

vm2 - Microsoft Azure x AZ-500JA-AzureSecurityTech x event tracing for windows etw x Windows カウンター データを取 x Windows イベント トレーシング x ストレージ アカウント ログ - Mic x

https://portal.azure.com/#@se109workoutlook.onmicrosoft.com/resource/subscriptions/c713fe0c-2617-4d8d-a25a-e788c3fa840c/resourceGroups/MOD2RG/providers/Microsoft.Compute/virtualMac...

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > vm2

vm2 | 診断設定
仮想マシン

検索 (Cmd+/)

バックアップ
ディザスター リカバリー
更新プログラム
インベントリ
変更の追跡
構成管理 (プレビュー)
ポリシー
実行コマンド

監視

分析情報
警告
メトリック
診断設定
ログ
接続モニター (クラシック)
ブック

オートメーション

タスク (プレビュー)
テンプレートのエクスポート

ヘルプ

リソース正常性

保存 破棄

概要 パフォーマンス カウンター ログ クラッシュ ダンプ シンク エージェント

パフォーマンス カウンター

次のカウンターについてデータを収集しています:

- CPU
- メモリ
- ディスク
- ネットワーク

パフォーマンス カウンターを構成する

イベント ログ

次のログについてデータを収集しています:

- アプリケーション: 重大, エラー, 警告
- セキュリティ: 監査の失敗
- システム: 重大, エラー, 警告, 情報, 詳細

イベント ログを構成する

ディレクトリ

構成されていません。

ディレクトリを構成する

クラッシュ ダンプ

メモリ ダンプを収集しません。

クラッシュ ダンプの構成

シンク

診断データはどのシンクにも送信されていません。
シンクを構成する

エージェント

診断データはこのストレージ アカウントに送信されています:

OS内部のパフォーマンスデータ
取得設定
VMの診断設定を選択

vm2 - Microsoft Azure x AZ-500JA-AzureSecurityTech x event tracing for windows etw x Windows カウンター データを取 x Windows イベント トレーシング x ストレージ アカウント ログ - Mic x +

https://portal.azure.com/#@se109workoutlook.onmicrosoft.com/resource/subscriptions/c713fe0c-2617-4d8d-a25a-e788c3fa840c/resourceGroups/MOD2RG/providers/Microsoft.Compute/virtualMac... A ☆ ☆ 8 se109work@outlook.jp 既定のディレクトリ

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+/)

ホーム > vm2

vm2 | 診断設定

仮想マシン

検索 (Cmd+/) <

- バックアップ
- ディザスター リカバリー
- 更新プログラム
- インベントリ
- 変更の追跡
- 構成管理 (プレビュー)
- ポリシー
- 実行コマンド

監視

- 分析情報
- 警告
- メトリック
- 診断設定
- ログ
- 接続モニター (クラシック)
- ブック

オートメーション

- タスク (プレビュー)
- テンプレートのエクスポート

ヘルプ

- リソース正常性

ディレクトリ

収集する IIS ログと監視するログ ディレクトリを選びます。

IIS ログ ① ☐

ストレージ コンテナ名: ①

失敗した要求のログ ① ☐

ストレージ コンテナ名: ①

アプリケーション ログ

.NET アプリケーションによって生成されるトレース出力を収集します。

☒ 無効 ☐ 有効

Windows イベント トレーシング (ETW) イベント

指定するイベント ソースとマニフェストから生成される ETW データを収集します。

☐ 無効 ☒ 有効

イベント ソース

プロバイダー クラス	ログ レベル
<ソース名>	すべて ▼ ...

イベント ソースは指定されていません。

イベント マニフェスト

ETWイベントを有効

vm2 - Microsoft Azure | AZ-500JA-AzureSecurityTech | event tracing for windows etw | Windows カウンター データを取 | Windows イベント トレーシング | ストレージ アカウント ログ - Mic |

https://portal.azure.com/#@se109workoutlook.onmicrosoft.com/resource/subscriptions/c713fe0c-2617-4d8d-a25a-e788c3fa840c/resourceGroups/MOD2RG/providers/Microsoft.Compute/virtualMac...

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

se109work@outlook.jp | 既定のディレクトリ

vm2 | 診断設定

仮想マシン

検索 (Cmd+/) << 保存 破棄

バックアップ
ディザスター リカバリー
更新プログラム
インベントリ
変更の追跡
構成管理 (プレビュー)
ポリシー
実行コマンド

監視

分析情報
警告
メトリック
診断設定
ログ
接続モニター (クラシック)
ブック

オートメーション

タスク (プレビュー)
テンプレートのエクスポート

ヘルプ

リソース正常性

概要 パフォーマンス カウンター ログ クラッシュ ダンプ シンク エージェント

Azure Diagnostics エージェントの追加のオプションを構成します。

ストレージ アカウント *

mod2rgguestdiag

ディスク クォータ (MB)

5120

診断インフラストラクチャのログ:

無効 有効

ログレベル: ①

すべて

Azure Diagnostics エージェントの削除

診断データが収集されない場合や、ポータルで正しく表示されない場合は、エージェントを再インストールすると役立つことがあります。

エージェントは削除されますが、ストレージ アカウント内の既存の診断データはすべて保持されます。エージェントが削除された後に、この仮想マシンに対する診断を再有効化できます。

削除

このストレージアカウントをLog Analytics ワークスペースに接続する

ログレベルをエラー → すべて

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)






se109work@outlook.jp
既定のディレクトリ

ホーム > Log Analytics ワークスペース > logse109 >

ストレージ アカウント ログ

Log Analytics ワークスペース

+ 追加 📄 ドキュメント

名前	データ型	ソース	Log Analytics 接続
 az500lab131415guestdi799	イベント	WADWindowsEventLogsTable	✔ 接続済み
 az500lab131415guestdi799	ETW ログ	WADETWEventTable	✔ 接続済み
 az500lab131415guestdi799	Service Fabric イベント	WADServiceFabric*EventTable	✔ 接続済み
 mod2rgguestdiag	イベント	WADWindowsEventLogsTable	✔ 接続済み
 mod2rgguestdiag	ETW ログ	WADETWEventTable	✔ 接続済み

Log Analytics ワークスペースから先程
のストレージアカウントを接続設定する