



システムロギングの設定

表 1: 機能の履歴

機能名	リリース情報	説明
TLS 経由で Syslog メッセージを送信する機能	Cisco IOS XE リリース 17.2.1r	この機能を使用すると、Transport Layer Security (TLS) 接続を確立することにより、syslog メッセージを外部の設定済みホストに転送できます。TLS プロトコルを使用すると、ホップごとに、syslog メッセージの内容の機密性、安全性を保ち、改ざんや変更を防ぐことができます。

- [システムロギング \(1 ページ\)](#)
- [Syslog メッセージの形式、Syslog メッセージのレベル、およびシステムログファイル \(2 ページ\)](#)
- [Syslog メッセージの送信に TLS を使用する利点 \(6 ページ\)](#)
- [TLS のサーバー認証でのロギングの設定 \(6 ページ\)](#)
- [TLS の相互認証でのロギングの設定 \(7 ページ\)](#)
- [サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール \(7 ページ\)](#)
- [サーバー認証のために Syslog サーバーにルート認証局をインストール \(9 ページ\)](#)
- [相互認証のために Cisco IOS XE SD-WAN デバイスに Syslog ルート証明書をインストール \(10 ページ\)](#)
- [Cisco vManage を使用したロギング機能テンプレートの設定 \(11 ページ\)](#)
- [機能証明書署名要求の生成と機能証明書のインストール \(19 ページ\)](#)
- [Cisco IOS XE SD-WAN デバイスでのトラストポイント設定の確認 \(20 ページ\)](#)
- [Cisco vManage NMS 監査ログの Syslog サーバーへのエクスポート \(21 ページ\)](#)

システムロギング

システムロギング操作では、UNIX の syslog コマンドと同様のメカニズムを使用して、オーバーレイネットワーク内の Cisco SD-WAN デバイスで発生するシステム全体の高レベルの操作が記録されます。メッセージのログレベル (優先順位) は、標準の UNIX コマンドのログレベ

ル（優先順位）と同じです。また、syslogメッセージの優先順位を設定できます。Cisco SD-WAN デバイスは、UNIX スタイルの syslog サービスにログメッセージを送信できます。

Cisco IOS XE SD-WAN デバイスは、TCP および UDP を使用して、構成された外部ホスト上の syslog サーバーに syslog メッセージを送信します。これらのデバイスが syslog メッセージを送信している場合、メッセージは出力先に到達するためにいくつかのホップを通過する場合があります。ホップ中の中間ネットワークは、信頼できないか、別のドメインにあるか、セキュリティレベルが異なる可能性があります。このため Cisco IOS XE SD-WAN デバイスでは、RFC5425 に従って Transport Layer Security (TLS) を介した安全な syslog メッセージの送信をサポートするようになりました。潜在的な改ざんから syslog メッセージの内容を保護するために、証明書交換、相互認証、および暗号ネゴシエーションに TLS プロトコルが使用されます。

Cisco IOS XE SD-WAN デバイスは、TLS 経由で syslog メッセージを送信するための相互認証とサーバー認証の両方をサポートします。

Syslog メッセージの形式、Syslog メッセージのレベル、およびシステムログファイル

syslog メッセージ形式

Syslog メッセージはパーセント記号 (%) で始まり、syslog メッセージの形式は次のとおりです。

- Syslog メッセージ形式

seq no:timestamp: %facility-severity-MENEMONIC:description (hostname-n)

- RFC5424 に基づく Syslog メッセージ形式

<pri>ver timestamp hostname appname procid msgid structured data description/msg



(注) RFC5424 に基づく syslog メッセージ形式では、hostname、appname、procid、msgid、structured data などのオプションフィールドは - で指定されます。

syslog メッセージのフィールドの説明は次のとおりです。

表 2: Syslog メッセージ形式のフィールドの説明

フィールド	説明
facility	ロギングファシリティを 20 以外の値に設定します。これは、UNIX システムで想定されています。

フィールド	説明
シビラティ (重大度)	メッセージの重要度または重大度は、0 から 7 までの数値コードによって分類されます。この範囲で数値が小さいほど、システム状態の重大度が高いことを示します。
msg または description	syslog サーバーの状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、インターフェイス名、ポート番号、またはユーザー名が含まれていることがあります。 RFC5424 に基づく syslog メッセージ形式では、description は次を表します。 %facility-severity-MENEMONIC:description

通常、syslog メッセージの前には余分なテキストが付きます。

- プライオリティ値、シーケンス番号、およびタイムスタンプが前に付いたシステムロギングメッセージの例を以下に示します。

```
<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to administratively down
```

- RFC5424 に基づく、プライオリティ値、syslog プロトコル仕様のバージョン、およびタイムスタンプが前に付いたシステムロギングメッセージの例を次に示します。

```
<45>1 2003-10-11T22:14:15.003Z 10.64.48.125 polaris-user1 --- %LINK-5-CHANGED: Interface
GigabitEthernet0/0, changed state to administratively down
```



- (注) タイムスタンプの形式は、両方の syslog メッセージ形式で同じではありません。RFC5424 に基づくメッセージ形式では、T と Z は必須で、T は区切りを表し、Z はゼロタイムゾーンを表します。

Syslog メッセージのレベル

すべての syslog メッセージは、保存する syslog メッセージの重大度を示す優先度に関連付けられています。デフォルトのプライオリティ値は「informational」であるため、デフォルトでは、すべての syslog メッセージが記録されます。優先度には、次のいずれかを指定でき、順に重大度が下がります。

- [Emergency] : システムは使用できません (syslog 重大度 0 に対応)。
- [Alert] : ただちに対応するようにします (syslog 重大度 1 に対応)。
- [Critical] : 重大な状態 (syslog 重大度 2 に対応)。
- [Error] : システムのユーザビリティを完全に損なわないエラー状態 (syslog 重大度 3 に対応)。

- [Warning] : 軽微なエラー状態 (syslog 重大度 4 に対応)。
- [Notice] : 正常だが重大な状態 (syslog 重大度 5 に対応)。
- [Informational] : ルーチンの状態 (デフォルト) (syslog 重大度 6 に対応)。
- [Debug] : syslog 重大度 7 に対応するデバッグメッセージを発行します。

システムのログファイル

デフォルトまたは設定されたプライオリティ値以上のすべての syslog メッセージは、syslog サーバーのローカルデバイスの /var/log ディレクトリ内にあるいくつかのファイルに記録されます。ログファイルの内容は次のとおりです。

- auth.log : ログイン、ログアウト、スーパーユーザーのアクセスイベント、および認可システムの使用状況
- kern.log : カーネルメッセージ
- messages.log : すべてのソースからの syslog メッセージが記録された統合ログファイル。
- vconfd.log : 設定に関するすべての syslog メッセージ
- vdebug.log : デバッグ機能が有効になっているモジュールのすべてのデバッグメッセージ、およびデフォルトのプライオリティ値を超えるすべての syslog メッセージ。デバッグログメッセージは、モジュールに基づいてさまざまなレベルのログギングをサポートします。実装されているログギングレベルは、モジュールごとに異なります。たとえば、システムマネージャ (sysmgr) には 2 つのログギングレベル (オンとオフ) があり、シャーシマネージャ (chmgr) には 4 つの異なるログギングレベル (オフ、低、標準、高) があります。デバッグメッセージをリモートホストに送信することはできません。そのため、デバッグを有効にするには、**debug** 操作コマンドを使用します。
- vsyslog.log : 設定されたプライオリティ値を超える Cisco SD-WAN プロセス (デーモン) からのすべての syslog メッセージ。デフォルトのプライオリティ値は「informational」であるため、デフォルトでは「notice」、「warning」、「error」、「critical」、「alert」、および「emergency」のすべての syslog メッセージが保存されます。
- vmanage-syslog.log : Cisco vManage NMS 監査ログメッセージ

以下は、Cisco SD-WAN が使用しない標準の LINUX ファイルであり、/var/log ディレクトリにあります。

- cron.log
- debug.log
- lpr.log
- mail.log
- syslog

syslog ファイルに送信されるメッセージはレート制限されていないため、次のようになります。

- 各 syslog ファイルには、最大 16 MB のサイズ容量で 10 個のログファイルのストレージ制限が設定されています。
 - ストレージ容量が 16 MB のサイズ制限を超えると、ログファイルは日付が付けられて .GZ ファイルとして保存されます。
 - ストレージの制限が 10 個のログファイルを超えると、最も古いログファイルがドロップされます。
- 短時間に多くの syslog メッセージが生成された場合、オーバーフローメッセージはバッファに入れられ、syslog ファイルに保存するためのキューに入れられます。

syslog メッセージが繰り返された場合、つまり連続して同一メッセージが複数回発生した場合、メッセージは 1 回だけ syslog ファイルに記録されます。メッセージには、メッセージの発生回数を示す注釈が付けられます。

ログメッセージの最大長は 1024 バイトです。それより長いメッセージは切り捨てられます。

Cisco vManage NMS 監査ログメッセージの最大長は 1024 バイトです。それより長いメッセージはより小さいフラグメントに切り捨てられ、これらの各フラグメントは識別子によって示されます。識別子は、フラグメント 1/2、フラグメント 2/2 などです。たとえば、長い監査ログメッセージがより小さなフラグメントに切り捨てられると、次のように表示されます。

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {"logid":
"d9ed576a-43ae-49ce-921b-a51c1ed40698", "entry_time":
1576605512190, "statcycletime" 34542398334245, "logmodule": "maintenance", "logfeature":
"upgrade", "loguser": "admin", "logusersrcip":
"10.0.1.1", "logmessage": "Device validation Upgrade to version - Validation success",
"logdeviceid": "Validation", "auditdetails" :
["[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)",
"auditdetails": ["[18-Oct-2020 17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz", "Software image download may take up to 60]}

local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { "minutes",
"logprocessid": "software_install-7de0ec44-d290-4429-b24532435324", "tenant":, "default"}
```

AAA 認証および Netconf CLI のアクセス状況と使用状況に関連する syslog メッセージは、auth.log および messages.log ファイルに記録されます。Cisco vManage NMS がルータにログインして統計情報とステータス情報を取得し、ファイルをルータにプッシュするたびに、ルータは AAA 認証と Netconf のログメッセージを生成します。したがって、時間の経過とともに、これらのメッセージでログファイルがいっぱいになる可能性があります。これらのメッセージでログファイルがいっぱいにならないようにするには、Cisco vManage NMS から次のコマンドを使用して、AAA 認証と Netconf の syslog メッセージのロギングを無効にします。

AAA および Netconf Syslog メッセージのロギングの無効化

1. vManage# **config**

コンフィギュレーション モード端末を開始します。

2. vManage(config)# **system aaa logs**

AAA および Netconf システムロギング (syslog) メッセージのロギングを設定します。

3. vManage (config-logs) # **audit-disable**

AAA イベントのロギングを無効にします。

4. vManage (config-logs) # **netconf-disable**

Netconf イベントのロギングを無効にします。

5. vManage (config-logs) # **commit**

Commit complete.

Syslog メッセージの送信に TLS を使用する利点

syslog メッセージの送信に TLS を使用する利点は次のとおりです。

- Cisco IOS XE SD-WAN デバイス と syslog サーバー間のハンドシェイクで各 TLS セッションが開始されるため、メッセージコンテンツの機密性が確保されます。Cisco IOS XE SD-WAN デバイス と syslog サーバーでは、そのセッションに使用される特定のセキュリティキーと暗号化アルゴリズムが一致します。TLS セッションでは、syslog メッセージの内容の開示が拒否されます。
- 各メッセージの内容の整合性チェックにより、ホップ単位での転送中のメッセージに対する変更が無効になります。
- Cisco IOS XE SD-WAN デバイス と syslog サーバー間の相互認証により、syslog サーバーは証明書交換を通じて許可されたクライアントからのみログメッセージを受け入れるようになります。

TLS のサーバー認証でのロギングの設定

サーバー認証では、Cisco IOS XE SD-WAN デバイスは syslog サーバーの ID を確認します。syslog サーバーと証明書が正当なエンティティである場合、デバイスはサーバーとの TLS 接続を確立します。サーバー認証を実装するために、syslog サーバーは公開証明書を Cisco IOS XE SD-WAN デバイスと共有します。

前提条件

Cisco IOS XE SD-WAN デバイスに、暗号化モジュール CLI を使用して設定するルート認証局 (CA) が事前にインストールされていることを確認します。「[サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール](#)」を参照してください。

syslog サーバーの TLS プロファイルを設定するには、次の手順を実行します。

1. [Cisco vManage を使用したロギング機能テンプレートの設定](#)。

1. [ローカルディスクへのロギング属性の設定](#)。

2. リモートサーバーへのロギングの設定。
2. ロギング機能テンプレートからデバイステンプレートを作成します。

TLS の相互認証でのロギングの設定

相互認証では、syslog サーバーと Cisco IOS XE SD-WAN デバイスの両方がお互いを同時に認証します。Cisco IOS XE SD-WAN デバイスには、TLS セッションの相互認証のために、ルート証明書または ID 証明書が必要です。syslog サーバーの TLS プロファイルを設定するには、次の手順を実行します。

1. 相互認証のために Cisco IOS XE SD-WAN デバイスに Syslog ルート証明書をインストール。
2. Cisco vManage を使用したロギング機能テンプレートの設定。
 1. ローカルディスクへのロギング属性の設定。
 2. 機能証明書署名要求の生成と機能証明書のインストール (19 ページ)
 3. リモートサーバーへのロギングの設定。
3. ロギング機能テンプレートからデバイステンプレートを作成します。
4. 機能証明書署名要求の生成と機能証明書のインストール (19 ページ)。
5. Cisco IOS XE SD-WAN デバイス でのトラストポイント設定の確認。

サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール

始める前に

エンコードされた CA 証明書を syslog サーバーで生成していることを確認します。[サーバー認証のために Syslog サーバーにルート認証局をインストール \(9 ページ\)](#) を参照してください。

ステップ 1 認証局の PKI トラストポイントを設定するには、次のコマンドを使用して、PKI での証明書の許可および失効を設定します。

a) **enable**

特権 EXEC モードを有効にします。

例 :

```
Cisco XE SD-WAN> enable
```

b) **config-transaction**

コンフィギュレーション モードを開始します。

例：

```
Cisco XE SD-WAN# config-transaction
```

c) **crypto pki trustpoint name**

トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

例：

```
Cisco XE SD-WAN (config)# crypto pki trustpoint Syslog-signing-CA
```

d) **enrollment [mode] [retry period minutes] [retry count number] url url [pem]**

CA の登録パラメータを指定します。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# enrollment terminal
```

e) **chain-validation [{stop | continue}[parent-trustpoint]]**

証明書チェーンが、すべての証明書で処理されるレベルを設定します。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# chain-validation stop
```

f) **revocation-check method**

(任意) 証明書の失効ステータスをチェックします。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# revocation-check none
```

g) **exit**

グローバル コンフィギュレーション モードに戻ります。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# exit
```

ステップ 2 Cisco IOS XE SD-WAN デバイスに証明書を発行して証明書の登録を行う前に、ルート CA を取得して認証します。

CA を認証するには、**crypto pki authenticate** コマンドを使用します。

例：

```
Cisco XE SD-WAN(config)# crypto pki authenticate root
```

ステップ 3 Base 64 でエンコードされた CA 証明書が含まれているテキスト部分をコピーし、プロンプトにペーストします。

エンコードされた CA 証明書を含むテキストを生成してコピーするには、[サーバー認証のために Syslog サーバーにルート認証局をインストール \(9 ページ\)](#) を参照してください。

例：

Base 64 でエンコードされた CA 証明書のサンプル：

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswcQYD
```



```
VQQGEwJJtJESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQUHDA1CYW5nYWxvcmUx
DjAMBgNVBAcMBUNpc2NvMqwwCgYDVQQLDANDU0cxGzAZBgNVBAMMEVtYmQtbG54
LmNpc2NvLmNvbTEuMBSGCSqGSIb3DQEJARYOYW5idkBJaXNjb20wHhcNMkxw
OTIwMTQ1NjAxWhcNMjIwOTE5MTQ1NjAxWjCBjzELMAkGA1UEBHMCSU4xZjAQBgNV
BAGMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVDaXNj
bzEMMAoGA1UECwwDQ1NHRswGQYDVQDDbJlbWJkLWxueC5jaXNjb20xHTAb
BgkqhkiG9w0BCQEQWDMFuYnZAY2l2Y28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCqKCAQEAAuof+Dh8EdAQ7bHJPDnXhy9ibTLAQ+OpQrMBoOqeAsU/Jru8y
3ht2Eqci35aNjldCsTULZyUHBNAMtL69t1HxTRVCOghOZmipzOS+q8rFykHa+bcA
FqmHyqxNwdQcW3cQFZ6rvWTFD9046ONX3xewpdCR+s+0KFOHdd+RxpAb2NyDWIvn
/1/xwq2a4ZlwgM2d0G8sit0i0D/+6FbZuJjAf+PRTypo4IJyQjcOHpZuslLzPztM
HxLI7pOmR+8+WcInT010dyGdpKKHXi6lEbeiYubIym0z0Des5OckDYFejXgXpJDx
9jCVkz+r0bijqbT5PmpSAYycjdnQ0kdH43sykwIDAQABo1MwUTAdBgNVHQ4EFgQU
OcOmN72TyBqD/Ud2qBLUwIdlYv0wHwYDVR0jBBgwFoAUOcOmN72TyBqD/Ud2qBLU
wIdlYv0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAAUVVJHwo
rKxkFV2w7jR7mLZS1VtEvZueMXWPvYYP+Qt09MrRqWNDUJEvggTxU7lVlWtnITPM
1/dOmpoer8GhDtnxUnjsVeVWGIr74SJC50GU/03bEJ2sto/eAJEOzI7wDg7Fubgy
Pc3RHbk4JWtWs4JF8+E64p2UzJMuu0eLDPQWx17p2wd3sr4DBHB3qlfbg31T3VHr
PCcuZJmOEdeZYGL1/LFvPx7NZS8lwFAohe6h8ptm3ENg7dzIeyZFZVfcq11Q1rer
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

ステップ 4 **yes** と入力して、証明書の受け入れを確認します。

ルート CA 証明書が正常にインポートされました。

次のタスク

[Cisco vManage を使用したロギング機能テンプレートの設定 \(11 ページ\)](#)

サーバー認証のために Syslog サーバーにルート認証局をインストール

このドキュメントでは、TLS をサポートする syslog-ng サーバーをセットアップする手順について説明します。

ステップ 1 サーバーに syslog-ng をインストールするには、次のコマンドを使用します。

例：

```
# apt-get install syslog-ng openssl
```

ステップ 2 ディレクトリを syslog-ng フォルダに変更し、ルート証明書を保存するフォルダを作成するには、次のコマンドを使用します。

例：

```
# cd /etc/syslog-ng
# mkdir cert.d
# mkdir key.d
# mkdir ca.d
# cd cert.d
```

```
# openssl req -new -x509 -out cacert.pem -days 1095 -nodes  
# mv privkey.pem ../key.d
```

openssl コマンドを使用すると、cacert.pem ファイルでエンコードされたルート証明書を使用できます。このファイルは、cd/etc/syslog-ng/cert.d ディレクトリにあります。

ステップ 3 Cisco IOS XE SD-WAN デバイスでルート証明書をインストールするときに、cacert.pem ファイルからコンテンツをコピーします。サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール (7 ページ) のステップ 3 を参照してください。

次のタスク

[サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール \(7 ページ\)](#)

相互認証のために Cisco IOS XE SD-WAN デバイスに Syslog ルート証明書をインストール

Transport Layer Security (TLS) syslog プロトコルを使用して Cisco IOS XE SD-WAN デバイスを設定するには、デバイスに TLS セッションを相互認証するためのルート証明書またはアイデンティティ証明書が必要です。サードパーティの認証局 (CA) を使用して Public Key Infrastructure (PKI) サービスを取得するか、Microsoft Active Directory 証明書サービス (ADCS) を使用できます。ADCS を使用すると、PKI を作成し、要件に応じて公開キー暗号、デジタル証明書、およびデジタル署名機能を提供できます。

- ステップ 1** サードパーティの CA または Microsoft Active Directory 証明書サービスを使用して、エンタープライズルート証明書を生成します。
- ステップ 2** ルート CA を Base 64 形式でダウンロードし、ルート CA の内容を選択してコピーします。
- ステップ 3** Cisco vManage のメニューで、**[Administration] > [Settings]** を選択します。
- ステップ 4** **[Enterprise Feature Certificate Authorization]** をクリックし、**[Edit]** をクリックします。
- ステップ 5** **[Enterprise Root Certificate]** ボックスにルート CA の内容を貼り付けます。
- ステップ 6** (オプション) 証明書署名要求 (CSR) を生成する場合は、**[Set CSR Properties]** チェックボックスをオンにします。
- ステップ 7** **[Close]** をクリックします。

ルート CA は Cisco vManage にアップロードされ、Cisco vManage はルート証明書を Cisco IOS XE SD-WAN デバイス に保存します。

次のタスク

[Cisco vManage を使用したロギング機能テンプレートの設定 \(11 ページ\)](#)

Cisco vManage を使用したロギング機能テンプレートの設定

Cisco IOS XE SD-WAN デバイス では、Cisco vManage を使用してイベント通知システムログ (syslog) メッセージをローカルデバイス上またはリモートホスト上のファイルに記録できません。

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 2 **[Feature Templates]** をクリックして、**[Add Template]** をクリックします。

(注) Cisco vManage リリース 20.7.x 以前では、**[Feature Templates]** のタイトルは **[Feature]** です。

ステップ 3 **[Select Devices]** で、テンプレートを作成するデバイスを選択します。

ステップ 4 ロギング用のテンプレートを作成するには、**[Cisco Logging]** を選択します。

Cisco ロギング テンプレート フォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、ロギングパラメータを定義するためのフィールドが含まれています。タブまたはプラス記号 (+) をクリックして、他のフィールドを表示します。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータの範囲は **[Default]** に設定されています。デフォルトの設定または値は、パラメータの横に表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある **[Scope]** ドロップダウンリストをクリックします。

ステップ 5 **[Template Name]** に、テンプレートの名前を入力します。

名前には、最大 128 文字の英数字を使用できます。

ステップ 6 **[Template Description]** に、テンプレートの説明を入力します。

説明には、最大 2048 文字の英数字を使用できます。

次のタスク

[ローカルディスクへのロギング属性の設定 \(11 ページ\)](#)

ローカルディスクへのロギング属性の設定

1. **[Disk]** をクリックし、次のパラメータを設定します。

表 3: パラメータ情報

パラメータ	説明
Enable Disk	ローカルハードディスク上のファイルに syslog メッセージを保存する場合は [On] を、保存を許可しない場合は [Off] をクリックします。デフォルトでは、すべてのデバイスでローカルディスクファイルへのロギングが有効になっています。
最大ファイル サイズ (Maximum File Size)	syslog ファイルの最大サイズを入力します。syslog ファイルは、ファイルサイズに基づいて 1 時間ごとにローテーションされます。ファイルサイズが設定値を超えると、ファイルがローテーションされ、syslogd プロセスに通知されます。 範囲 : 1 ~ 20 MB デフォルト : 10 MB
Rotations	最も早く作成されたファイルを破棄するまでに作成できる syslog ファイルの数を入力します。 範囲 : 1 ~ 10 MB デフォルト : 10 MB

- 機能テンプレートを保存するには、[Save] をクリックします。
- 機能テンプレートをデバイステンプレートに関連付けるには、機能テンプレートからのデバイステンプレートの作成を参照してください。 <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/System-Interface/systems-interfaces-book-xe-sdwan/configure-devices.html>

次の作業

[サーバー認証用 TLS プロファイルの設定 \(12 ページ\)](#) または [相互認証用 TLS プロファイルの設定 \(15 ページ\)](#)

サーバー認証用 TLS プロファイルの設定

- [TLS Profile] をクリックします。
- [New Profile] をクリックし、次のパラメータを設定します。

表 4:パラメータ情報

パラメータ名	説明
プロファイル名	TLS プロファイル名を入力します。
TLS バージョン	TLS バージョン v1.1 または v1.2 を選択します。
認証タイプ	認証タイプとして [Server] を選択します。

パラメータ名	説明
Ciphersuites	<p>TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。</p> <p>以下は、暗号スイートのリストです。</p> <ul style="list-style-type: none"> • aes-128-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha 暗号化タイプ tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 以上) • dhe-aes-gcm-sha2 暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 以上) • ecdhe-ecdsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 以上) SuiteB • ecdhe-rsa-aes-128-cbc-sha 暗号化タイプ tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 以上) • ecdhe-rsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 以上) • rsa-aes-cbc-sha2 暗号化タイプ tls_rsa_with_aes_cbc_sha2 (TLS1.2 以上) • rsa-aes-gcm-sha2 暗号化タイプ tls_rsa_with_aes_gcm_sha2 (TLS1.2 以上)

TLS バージョンごとに、次の暗号スイートを使用できます。

TLS v1.1

```

aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha

```

TLS v1.2 以降

```



dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)

ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)

```

TLS プロファイルが表に表示されます。

- 別のプロファイルを作成するには、[Add] をクリックします。
- TLS プロファイル情報を編集または削除するには、[Action] の下にある  または  をクリックします。
- 機能テンプレートを保存するには、[Save] をクリックします。
- 機能テンプレートをデバイステンプレートに関連付ける場合は、「[機能テンプレートからのデバイステンプレートの作成](#)」を参照してください。

認証タイプとして [Server] を選択すると、トラストポイント情報を除く、TLS プロファイルに関するすべての情報が保存されます。

次の作業

[リモートサーバーへのロギングの設定 \(17 ページ\)](#)

相互認証用 TLS プロファイルの設定

- [TLS Profile] をクリックします。
- [New Profile] をクリックし、次のパラメータを設定します。

表 5: パラメータ情報

パラメータ名	説明
プロファイル名	TLS プロファイル名を入力します。
TLS バージョン	TLS バージョン v1.1 または v1.2 を選択します。
認証タイプ	認証タイプとして [Mutual] を選択します。

パラメータ名	説明
Ciphersuites	<p>暗号化に使用する必要がある TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。</p> <p>以下は、暗号スイートのリストです。</p> <ul style="list-style-type: none"> • aes-128-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha 暗号化タイプ tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 以上) • dhe-aes-gcm-sha2 暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 以上) • ecdhe-ecdsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 以上) SuiteB • ecdhe-rsa-aes-128-cbc-sha 暗号化タイプ tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 以上) • ecdhe-rsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 以上) • rsa-aes-cbc-sha2 暗号化タイプ tls_rsa_with_aes_cbc_sha2 (TLS1.2 以上) • rsa-aes-gcm-sha2 暗号化タイプ tls_rsa_with_aes_gcm_sha2 (TLS1.2 以上)

TLS バージョンごとに、次の暗号スイートを使用できます。



TLS v1.1


```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha  
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

TLS v1.2 以降

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)  
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)  
  
ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)  
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)  
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)  
  
rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)  
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

TLS プロファイルが表に表示されます。

3. 別のプロファイルを作成するには、[Add] をクリックします。
4. TLS プロファイル情報を編集または削除するには、[Action] の下にある  または  をクリックします。
5. 機能テンプレートを保存するには、[Save] をクリックします。
6. 機能テンプレートをデバイステンプレートに関連付けます。「[機能テンプレートからのデバイステンプレートの作成](#)」を参照してください。

相互認証された機能テンプレートは Cisco IOS XE SD-WAN デバイスに保存され、SYSLOG-SIGNING-CA 証明書などのトラストポイントはデバイスに保存されます。これで、Cisco vManage は Cisco IOS XE SD-WAN デバイスから証明書をインストールできるようになりました。

次の作業


[リモートサーバーへのロギングの設定 \(17 ページ\)](#)

リモートサーバーへのロギングの設定



IPv6 または IPv4 サーバー設定に TLS プロファイルを追加し、イベント通知システムログメッセージのリモートサーバーへのロギングを設定するには、次の手順を実行します。

1. [Server] をクリックします。
2. [Add New Server] をクリックし、IPv4 または IPv6 の次のパラメータを設定します。

表 6:パラメータ情報

パラメータ名	説明
ホスト名/IPアドレス (Hostname/IP Address)	<p>syslogメッセージを保存するシステムのドメインネームシステム (DNS) 名、ホスト名、または IPv4/IPv6 アドレスを入力します。</p> <p>別の syslog サーバーを追加するには、[+] をクリックします。</p> <p>syslog サーバーを削除するには、 をクリックします。</p>
VPN ID	<p>syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。</p> <p>VPN ID 範囲 : 0 ~ 65530</p>
Source Interface	<p>発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、syslog サーバーの設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスはすべて同じにする必要があります。</p>
プライオリティ	<p>保存する syslog メッセージの重大度を選択します。重大度は、syslog メッセージを生成したイベントの深刻度を示します。Syslog メッセージのレベルを参照してください。</p>
TLS	<p>Cisco IOS XE SD-WAN デバイスの場合は、[On] をクリックして TLS 経由の syslog を有効にします。</p>
カスタム プロファイル	<p>Cisco IOS XE SD-WAN デバイスの場合、[On] をクリックして TLS プロファイルの選択を有効にするか、[Off] をクリックして TLS プロファイルの選択を無効にします。</p>
TLS Profile	<p>Cisco IOS XE SD-WAN デバイスの場合、IPv4 または IPv6 サーバー設定でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。</p>

サーバーエントリがテーブルに表示されます。

3. サーバーの別のエントリを作成するには、[Add] をクリックします。
4. ロギングサーバーを編集するには、 をクリックします。
5. ロギングサーバーを削除するには、 をクリックします。
6. 機能テンプレートを保存するには、[Save] をクリックします。
7. 機能テンプレートをデバイステンプレートに関連付ける場合は、「[機能テンプレートからのデバイステンプレートの作成](#)」を参照してください。

機能証明書署名要求の生成と機能証明書のインストール

Cisco IOS XE SD-WAN デバイス および syslog サーバーを検証および認証するには、Cisco vManage の [Certificates] 画面で次の操作を実行します。エンタープライズ証明書については、『[Cisco SD-WAN Getting Started Guide](#)』を参照してください。

ステップ 1 Cisco vManage のメニューから **[Configuration] > [Certificates]** の順に選択します。

ステップ 2 [Certificates] から、Cisco IOS XE SD-WAN デバイス を選択します。

- a) **機能証明書署名要求 (CSR) を生成します。**

機能 CSR を生成すると、[View Feature CSR] および [Install Feature certificate] オプションが使用できるようになります。

- b) **機能 CSR を表示します。**
- c) 機能 CSR をダウンロードするには、[Download] をクリックします。

ステップ 3 証明書に署名するには、証明書をサードパーティの署名機関に送信します。

ステップ 4 Cisco IOS XE SD-WAN デバイス に証明書をインポートするには、**機能証明書をインストールします。**

[Install Feature Certificate] 画面では、署名された証明書を使用し、それを Cisco IOS XE SD-WAN デバイス にインストールします。

機能証明書のインストールが成功すると、[Revoke Feature Certificate] および [View Feature Certificate] オプションが Cisco vManage で使用できるようになります。<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c-Certificates-12278><https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c-Certificates-12278>

次のタスク

[Cisco IOS XE SD-WAN デバイス でのトラストポイント設定の確認 \(20 ページ\)](#)

Cisco IOS XE SD-WAN デバイスでのトラストポイント設定の確認

Cisco IOS XE SD-WAN デバイスのトラストポイント情報を含む syslog ファイルの内容を表示するには、**show crypto pki trustpoints status** コマンドを使用します。

例

サーバー認証

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

相互認証

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Syslog-signing-CA 証明書のデバイス上のトラストポイントを確認します

```
Cisco XE SD-WAN# show crypto pki trustpoints SYSLOG-SIGNING-CA status

Trustpoint SYSLOG-SIGNING-CA:

  Issuing CA certificate not configured.

State:

Keys generated ..... No

  Issuing CA authenticated ..... No

  Certificate request(s) ..... None
```

Cisco vManage NMS 監査ログの Syslog サーバーへのエクスポート

表 7: 機能の履歴

機能名	リリース情報	説明
vManage 監査ログを Syslog としてエクスポート	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	Cisco vManage NMS は、監査ログを syslog メッセージ形式で、構成済みの外部 syslog サーバーにエクスポートします。この機能により、ネットワークアクティビティログを一元的な場所に統合して保存できます。

Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス では、CLI を使用してイベント通知システムログ (syslog) メッセージをローカルデバイス上またはリモートホスト上のファイルに記録できます。これらのイベント通知ログは、システムログファイルに変換され、syslog サーバーにエクスポートされます。その後、syslog サーバーからシステムログ情報を取得できます。

CLI を使用したシステムロギングの設定

Syslog メッセージをローカルデバイスに記録する

デフォルトでは、ローカルデバイス上のファイルに syslog メッセージを記録するときには、「情報」の優先度レベルが有効になっています。次のコマンドを使用します。

1. logging disk

ハードディスクに syslog メッセージを記録します

例 :

```
vm01(config-system)# logging disk
```

2. enable

ディスクへのロギングを有効にします

例 :

```
vm01(config-logging-disk)# enable
```

3. file size size

syslog ファイルのサイズをメガバイト (MB) で指定します。デフォルトでは、syslog ファイルは 10 MB です。syslog ファイルのサイズは 1 ~ 20 MB に設定できます。

例 :

```
vm01(config-logging-disk)# file size 3
```

4. **file rotate number**

ファイルのサイズに基づいて、1 時間ごとに syslog ファイルをローテーションします。デフォルトでは、10 個の syslog ファイルが作成されます。rotate コマンドは、1 ~ 10 の数値に設定できます。

例：

```
vm01(config-logging-disk)# file rotate 3
```

logging disk コマンドの詳細については、「[logging disk](#)」コマンドを参照してください。

Syslog メッセージをリモートデバイスに記録する

イベント通知システムログ (syslog) メッセージをリモートホストに記録するには、次のコマンドを使用します。

1. **logging server**

syslog メッセージをリモートホストまたは syslog サーバーに記録します。サーバーの名前は、DNS 名、ホスト名、または IP アドレスで設定できます。最大 4 つの syslog サーバーを設定できます。

例：

```
vm01(config-system)# logging server 192.168.0.1
```

2. (オプション) **vpn vpn-id**

syslog サーバーの VPN ID を指定します

3. (オプション) **source interface interface-name**

syslog サーバーに到達するソースインターフェイスを指定します。インターフェイス名は、物理インターフェイスまたはサブインターフェイス (VLAN タグ付きインターフェイス) にすることができます。インターフェイスが syslog サーバーと同じ VPN にあることを確認します。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。

例：

```
vm01(config-server-192.168.0.1)# source interface eth0
```

4. **priority priority**

保存する syslog メッセージの重大度を指定します。デフォルトのプライオリティ値は「情報」であり、デフォルトでは、すべての syslog メッセージが記録されます。

例：

次の例では、syslog の優先度をログアラート条件に設定します。

```
vm01(config-server-192.168.0.1)# priority alert
```

syslog サーバーに到達できない場合、システムは syslog メッセージの送信を 180 秒間停止します。サーバーが到達可能になると、ロギングが再開されます。logging server コマンドの詳細については、「[logging server](#)」コマンドを参照してください。

システムロギング情報の表示

リモートホストに syslog メッセージを記録した後にシステムログ設定を表示するには、**show logging** コマンドを使用します。次に例を示します。

```
vm01(config-server-192.168.0.1)# show logging
```

```
System logging
  server 192.168.0.1
  source interface eth0
  exit
!
!
```

syslog ファイルの内容を表示するには、**show log** コマンドを使用します。次に例を示します。

```
vm01(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

Cisco vManage から設定されたシステムロギング設定を表示するには、[監査ログ](#)を参照してください。

Cisco vManage からデバイス固有の syslog ファイルを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから **[Administration]** > **[Settings]** を選択し、**[Data Stream]** を有効にしていることを確認します。
2. Cisco vManage のメニューから **[Monitor]** > **[Devices]** を選択し、Cisco IOS XE SD-WAN デバイスを選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから **[Monitor]** > **[Network]** を選択し、Cisco IOS XE SD-WAN デバイスを選択します。

3. **[Troubleshooting]** をクリックします。
4. **[Logs]** で、**[Debug Log]** をクリックします。
5. **[Log Files]** から、ログファイルの名前を選択してログ情報を表示します。

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。