ISEでの外部syslogサーバの設定

```
内容

   はじめに

   前提条件

   要件

   使用するコンポーネント

   背景説明

   コンフィギュレーション

   リモートロギングターゲットの設定(UDP Syslog)

   例

   ロギング・カテゴリの下でのリモート・ターゲットの構成

   カテゴリについて

   確認とトラブルシューティング
```

はじめに

このドキュメントでは、ISEで外部syslogサーバを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Identity Services Engine(ISE)を使用します。
- syslog サーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)3.3バージョン
- Kiwi Syslogサーバv1.2.1.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

ISEからのsyslogメッセージは、ログコレクタによって収集および保存されます。これらのログコ レクタはモニタリングノードに割り当てられるため、MnTは収集されたログをローカルに保存し ます。

ログを外部から収集するには、ターゲットと呼ばれる外部syslogサーバを設定します。ログは、 さまざまな定義済みカテゴリに分類されます。

ロギング出力をカスタマイズするには、ターゲットや重大度などのカテゴリを編集します。

コンフィギュレーション

Webインターフェイスを使用して、システムログメッセージの送信先となるリモートsyslogサー バターゲットを作成できます。ログメッセージは、syslogプロトコル標準(RFC-3164を参照)に 従ってリモートsyslogサーバターゲットに送信されます。



リモートロギングターゲットの設定(UDP Syslog)

Cisco ISE GUIで、メニュー(

)をクリックし、Administration>System>Logging>Remote Logging Targets>Addの順に選択します。



注:この設定例は、Configuring Remote Logging Targetという名前のスクリーンショット に基づいています。

- Name as Remote_Kiwi_Syslog。ここでは、リモートSyslogサーバの名前を入力できます。
 この名前は説明目的で使用されます。
- Target TypeをUDP Syslogとして設定した場合、この設定例ではUDP Syslogが使用されていますが、Target Typeドロップダウンリストからさらに多くのオプションを設定できます。

UDP syslog:UDPを介したsyslogメッセージの送信に使用されます。軽量で高速なロギングに適し ています。

TCP syslog:TCP経由でsyslogメッセージを送信するために使用されます。これにより、エラーチェックと再送信機能で信頼性が提供されます。

セキュアSyslog:TLS暗号化を使用してTCP経由で送信されるsyslogメッセージを指し、データの 整合性と機密性を確保します。

- StatusがEnabledの場合は、Statusdrop-downリストからEnabledfromを選択します。
- 摘要。オプションで、新規ターゲットの簡単な摘要を入力できます。
- Host / IP Address: ログを保存する宛先サーバのIPアドレスまたはホスト名を入力します。 Cisco ISEは、ロギング用にIPv4およびIPv6形式をサポートします。



注:syslogサーバにFQDNを設定する場合は、パフォーマンスに影響を与えないように DNSキャッシングを設定する必要があることを説明してください。DNSキャッシングを 使用しない場合、ISEは、FQDNで設定されたリモートロギングターゲットにsyslogパケ ットを送信する必要があるたびにDNSサーバにクエリを送信します。これは、ISEのパフ ォーマンスに重大な影響を与えます。

この問題を解決するには、導入のすべてのPSNでservice cache enableコマンドを使用します。

ise/admin(config)# service cache enable hosts ttl 180

• Portに514を指定した場合、この設定例では、Kiwi Syslogサーバはポート514(UDP syslogメッセージのデフォルトポート)でリスニングします。 ただし、ユーザはこのポート番号を1 ~ 65535の任意の値に変更できます。目的のポートがファイアウォールによってブロックされていないことを確認してください。

• Facility CodeをLOCAL6に設定した場合は、ロギングに使用する必要があるsyslogファシリティコードをドロップダウンリストから選択できます。有効なオプションはLocal0 ~ Local7です。

• Maximum Lengthを1024に設定した場合は、リモートログターゲットメッセージの最大長を入力できます。 最大長は 、デフォルトで1024に設定されています。ISE 3.3バージョンの値は200 ~ 1024バイトです。



注:切り捨てられたメッセージがリモートロギングターゲットに送信されないようにするには、最大長を8192に変更します。

 アラームを含めるこのターゲットについては、単純さを保つために、この設定例では「このターゲットのアラームを 含める」はチェックされていません。ただし、このチェックボックスをチェックすると、アラームメッセージもリモート サーバに送信されます。

• Comply to RFC 3164 is checked」チェックボックスをオンにすると、バックスラッシュ(\)を使用しても、リモートサーバに送信されるsyslogメッセージの区切り記号(,; { } \ \)はエスケープされません。

設定が終了したら、Saveをクリックします。

保存すると、システムは次の警告を表示します: You have chosen to create an unsecure (TCP/UDP) connection to the server.**続行しますか?**、「**はい**」をクリックしてください。

	dentity Services	Engine					Adn	ninistration /	'System				Q	۵	?	Ģ
Į	Bookmarks	Deployment	Licensing	Certif	ficates	Logging	Maintenance	Upgrade	Health Check	s Backup & Restore	Admin Access	Settings				
	Dashboard	Log Settings				ing Targets List	> Remote Kiwi Svslog									
망	Context Visibility	Remote Logging	Targets		Logging ⁻	Farget										
×	Operations	Logging Categor	ies 9		* Name		Remote_Kit	wi_Syslog	Target Type	UDP SysLog						
•	Policy	Collection Filters														
20	Administration				Descriptio	n	Remote Log	ging Target	Status	Enabled V						
គា	Work Centers				* Host / IF	Address	10.:									
					* Port		514		(Valid Range	1 to 65535)						
?	Interactive Help				Facility Co	de	LOCAL6									
					* Maximur	n Length	1024		(Valid Range	200 to 8192)						
					Include Al	arms For this	Target									
					Comply to	RFC 3164	0									
													Save			

リモート・ターゲットの構成

٠

ロギング・カテゴリの下でのリモート・ターゲットの構成

Cisco ISEは監査可能なイベントをsyslogターゲットに送信します。リモートロギングターゲットを設定したら、次にその**リモート** ロギングターゲットを目的のカテゴリにマッピングし、監査可能なイベントを転送する必要があります。

その後、ロギングターゲットをこれらのロギングカテゴリのそれぞれにマッピングできます。 これらのログカテゴリのイベント

ログはPSNノードからのみ生成され、これらのノードで有効になっているサービスに応じて関連ログをリモートsyslogサーバに送 信するように設定できます。

AAA監査

AAA診断

•

•

•

アカウンティング

•

外部MDM

•

パッシブID

•

•

•

•

ポスチャとクライアントプロビジョニングの監査

ポスチャおよびクライアントプロビジョニング診断

プロファイラ

次のログカテゴリのイベントログは、展開のすべてのノードから生成され、関連するログをリモートsyslogサーバに送信するよう に設定できます。 管理監査および運用監査

システム診断

•

システム統計情報

この設定例では、4つのロギングカテゴリ(認証に成功、試行に失敗、およびアカウンティング)でリモートターゲットを設定して、認証トラフィックログを送信します。具体的には、認証に失敗、RADIUSアカウンティング、およびISE管理者ロギングトラフィックのこのカテゴリです。



注:この設定例は、Configuring Remote Logging Targetという名前のスクリーンショットに基づいています。



Cisco ISE GUIで、メニュー(

)をクリックし、Administration>System>Logging>Logging Categoriesの順に選択し、必要なカテゴリ(Passed Authentications、Failed Attempts、およびRadius Accounting)をクリックします。

ステップ1:ログの重大度レベル:イベントメッセージは重大度レベルに関連付けられます。これにより、管理者はメッセージをフィルタリングして優先順位を付けることができます。必要に応じて、ログの重大度を選択します。一部のロギングカテゴリでは、この値はデフォルトで設定され、編集できません。一部のロギングカテゴリでは、ドロップダウンリストから次のいずれかの重 大度レベルを選択できます。

FATAL:緊急レベル。このレベルでは、Cisco ISEを使用できないため、すぐに必要な措置を講じる必要があります。

エラー:このレベルは重大なエラー状態を示しています。

WARN:このレベルは、正常であるが重要な状態を示す。これは、多くのロギングカテゴリに対して設定されるデフォルトのレベルです。

INFO:このレベルは情報メッセージを示します。

•

DEBUG:このレベルは診断バグメッセージを示します。

ステップ2:**ローカルロギング:このチェックボックスでローカルログの生成を有効にします**。つまり、PSNによって生成されたロ グは、ログを生成する特定のPSNにも保存されます。デフォルト設定を保持することをお勧めします

ステップ3-Targets:このエリアでは、左矢印および右矢印アイコンを使用してAvailableとSelectedareasの間でターゲットを転送する ことにより、ロギングカテゴリのターゲットを選択できます。

Availableareaには、既存のロギングターゲット(ローカル(事前定義)と外部(ユーザ定義)の両方)が含まれます。

最初は空のSelectedareaには、カテゴリに対して選択されたターゲットが表示されます。

ステップ4:ステップ1からステップ3までを繰り返し、Failed AttemptsカテゴリとRadius Accountingカテゴリの下にRemote Targetを 追加します。

	dentity Services	Engine				Adm	nistration	/ System				Q	۵
Į	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
≣ ⊌ *	Dashboard Context Visibility Operations	Log Settings Remote Logging Logging Catego Message Catalo) Targets ries 9	Logging Categ Logging C Name	ories List > F Category Pas	Passed Authentications							
	Policy Administration Work Centers	Collection Filter	S	Log Severi	ty Level IN (L	IFO og level can not be cha	nged.)						
?	Interactive Help			Targets	Av	ailable:	Sel > < () (ected: LogCollector ProfilerRadiusProbe Remote_Kiwi_Syslog					
												Save	

リモートターゲットと目的のカテゴリのマッピング

ステップ5:リモートターゲットが必要なカテゴリの下にあることを確認します。追加したリモートターゲットが表示されている必要があります。

このスクリーンショットでは、リモートターゲットRemote_Kiwi_Syslogが必要なカテゴリにマッピングされていることがわかります。

	dentity Services I	Engine									Administration / S	System	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
52	Dashboard	Log Settings											
	Context Visibility	Remote Logging	Targets	Logg	Logging Categories								
×	Operations	Logging Categor	ries										
 	Policy	Collection Filters	9										
	Administration				Parent Categor	v	Ca	tegory	Targets			Severity	Local Log
	Administration			0	AAA Audit				LogCollector			INFO	enable
- All	Work Centers			0					LogCollector,P	rofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
				0					LogCollector,P	rofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
	Interactive Help			0	AAA Diagnostie	:\$			LogCollector			WARN	enable
				0								WARN	enable
				0								WARN	enable
				0								WARN	enable
				0								WARN	enable
				0					LogCollector			WARN	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0					LogCollector			WARN	enable
				0	ACI Binding				LogCollector			INFO	enable
				0	Accounting				LogCollector			INFO	enable
				0					LogCollector,P	rofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
				0					LogCollector			INFO	enable
				0	Administrative	and Operational Audit			dit LogCollector,R	temote_Kiwi_Syslog		INFO	enable
				0	External MDM				LogCollector			INFO	enable
				0	PassiveID				LogCollector			INFO	enable
				0	Posture and Cli	ient Provisioning Audit			dit ProfilerRadius	Probe,LogCollector		INFO	enable
				0	Posture and Cli	ient Provisioning Diagno	ostics Po		gno LogCollector			WARN	enable
				0	Profiler				LogCollector			INFO	enable
				0	System Diagno	stics			LogCollector			WARN	enable
				0								WARN	enable
				0								WARN	enable
				0					LogCollector			INFO	enable
				0					LogCollector			INFO	enable
				0	System Statisti	cs			LogCollector			INFO	enable

カテゴリの確認

カテゴリについて

イベントが発生すると、メッセージが生成されます。カーネル、メール、ユーザレベルなど、複数の機能から生成されるイベント メッセージには、さまざまなタイプがあります。

これらのエラーはメッセージカタログ内で分類され、これらのイベントも階層構造でカテゴリに分類されます。

これらのカテゴリには、1つまたは複数のカテゴリを含む親カテゴリがあります。

親カテゴリ	[Category]
AAA監査	AAA監査
	失敗した試行(Failed Attempts)
	認証に成功
AAA診断	AAA診断
	管理者の認証と許可

	認証フロー診断
	IDストア診断
	ポリシー診断
	Radius診断
	ゲスト
アカウンティング	アカウンティング
	RADIUS アカウンティング
管理監査および運用監査	管理監査および運用監査
ポスチャとクライアントプロビジョニングの監 査	ポスチャとクライアントプロビジョニングの監 査
ポスチャおよびクライアントプロビジョニング 診断	ポスチャおよびクライアントプロビジョニング 診断
プロファイラ	プロファイラ
システム診断	システム診断
	分散管理
	内部運用診断
システム統計情報	システム統計情報

このスクリーンショットでは、Guestがメッセージクラスであり、**ゲストカテゴリ**として分類されていることがわかります。 この ゲストカテゴリには、AAA Diagnosticsという親カテゴリがあります。

=	E dentity Services	Engine									Administration / System			
,	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
5	Dashboard	Log Settings												
R	Context Visibility	Remote Logging	Targets	Mess	sage Ca	italog								
3	Operations	Message Catalog	D D											
	Policy	Collection Filters												
(2	Administration			Category	y Name			Message Class	Message Code	Message Tex		N	Message Description	Severity
	Work Centers			gues										
				Guest				Guest	86001	Guest user ha	s entered the guest portal login page	G	Suest user has entered the guest portal login page	INFO
				Guest				Guest	86002	Sponso Gues	user has entered the guest portal login page	s	Sponsor has suspended a guest user account	INFO
(3	Interactive Help			Guest				Guest	86003	Sponsor has e	nabled a guest user account	s	Sponsor has enabled a guest user account	INFO
				Guest				Guest	86004	Guest user ha	s changed the password	G	Swest user has changed the password	INFO
				Guest				Guest	86005	Guest user ha	s accepted the Use Policy	G	Suest user has accepted the use policy	INFO
				Guest				Guest	86006	Guest user ac	count is created	G	Swest user account is created	INFO
				Guest				Guest	86007	Guest user ac	count is updated	G	Suest user account is updated	INFO
				Guest				Guest	86008	Guest user ac	count is deleted	G	Suest user account is deleted	INFO
				Guest				Guest	86009	Guest user is	not found	G	Suest user record is not found in the database	INFO
				Guest				Guest	86010	Guest user au	thentication failed	G	Suest user authentication failed. Please check your password and account permis	INFO
				Guest				Guest	86011	Guest user is	not enabled	G	Guest user authentication failed. User is not enabled. Please contact your system	INFO
				Guest				Guest	86012	User declined	Access-Use Policy	G	Suest User must accept Access-Use policy before network access is granted	INFO
				Guest				Guest	86013	Portal not four	nd	P	Portal is not found in the database. Please contact your system administrator	INFO
				Guest				Guest	86014	User is suspe	nded		Jser authentication failed. User account is suspended	INFO
				Guest				Guest	86015	Invalid Passw	ord Change	Ir	nvalid password change. Use correct password based on the password policy	INFO
E.				Guest				Quest	96016	Quest Timeou	Exceeded		Emoust from contrast has exceeded the threshold. Disaste content your system oder	INFO

メッセージカタログ

確認とトラブルシューティング

リモートロギングターゲットに対してTCPダンプを実行することは、ログイベントが送信されているかどうかを確認するための最 も迅速なトラブルシューティングおよび確認の手順です。

PSNはログメッセージを生成し、これらのメッセージはリモートターゲットに送信するため、ユーザを認証するPSNからキャプチ ャを取得する必要があります



)をクリックし、Operations> Troubleshoot>TCP Dump> Addの順に選択します。

- トラフィックをフィルタリングし、ip host <remote_target_IP_addres> filterフィールドを追加する必要があります。
- 認証を処理するPSNからキャプチャを取得する必要があります。



TCPダンプ

このスクリーンショットでは、ISEがISE管理者ロギングトラフィックに対してSyslogメッセージを送信する方法を確認できます。

			-											Z SSPT33A_GigabitEthernet 5.pcap
	a o	•) Q		🔅 7	<u>~</u> 4			Đ.		a 1	•	
Lanhun die	valau filtor	12/5		•		_	• <u>-</u>		-		<u> </u>	<u> </u>	-	
No. I	Time			Course			actionti			Protoco		ongth		nfn
- 1	2024-07-25	10:29:37	.235441	10.201.2	31.67	16	3.201.	231.90		Svsloo		engen	385	nno LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE Administrative and Operational Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891
2	2024-07-25	10:29:49	.056594	10.201.2	31.67	16	9.201.	231.90		Syslog			423	LOCAL6.NOTICE: Jul 25 11:29:49 SSPT33A CISE Administrative_and_Operational_Audit 0000000021 1 0 2024-07-25 11:29:49.056 -05:00 0000012892
3	2024-07-25	10:30:00	.559293	10.201.2	31.67	16	9.201.	231.90		Syslog			385	LOCAL6.NOTICE: Jul 25 11:30:00 SSPT33A CISE_Administrative_and_Operational_Audit 0000000022 1 0 2024-07-25 11:30:00.558 -05:00 0000012893
4	2024-07-25	10:31:12	.796473	10.201.2	31.67	16	9.201.	231.90		Syslog			423	LOCAL6.NOTICE: Jul 25 11:31:12 SSPT33A CISE_Administrative_and_Operational_Audit 0000000023 1 0 2024-07-25 11:31:12.796 -05:00 0000012895
5	2024-07-25	10:32:01	.217780	10.201.2	31.90	16	0.201.	231.95		BROWSE	R		243	Host Announcement DESKTOP-J6CKUCC, Workstation, Server, SQL Server, NT Workstation
6	2024-07-25	10:32:10	.383530	10.201.2	31.67	16	9.201.	231.90		Syslog			520	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000024 1 0 2024-07-25 11:32:10.382 -05:00 0000012896
7	2024-07-25	10:32:10	.383668	10.201.2	31.67	16	9.201.	231.90		Syslog			519	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000025 1 0 2024-07-25 11:32:10.383 -05:00 0000012897
8	2024-07-25	10:32:10	.383760	10.201.2	31.67	16	9.201.	231.90		Syslog			516	LOCAL6.NOTICE Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000026 1 0 2024-07-25 11:32:10.383 -05:00 0000012896
9	2024-07-25	10:32:10	.383807	10.201.2	31.67	16	9.201.	231.90		Syslog			516	LOCALG.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000027 1 0 2024-07-25 11:32:10.383 -05:00 0000012899
10	2024-07-25	10:32:10	3838/8	10.201.2	31.67	10	201.	231.90		Systog			528	LUCALE.NUILE: JUL 25 11:32:10 SSPI33A LISE_ADDINISTRATIVE_AND_UPERATIONAL_AUDIT 0000000020 1 0 2024-07-25 11:32:10.383 -05:00 0000012900 LUCALE.NUILE: JUL 25 11:32:10 SSPI33A LISE_ADDINISTRATIVE_AND_UPERATIONAL_AUDIT 0000000020 1 0 2024-07-25 11:32:10.383 -05:00 0000012900
12	2024-07-25	10:32:10	384053	10.201.2	31.67	16	201.	231.90		Syslog			505	LUCHCO.NUILE: JUL 25 11:32:10 SSF133A LISE_AUMINISTRATIVE_AND_UPERATIONAL_AUDIT 000000029 1 0 2024-07-25 11:32:10:363 -05:00 000001290 J IDCAL6 NOTICE: JUL 25 11:32:10 SSF133A CISE_AUMINISTRATIVE_AND_UPERATIONAL_AUDIT 0000000029 1 0 2024-07-25 11:32:10:363 -05:00 0000001290 J
Erame 1:	385 hytes	on wire	(3080 h	itc). 385	hytes car	stured	13080	hits)						
> Ethernet	II. Src:	Mware a5	:46:12	(00:50:56:	:a5:46:12	. Dst:	VMwar	e a5:e5	:86 (0	0:50:5	5:a5:e5	:86)		
> Internet	Protocol	/ersion 4	, Src:	10.201.231	1.67, Dst:	10.20	1.231.	90						
> User Dat	agram Prot	ocol, Src	Port:	32724, Ds1	t Port: 51	L4								
~ [trunca	ited]Syslog	message:	L0CAL6	.NOTICE: 2	Jul 25 11:	29:37 9	SSPT33	A CISE_	Admini	strati	e_and_	Opera	tion	al_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersi
1011	0 = Faci	lity: LOC	CAL6 – 1	reserved f	or local	use (22								
	.101 = Leve	1: NOTICE	E – norm	nal but si	gnificant	condit	ion (5)						
✓ Messa	ge [truncat	ed]: Jul	25 11:2	9:37 SSPT	33A CISE_	Adminis	trati	/e_and_(Operat:	ional_#	udit 0	996996	020	1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInter
Sys	slog timest	amp (RFC3	164): J	ul 25 11:	29:37									
Sys	log hostna	ne: SSPT3	3A -											
Sys	log messag	s id: CIS	c ncated]	• Admini	strative :	and One	ration	al Audi	+ 0000	000070	1 0 20	24-07	-25	11.70.37 234 _85.88 8888812881 51882 NATTE Administrator-Ionin. Administrator Ionned off ConfinVersionId-285. AdminInterface-CUI Admin
	ntog messay		mearced J		serucive_e	ma_ope	101201			000020	2 0 20	24 07	-2-0	



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。