



[Tech Support]

- [テクニカル サポートおよびシステム ログ \(1 ページ\)](#)
- [システム ログのダウンロード \(2 ページ\)](#)
- [外部アナライザへのストリーミング システム ログ \(2 ページ\)](#)

テクニカル サポートおよびシステム ログ

Cisco Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

追加のツールを使用して重要なイベントを遅延なく迅速に解析、表示、応答する必要がある場合は、いつでも、ログをダウンロードするか、Splunk などの外部ログ アナライザにストリーミングするかを選択できます。

テクニカル サポートログは次の 2 つの部分に分割されています。

- 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ ファイル
- 可読性を高めた、JSON ベースのデータベース バックアップ

各バックアップ アーカイブには、次の内容が含まれています。

- `xxxx` : バックアップ時に使用可能なコンテナ ログ用の `xxxx` 形式の 1 つ以上のファイル。
- `msc-backup-<date>_temp` : 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ。
- `msc-db-json-<date>_temp` : JSON 形式のバックアップ コンテンツ。

例 :

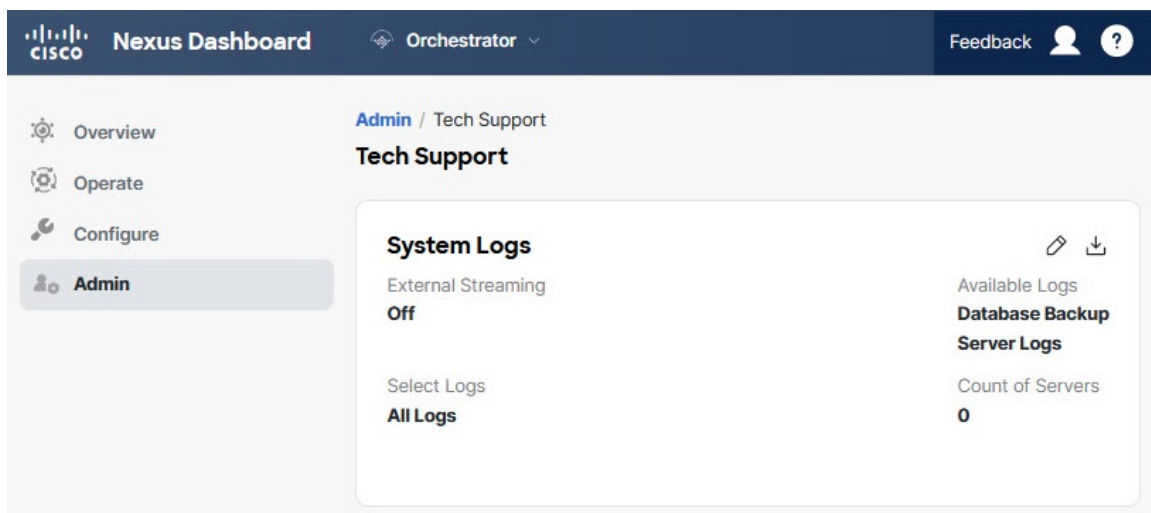
```
msc_anpEpgRels.json
msc_anpExtEpgRels.json
msc_asyncExecutionStatus.json
msc_audit.json
msc_backup-versions.json
msc_backupRecords.json
msc_ca-cert.json
msc_cloudSecStatus.json
msc_consistency.json
...
```

システム ログのダウンロード

このセクションでは、Cisco Nexus Dashboard Orchestrator により管理されているすべてのスキーマ、サイト、テナント、およびユーザのトラブルシューティングレポートとインフラストラクチャ ログ ファイルを生成します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [システムログ (System Logs)] 画面を開きます。



- メインメニューで、[管理 (Admin)] > [ソフトウェア管理 (Software Management)] を選択します。
- [システム ログ (System Logs)] フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 [ログのダウンロード (Download Log)] ボタンをクリックしてログをダウンロードします。

アーカイブがシステムにダウンロードされます。この章の最初のセクションで説明されているすべての情報を含んでいます。

外部アナライザへのストリーミング システム ログ

Cisco Nexus Dashboard Orchestrator を使用すると、Orchestrator ログを外部のログアナライザーツールにリアルタイムで送信できます。生成されたイベントをストリーミングすることにより、追加のツールを使用して、遅延なしで重要なイベントをすばやく解析、表示、および対応できます。

ここでは、Cisco Nexus Dashboard Orchestrator が外部アナライザーツール (Splunk や syslog など) にログをストリーミングできるようにする方法について説明します。

始める前に

- このリリースでは、外部ログアナライザとして Splunk と syslog のみがサポートされています。
- このリリースでは、Application Services Engine 展開で Cisco Nexus Dashboard Orchestrator の syslog のみがサポートされます。
- このリリースは、最大 5 台の外部サーバ0をサポートします。
- Splunk を使用する場合は、ログアナライザ サービス プロバイダをセットアップして構成します。

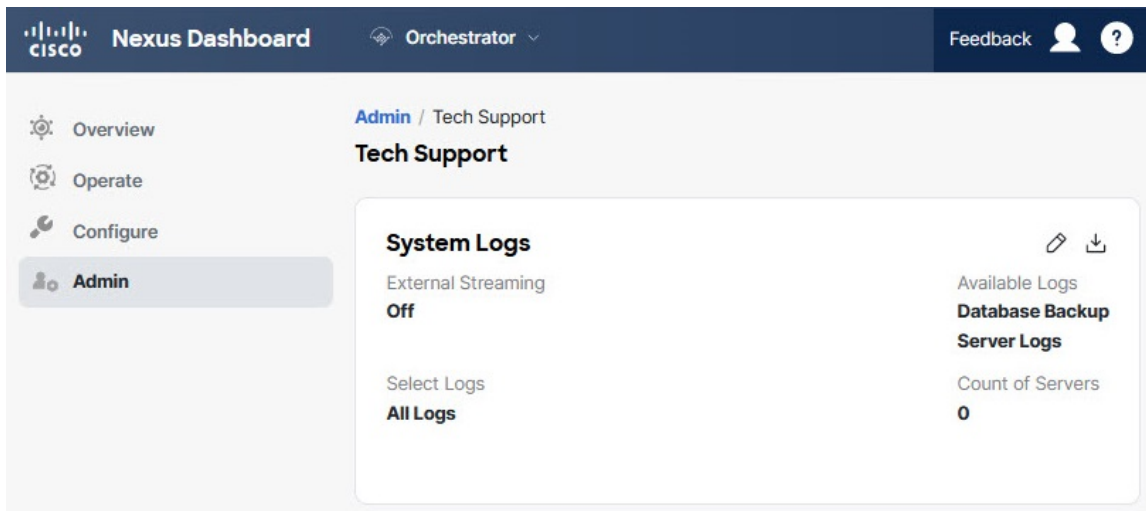
外部ログアナライザの設定方法の詳細については、マニュアルを参照してください。

- Splunk を使用する場合は、サービス プロバイダの認証トークンを取得します。

分裂サービスの認証トークンの取得については、「分裂」のマニュアルで詳しく説明していますが、要するに、[設定 (Settings)] > [データ入力 (Data Inputs)] > [HTTP イベントコレクタ (Data input HTTP Event Collector)]を選択し、[新規トークン (New token)]をクリックして、認証トークンを取得できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [管理 (Admin)]、[テクニカルサポート (Tech Support)]、[システムログ (System Logs)] 画面を開きます。



- a) メインメニューで、[管理 (Admin)] > [ソフトウェア管理 (Software Management)] を選択します。
- b) [システム ログ (System Logs)] フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 [システムログ (System Logs)] ウィンドウで、外部ストリーミングを有効にし、サーバを追加します。

System Logs ×

External Streaming a

Select Logs

All Logs Audit Logs b

Logging Servers ⓘ * c

Server Type	Protocol	Host	Port
+ Add Server			

Save

- a) **外部ストリーミング (External Streaming)** ノブを有効にします。
- b) **すべてのログ (All Logs)** をストリーミングするか、**監査ログ (Audit Logs)** のみをストリーミングするかを選択します。
- c) **サーバーの追加 (Add Server)** をクリックして、外部ログ アナライザー サーバーを追加します。

ステップ 4 Splunk サーバーを追加します。

Splunk サービスを使用する予定がない場合は、この手順をスキップします。

The screenshot shows the 'Logging Servers' configuration interface. At the top, there is a table header with columns: 'Server Type', 'Protocol', 'Host', and 'Port'. Below the header, the 'Select Service' dropdown is set to 'splunk' (callout a). The 'Protocol' section has 'HTTP' and 'HTTPS' buttons, with 'HTTP' selected (callout b). The 'Host' field is empty (callout c). The 'Port' dropdown is set to '8088' (callout c). The 'Token' field contains 'ddd' (callout c). The 'Index' dropdown is set to 'main' (callout d). At the bottom right, there are 'Cancel' and 'Save' buttons (callout d). Below the form, there is an '+ Add Server' button and a 'Save' button.

- a) サーバーのタイプとして [Splunk] を選択します。
- b) プロトコルを選択します。
- c) Splunk サービスから取得したサーバ名または IP アドレス、ポート、および認証トークンを入力します。

Splunk サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、要するに、[設定 (Settings)] > [データ入力 (Data Inputs)] > [HTTP イベントコレクタ (HTTP Event Collector)] を選択し、[新規トークン (New token)] をクリックして、認証トークンを取得できます。

- d) チェックマーク アイコンをクリックして、サーバの追加を終了します。

ステップ 5 syslog サーバーを追加します。

syslog を使用しない場合は、この手順をスキップします。

System Logs

✕

Logging Servers ⓘ *

Server Type	Protocol	Host	Port
Select Service			
<input type="text" value="syslog"/>			
Protocol			
<input type="radio"/> TCP <input checked="" type="radio"/> UDP			
Host *			
<input type="text" value="10.30.11.69"/>			
Port *			
<input type="text" value="8088"/>			
Severity			
<input type="text" value="Alert"/>			
TLS			
<input type="checkbox"/>			
<input type="button" value="Cancel"/> <input type="button" value="Save"/>			
+ Add Server			

- サーバーのタイプとして [syslog] を選択します。
- プロトコルを選択します。
- サーバー名またはIPアドレス、ポート番号、およびストリーミングするログメッセージのシビラティ（重大度）を指定します。
- チェックマークアイコンをクリックして、サーバーの追加を完了します。

ステップ 6 複数のサーバーを追加する場合は、この手順を繰り返します。

このリリースは、最大 5 台の外部サーバ0をサポートします。

ステップ 7 [保存 (Save)] をクリックして、変更内容を保存します。

System Logs ×

Download Logs
[Download](#)

External Streaming

Select Logs
[All Logs](#) [Audit Logs](#)

* Logging Servers ⓘ

Server Type	Protocol	Host	Port	
splunk	http	10.30.11.69	8088	✖
syslog	tcp	10.195.223.220	514	✖

[+ Add Server](#)

[SAVE](#)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。