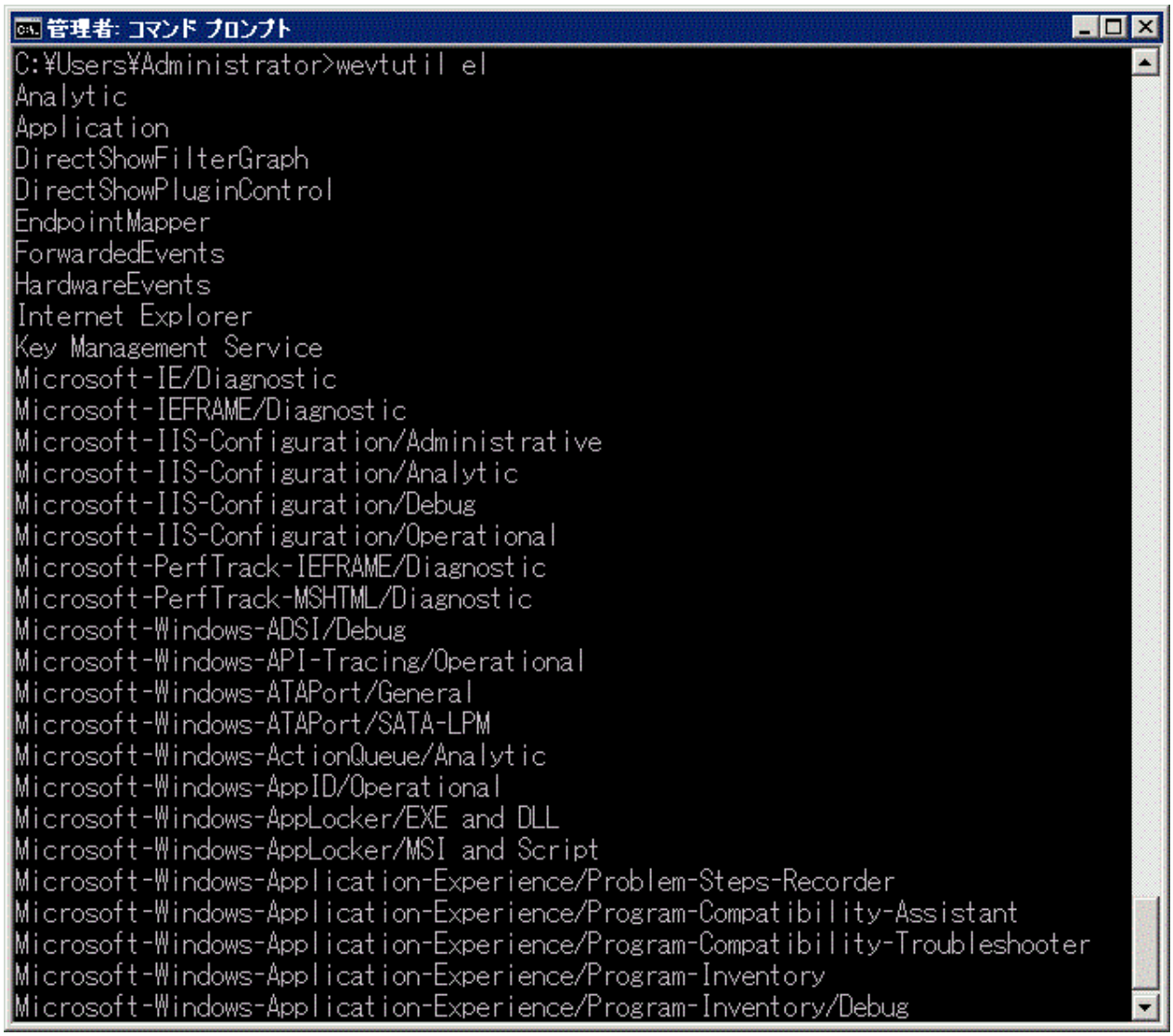
   →[管理者: コマンドプロンプト]が表示されます。

2. [管理者: コマンドプロンプト]で以下のコマンドを実行します。

   ```
   wevtutil.exe  el
   ```

3. 実行結果一覧から監視の対象とするカスタム イベントログ名を確認します。

   カスタム イベントログ名は、1行に表示されるすべての文字列が該当します。

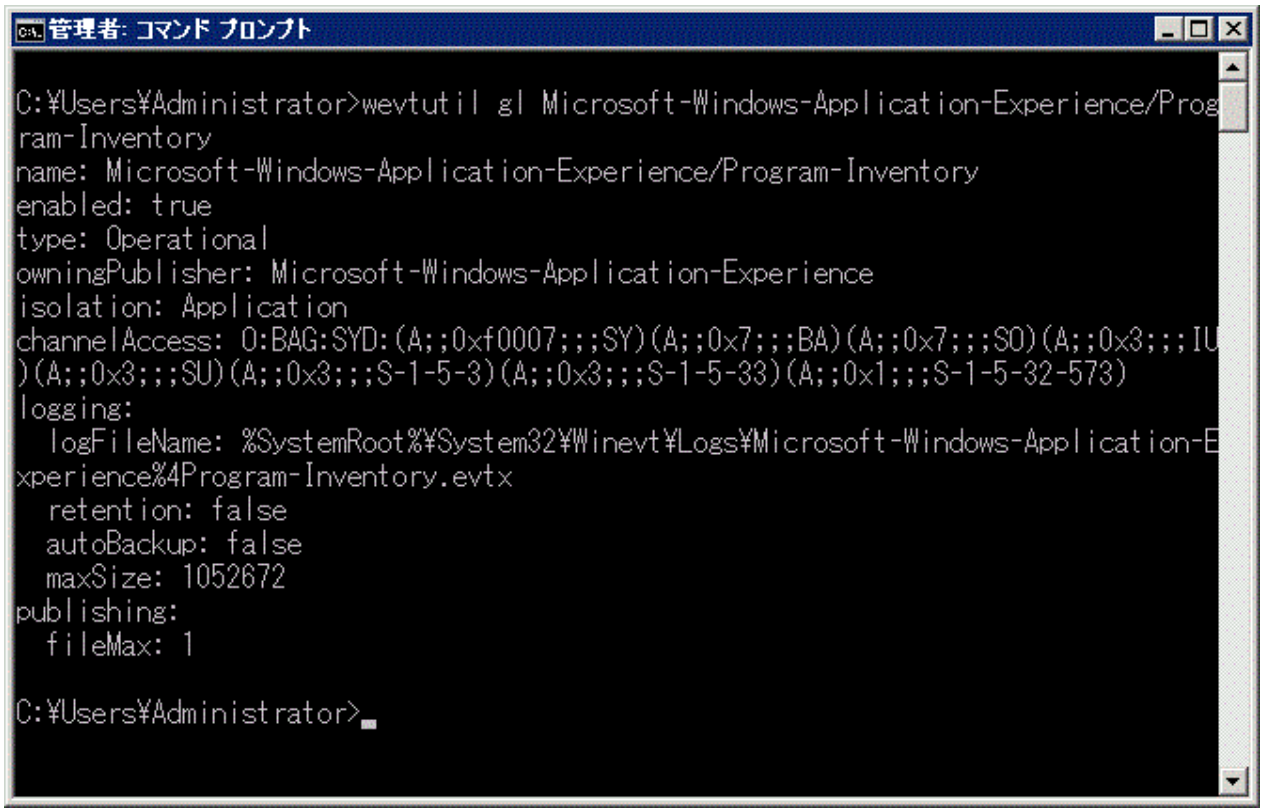


4. 監視対象とするカスタム イベントログの種類が監視対象にできるかを確認します。

   以下のコマンドを実行した結果、typeが“Admin”、または“Operational”と表示されるものが、監視可能なカスタム イベントログです。

```
wevtutil.exe  gl  カスタムイベントログ名
```

   例)
   “Microsoft-Windows-Application-Experience/Program-Inventory”を指定した場合の例です。
   typeに“Operational”と表示されたため、監視可能なカスタム イベントログであることが確認できます。



2. イベント監視の定義を設定する

監視するカスタム イベントログ名をイベント監視に定義するための設定を行います。

イベント監視の定義は、カスタム イベントログを監視するサーバで行います。

なお、“クラスタシステム上の運用管理サーバ、または部門管理サーバの場合【EE】”と“クラスタシステムではない、またはクラスタシステム上の業務サーバで起動する場合”で手順が異なります。

クラスタシステム上の運用管理サーバ、または部門管理サーバの場合【EE】

プライマリノードで定義を実施後、セカンダリノードで定義を行います。

その後、プライマリノード、セカンダリノードそれぞれでSystemwalker Centric Managerのサービスを起動します。

1. プライマリノードの定義を行います。

   a. Systemwalker Centric Managerを停止します。

   注意

   運用管理サーバと同じサーバに、Systemwalker Service Quality CoordinatorのManager、またはAgentを導入し、Systemwalker Centric ManagerのRDBシステム(RDBシステム名:CENTRIC)を性能監視している場合、Systemwalker Centric Managerを停止する前にSystemwalker Service Quality Coordinatorを停止し、Systemwalker Centric Manager RDBシステムの性能情報収集処理を停止してください。

   詳細については、Systemwalker Service Quality Coordinatorのマニュアルを参照してください。

   1. クラスタアドミニストレータで、Systemwalker Centric Manager のグループをオフラインにします。
   2. Systemwalker Centric Managerを停止するために、以下のコマンドを実行します。

```
pcentricmgr
```

b. Systemwalker Centric Managerで使用する共有ディスクの所有権を獲得し、オンライン化します。

本手順は、運用管理サーバをインストールしている環境の場合に必要な手順です。

それ以外の環境の場合は、手順1. のc.に進んでください。

なお、所有権の獲得方法/オンライン化の設定方法については、使用しているクラスタのマニュアルを参照してください。

c. コマンドプロンプトで滞留イベント初期化コマンドを実行します。

```
mpstayevtinit
```

d. 以下のファイルをテキストエディタで開きます。

```
Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpopagt¥etc¥opaevtlogkind
```

e. 監視するカスタム イベントログを以下の形式で追加します。

イベント監視の定義ファイルの形式:

```
カスタムイベントログ名<タブ>ラベル先頭2文字<タブ>監視イベント種別
```

カスタムイベントログ名:

"1. カスタム イベントログ名を確認する"で確認した、カスタム イベントログ名から追加するものを定義します。

ラベル先頭2文字:

Systemwalker Centric Managerがイベントログを読み込み、処理した時に付加されるラベル先頭2文字を半角英数字で2バイト定義します。

メッセージのラベルは、このラベルが利用され以下のとおりに組み立てられます。

ラベル:ソース名:

例)
ラベルがSYと定義されたイベントログにソース名Source1のメッセージが出力された場合のラベルは、以下のとおりです。

```
SY:Source1:
```

監視イベント種別:

該当のカスタム イベントログに出力されたイベントの監視イベント種別を定義します。

16バイト以下で定義します。

例)
"Microsoft-Windows-Application-Experience/Program-Inventory"のカスタム イベントログを定義する場合
opaevtlogkindファイル

```
Application AP アプリケーション
System SY システム
・・・
Microsoft-Windows-Hyper-V-Worker-Admin SY システム
Microsoft-Windows-Application-Experience/Program-Inventory  SY  アプリケーション
```

【条件】

- 文字コードは、Shift-JISで定義します。
- 1行1イベントログで定義します。
- 各項目区切り文字は必ずタブを使用します。半角空白は利用できません。

- 定義できるイベントログ数は50種類までです。

  なお、デフォルト定義で27種類が定義されているため、追加できるのは23種類のイベントログになります。

- 行の先頭に“#”がある場合はコメント行になります。

- 本定義ファイルは削除しないでください。

- 既存の定義は変更しないでください。OSのイベントログ監視ができなくなります。

- 本定義は、バージョンアップ、バックアップ・リストアの対象とはなっていません。バージョンアップ、バックアップ・リストア時には再設定してください。

- クラスタシステム上の運用管理サーバに定義する場合、プライマリとセカンダリノードの定義内容を同じにしてください。【EE】

2. セカンダリノードの定義を行います。

   a. Systemwalker Centric Managerを停止するために、以下のコマンドを実行します。

   ```
   pcentricmgr
   ```

   b. Systemwalker Centric Managerで使用する共有ディスクの所有権を獲得し、オンライン化します。

   本手順は、運用管理サーバをインストールしている環境の場合に必要な手順です。

   それ以外の環境の場合は、手順2. のc.に進んでください。

   なお、所有権の獲得方法/オンライン化の設定方法については、使用しているクラスタのマニュアルを参照してください。

   c. コマンドプロンプトで滞留イベント初期化コマンドを実行します。

   ```
   mpstayevtinit
   ```

   d. 以下のファイルをテキストエディタで開きます。

   ```
   Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpopagt¥etc¥opaevtlogkind
   ```

   e. 監視するカスタム イベントログを追加します。

   定義内容は、プライマリノードと同じ内容にします。

3. Systemwalker Centric Managerのサービスを起動します。

   a. 共有ディスクの所有権を獲得します。

   以下のリソースが所属するグループの所有権をプライマリノードで獲得します。

   獲得方法については、クラスタのマニュアルを参照してください。

   - Quorumディスク
   - Systemwalkerで使用する共有ディスク

   b. プライマリノードとセカンダリノードで、以下のコマンドを実行し、Systemwalker Centric Managerを起動します。

   ```
   scentricmgr
   ```

   c. クラスタアドミニストレータで、Systemwalker Centric Manager のグループをオンラインにします。

クラスタシステムではない、またはクラスタシステム上の業務サーバで起動する場合

1. Systemwalker Centric Managerを停止するために、以下のコマンドを実行します。

```
pcentricmgr
```

2. コマンドプロンプトで滞留イベント初期化コマンドを実行します。

```
mpstayevtinit
```

3. 以下のファイルをテキストエディタで開きます。

```
Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpopagt¥etc¥opaevtlogkind
```

4. 監視するカスタム イベントログを追加します。

   例)
   “Microsoft-Windows-Application-Experience/Program-Inventory”のカスタム イベントログを

   定義する場合
   opaevtlogkindファイル

```
Application AP アプリケーション
System SY システム
・・・
Microsoft-Windows-Hyper-V-Worker-Admin SY システム
Microsoft-Windows-Application-Experience/Program-Inventory  SY  アプリケーション
```

   定義の詳細については、“クラスタシステム上の運用管理サーバ、または部門管理サーバの場合【EE】”の“イベント監視の定義ファイルの形式”を参照してください。

5. Systemwalker Centric Managerを起動するために、以下のコマンドを実行します。

```
scentricmgr
```

第3章 ログ収集する

3.1 カスタム イベントログを収集する

Systemwalker Centric Managerの監査ログ管理機能でカスタム イベントログを収集する手順を説明します。

1. カスタム イベントログ名を確認する

   カスタム イベントログの一覧を出力し、確認します。

2. 監査ログの収集を設定する

   収集したいカスタム イベントログのログ収集を設定します。

3. 監査ログを収集する

   カスタム イベントログを収集します。

3.2 カスタム イベントログを収集する方法

Systemwalker Centric Managerの監査ログ管理機能でカスタム イベントログを収集する設定方法を説明します。

1. カスタム イベントログ名を確認する

カスタム イベントログの収集を行いたいサーバ上で、カスタム イベントログ名を確認します。

1. [スタート]-[アクセサリ]-[コマンドプロンプト]を右クリックし、[管理者として実行]を選択します。

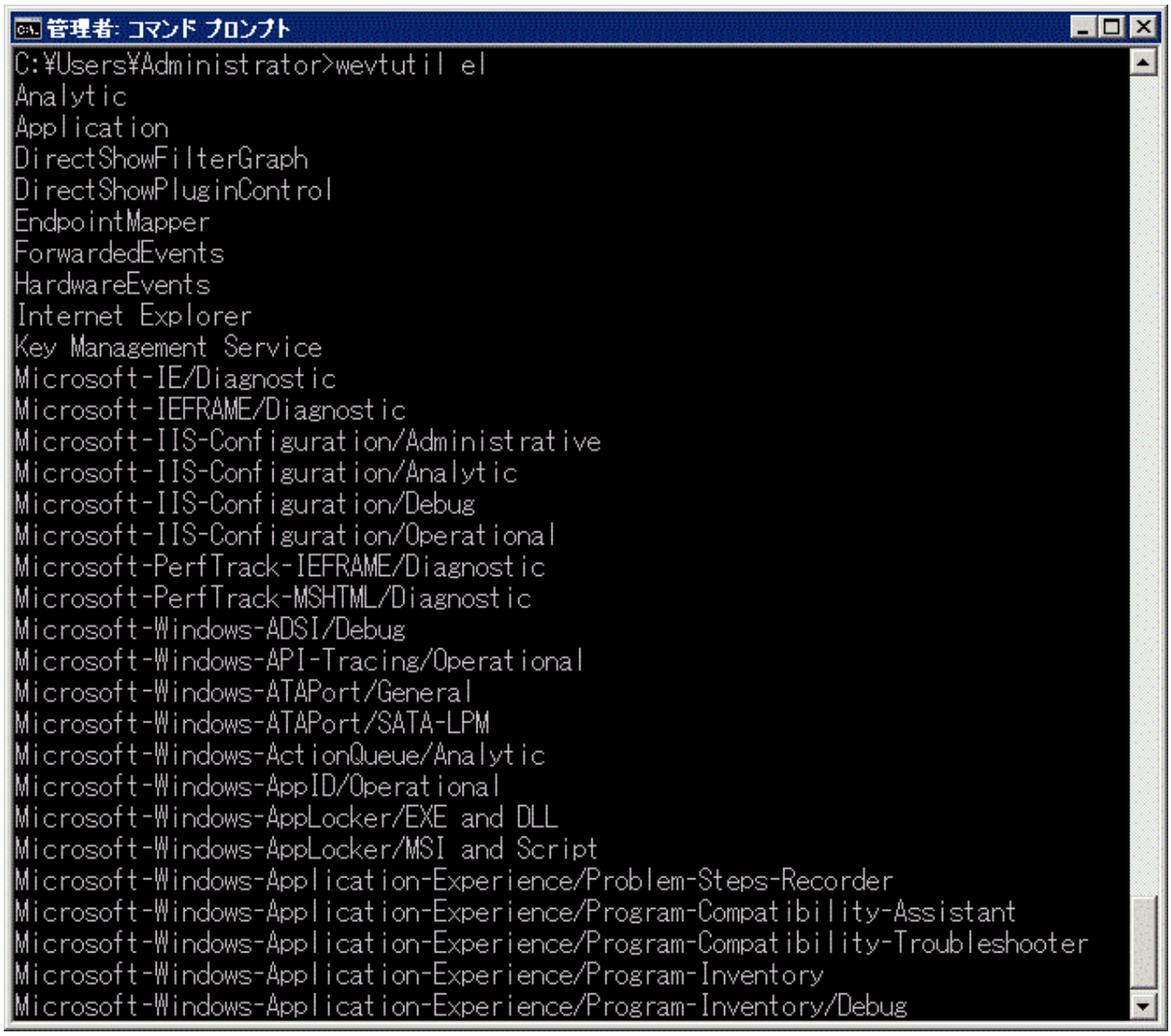
   →[管理者: コマンドプロンプト]が表示されます。

2. コマンドプロンプトで以下のコマンドを実行します。

   ```
   wevtutil.exe el
   ```

3. 実行結果一覧から監査ログ収集するカスタム イベントログ名を確認します。

   カスタム イベントログ名は、1行に表示されるすべての文字列が該当します。

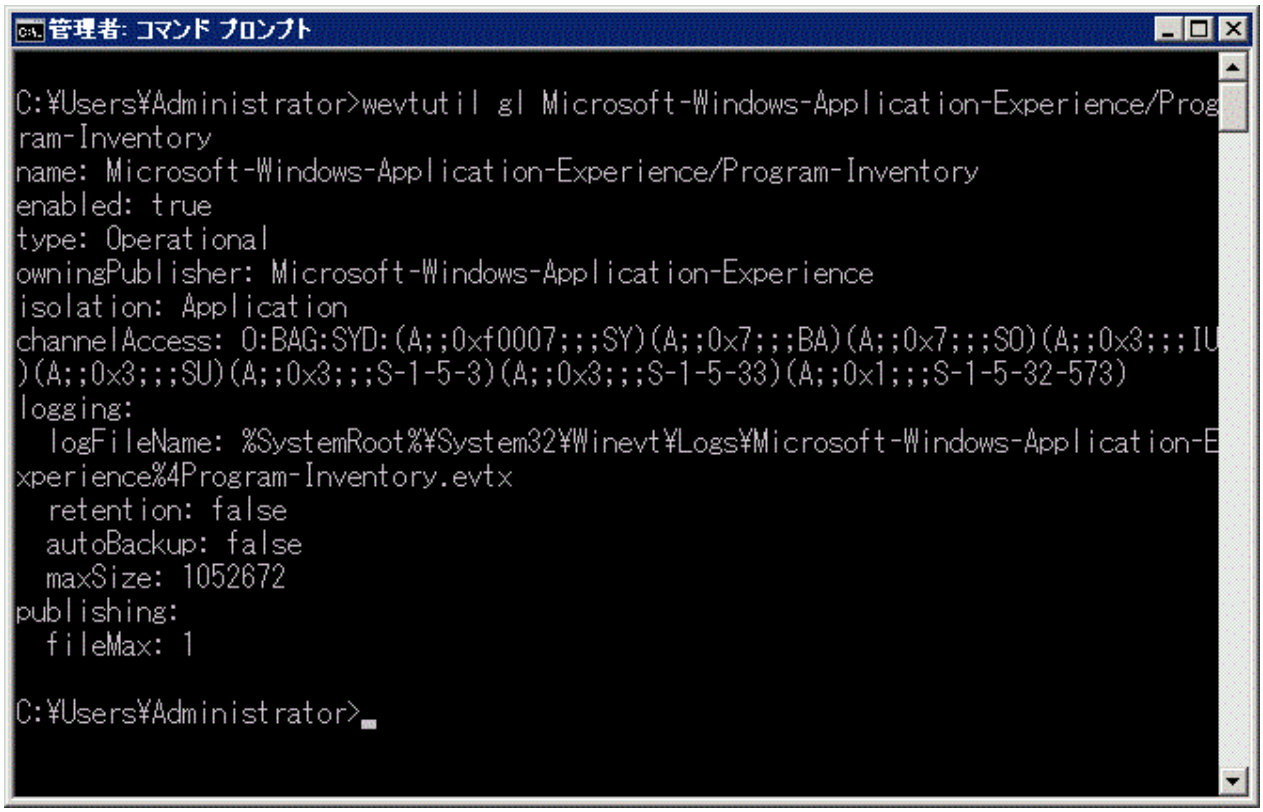


4. 監視対象とするカスタム イベントログの種類が収集できるかを確認します。

   以下のコマンドを実行した結果、typeが“Admin”、または“Operational”と表示されるものが、収集可能なカスタム イベントログです。

```
wevtutil.exe  gl  カスタムイベントログ名
```

   例)
   “Microsoft-Windows-Application-Experience/Program-Inventory”を指定した場合の例です。
   typeに“Operational”と表示されたため、収集可能なカスタム イベントログであることを確認できます。



2. 監査ログの収集を設定する

収集するカスタム イベントログをログ収集するための設定を行います。ログ収集の設定は、収集対象サーバで行います。

1. 以下のファイルをテキストエディタで開きます。

Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpatm¥etc¥mpatm_eventlog.def

2. 収集するカスタム イベントログのログ識別名とカスタム イベントログ名を以下の形式で追加します。

ログ識別名<タブ>カスタムイベントログ名

   ログ識別名:

   “EventLog”で始まる文字列を、ASCII(80文字以内)で指定します。

   半角英数字、および“-”(ハイフン)以外の文字列を指定しないでください。

   カスタムイベントログ名:

   “1. カスタム イベントログ名を確認する”で確認した、カスタム イベントログ名から追加するものを定義します。

   【条件】

   - 文字コードは、Shift-JISで定義します。
   - 1行1イベントログで定義します。
   - 各項目区切り文字は必ずタブを使用します。半角空白は利用できません。
   - 本定義ファイルは削除しないでください。
   - 既存の定義は変更しないでください。OSのイベントログ収集ができなくなります。
   - 本定義は、バージョンアップ、バックアップ・リストアの対象とはなっていません。バージョンアップ、バックアップ・リストア時には再設定してください。

例)
“Microsoft-Windows-Application-Experience/Program-Inventory”のカスタム イベントログを定義する場合
mpatm_eventlog.defファイル

```
EventLogApplication Application
EventLogSystem System
…
EventLogHVWAdmin Microsoft-Windows-Hyper-V-Worker-Admin
NREventLog Security
EventLogMWAEPI  Microsoft-Windows-Application-Experience/Program-Inventory
```

3. mpatmlogapdef(ログ収集設定コマンド)により、ログ収集の定義を行います。

   mpatmlogapdef(ログ収集設定コマンド)の詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

   例)
   “Microsoft-Windows-Application-Experience/Program-Inventory”のカスタム イベントログを定義する場合

```
mpatmlogapdef ADD -A EventLogMWAEPI -L  “Systemwalkerインストールディレクトリ¥MPWALKER.DM
¥mpatm¥EventLog¥EventLogMWAEPI”
```

   【条件】

   ー ログ識別名は、手順2で追加した文字列を指定してください。

   ー ログファイル名は、イベントログを出力する任意の一時ファイル名を指定してください。

   ただし、一時ファイル名のパスは存在する必要があります。

   ー 日付書式定義ファイル名は、ログ識別名に“EventLog”で始まる文字列を指定することにより、“mpatmevt.fmt”がデフォルト定義されます。

3. 監査ログを収集する

監査ログを運用管理サーバで収集します。

ログ収集の詳細については、“Systemwalker Centric Manager 使用手引書 セキュリティ編”の“監査ログを収集する”を参照してください。

第4章 ログ分析する

4.1 カスタム イベントログを分析する

Systemwalker Centric Managerの監査ログ分析機能でカスタムイベントログを分析する手順を説明します。

なお、“ログ収集する”で収集したカスタム イベントログを分析します。

1. 監査ログの分析を設定する

分析したいカスタム イベントログのログ分析を設定します。

2. 監査ログを分析する

カスタム イベントログを分析します。

4.2 カスタム イベントログを分析する方法

Systemwalker Centric Managerの監査ログ分析機能でカスタム イベントログを分析する設定方法を説明します。

1. 監査ログの分析を設定する

カスタム イベントログをログ分析するための設定を行います。ログ分析の設定は、運用管理サーバ、および運用管理クライアントで行います。

1. 運用管理サーバ上で、正規化ルール定義ファイルをコピーし、mpatarulectl(正規化ルール管理コマンド)を利用して登録します。mpatarulectl(正規化ルール管理コマンド)の詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

   例)
   “Microsoft-Windows-Application-Experience/Program-Inventory”のカスタム イベントログを

   分析する場合
   【Windows】

   ```
   cd Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpata¥etc¥rule
   copy mpatarule_EventLogApplication.ini mpatarule_EventLogMWAEPI.ini
   mpatarulectl -A mpatarule_EventLogMWAEPI.ini
   ```

   【Solaris/Linux】

   ```
   cd /etc/opt/FJSVmpata/etc/rule
   cp mpatarule_EventLogApplication.ini mpatarule_EventLogMWAEPI.ini
   /opt/systemwalker/bin/mpatarulectl -A mpatarule_EventLogMWAEPI.ini
   ```

   ログ識別名は、“監査ログの収集を設定する”の手順2で追加した文字列を指定してください。

2. 運用管理サーバ上の以下の問い合わせサンプルファイルを、運用管理クライアント上の任意のディレクトリにバイナリファイルとしてコピーします。

   【Windows】

運用管理サーバ上のファイル格納ディレクトリ	サンプルファイル名
Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpata¥sample¥total	DayOfWeek.RNE
	EachTimeSlot.RNE
	ExecutionHost.RNE

運用管理サーバ上のファイル格納ディレクトリ	サンプルファイル名
	LogType.RNE
	severity.RNE

【Solaris/Linux】

運用管理サーバ上のファイル格納ディレクトリ	サンプルファイル名
/etc/opt/FJSVmpata/sample/total	DayOfWeek.RNE
	EachTimeSlot.RNE
	ExecutionHost.RNE
	LogType.RNE
	severity.RNE

3. 運用管理クライアント上で、コピーした各問い合わせサンプルファイルをInterstage Navigatorクライアントで開き、条件の[ログ種別]にログ識別名を追加し、保存します。

   条件の追加方法の詳細については、“Systemwalker Centric Manager 使用手引書 セキュリティ編”の“問い合わせサンプルファイルを編集する”を参照してください。

4. 運用管理クライアント上で保存した各問い合わせサンプルファイルを、運用管理サーバの以下のディレクトリにコピーします。

   【Windows】

   ```
   Systemwalkerインストールディレクトリ¥MPWALKER.DM¥mpata¥data¥total
   ```

   【Solaris/Linux】

   ```
   /etc/opt/FJSVmpata/data/total
   ```

2. 監査ログを分析する

監査ログを運用管理サーバで分析します。

ログ分析の詳細については、“Systemwalker Centric Manager 使用手引書 セキュリティ編”の“監査ログを分析する”を参照してください。なお、[監査ログ分析－検索]画面で追加したカスタム イベントログの監査ログを検索する場合、[検索条件の設定]の[ログ種別]の[候補一覧]に、ログ識別名がすべて小文字で表示されます。

例)
ログ識別名が“EventLogMWAEPI”の場合、[検索条件の設定]の[ログ種別]の[候補一覧]に“eventlogmwaepi”と表示されます。