L コマンド

この章では、L で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

ldap-server deadtime

すべての Lightweight Directory Access Protocol（LDAP）サーバのデッド タイム間隔を設定するには、**ldap-server deadtime** コマンドを使用します。デッド タイム間隔は、LDAP サーバが停止したことを宣言した後に、サーバが実行を開始したかどうかを判断するテスト パケットを送信するまで、Cisco NX-OS デバイスが待機する時間を指定します。グローバル デッドタイム間隔設定を削除するには、このコマンドの **no** 形式を使用します。

ldap-server deadtime *minutes*

no ldap-server deadtime *minutes*

構文の説明

minutes	LDAP サーバのグローバル デッドタイム間隔。有効な範囲は 1 ～ 60 分です。

デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

デッド タイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバのグローバル デッドタイム間隔を設定する例を示します。

```
switch# config t
switch(config)# ldap-server deadtime 5
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show ldap-server	LDAP サーバの設定を表示します。

ldap-server host

Lightweight Directory Access Protocol（LDAP）サーバ ホスト パラメータを設定するには、**ldap-server host** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

no ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

構文の説明

ipv4-address	*A.B.C.D* 形式のサーバの IPv4 アドレス
ipv6-address	*X:X:X:X* 形式のサーバの IPv6 アドレス
host-name	サーバ名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
enable-ssl	（任意）バインドまたは検索要求を送信する前に、LDAP クライアントに Secure Sockets Layer（SSL）セッションを確立させることによって、転送されるデータの整合性と機密保持を確保します。
port ***tcp-port***	（任意）サーバへの LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。
timeout ***seconds***	（任意）サーバのタイムアウト間隔を指定します。有効な範囲は 1 ～ 60 秒です。
rootDN *root-name*	（任意）LDAP サーバ データベースのルート指定名（DN）を指定します。ルート名には、最大 128 文字の英数字を入力できます。
password ***password***	（任意）ルートのバインド パスワードを指定します。
test	（任意）テスト パケットを LDAP サーバに送信するようにパラメータを設定します。
idle-time ***minutes***	サーバをモニタリングするための時間間隔を分で指定します。有効な範囲は 1 ～ 1440 分です。
username ***name***	テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。 **（注）** ネットワークのセキュリティを保護するために、LDAP データベースの既存のユーザ名と同じものを使用しないことを推奨します。

デフォルト

サーバ モニタリング：ディセーブル
TCP ポート：グローバル値か、グローバル値が設定されていない場合は 389
タイムアウト：グローバル値か、グローバル値が設定されていない場合は 5 秒
アイドル時間：60 分
テスト ユーザ名：test
テスト パスワード：Cisco

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにし、リモート LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得する必要があります。

SSL プロトコルをイネーブルにする予定がある場合は、Cisco NX-OS デバイスで、LDAP サーバ証明書が手動で設定されていることを確認します。

デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバ グループに追加されます。LDAP サーバを別の LDAP サーバ グループに追加することもできます。

特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバの IPv6 アドレスを設定する例を示します。

```
switch# config t
switch(config)# ldap-server host 10.10.2.2 timeout 20
```

次に、LDAP サーバのモニタリング用のパラメータを設定する例を示します。

```
switch# config t
switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password
Ur2Gd2BH idle-time 3
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show ldap-server	LDAP サーバの設定を表示します。

ldap-server port

クライアントが TCP 接続を開始するために使用するグローバル Lightweight Directory Access Protocol（LDAP）サーバ ポートを設定するには、**ldap-server port** コマンドを使用します。LDAP サーバ ポート設定を削除するには、このコマンドの **no** 形式を使用します。

ldap-server port *tcp-port*

no ldap-server port *tcp-port*

構文の説明

tcp-port	サーバへの LDAP メッセージに使用するグローバル TCP ポート。有効な範囲は 1 ～ 65535 です。

デフォルト

TCP ポート 389

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドは廃止されました。
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP メッセージ用のグローバル TCP ポートを設定する例を示します。

```
switch# config t
switch(config)# ldap-server port 2
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show ldap-server	LDAP サーバの設定を表示します。

ldap-server timeout

Cisco NX-OS デバイスが、タイムアウト失敗を宣言するまで、すべての Lightweight Directory Access Protocol（LDAP）サーバからの応答を待機する時間を指定するグローバル タイムアウト間隔を設定するには、**ldap-server timeout** コマンドを使用します。グローバル タイムアウト設定を削除するには、このコマンドの **no** 形式を使用します。

ldap-server timeout *seconds*

no ldap-server timeout *seconds*

構文の説明

seconds	LDAP サーバのタイムアウト間隔。有効な範囲は 1 ～ 60 秒です。

デフォルト

5 秒

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバのグローバル タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# ldap-server timeout 10
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show ldap-server	LDAP サーバの設定を表示します。

ldap search-map

Lightweight Directory Access Protocol（LDAP）検索マップを、LDAP サーバに検索クエリーを送信するように設定するには、**ldap search-map** コマンドを使用します。検索マップをディセーブルにするには、このコマンドの **no** 形式を使用します。

ldap search-map *map-name*

no ldap search-map *map-name*

構文の説明

map-name	LDAP 検索マップの名前。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP 検索マップを設定する例を示します。

```
switch# config t
switch(config)# ldap search-map map1
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show ldap-search-map	設定された LDAP 検索マップを表示します。
CRLLookup	検索クエリーを LDAP サーバに送信するために、CRL 検索操作の属性名、検索フィルタ、ベース DN を設定します。
trustedCert	検索クエリーを LDAP サーバに送信するために、信頼される証明書検索操作の属性名、検索フィルタ、ベース DN を設定します。

コマンド	説明
user-certdn-match	検索クエリーを LDAP サーバに送信するために、証明書 DN 一致検索操作の属性名、検索フィルタ、ベース DN を設定します。
user-pubkey-match	検索クエリーを LDAP サーバに送信するために、公開キー一致検索操作の属性名、検索フィルタ、ベース DN を設定します。
user-switch-bind	検索クエリーを LDAP サーバに送信するために、ユーザスイッチグループ検索操作の属性名、検索フィルタ、ベース DN を設定します。
userprofile	検索クエリーを LDAP サーバに送信するために、ユーザ プロファイル検索操作の属性名、検索フィルタ、ベース DN を設定します。

logging drop threshold

ドロップされるパケットのしきい値を設定し、ドロップ カウントがコントロール プレーン ポリシング（CoPP）のポリシー マップで設定されたしきい値を超えた場合に Syslog を生成するには、ロギングの **logging drop threshold** コマンドを使用します。

logging drop threshold [*drop-count* [**level** *syslog-level*]]

構文の説明

drop-count	ドロップ カウント。指定できる範囲は 1 ～ 80000000000 です。
level	（任意）Syslog レベルを指定します。
syslog-level	Syslog レベル。指定できる範囲は 1 ～ 7 です。

デフォルト

Syslog レベル 4

コマンド モード

config-pmap-c

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.1(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルト VDC にいることを確認します。

クラス マップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

このコマンドには、ライセンスは必要ありません。

例

次に、ドロップされるパケットのしきい値を設定し、ドロップ カウントが CoPP のポリシー マップで設定されたしきい値を超えた場合に Syslog を生成する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane ClassMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 52000
switch(config-pmap-c)# police cir 52000 bc 2000
switch(config-pmap-c)# police cir 5000 conform transmit exceed drop violate set1 dscp3
dscp4 table1 pir-markdown-map
switch(config-pmap-c)# police cir 52000 pir 78000 be 2000
switch(config-pmap-c)# logging drop threshold 1800 level 2
switch(config-pmap-c)#
```

関連コマンド

コマンド	説明
policy-map type control-plane	コントロール プレーン ポリシー マップを設定し、ポリシー マップ コンフィギュレーション モードを開始します。

lt

IP ポート オブジェクト グループの less-than グループ メンバーを指定するには、**lt** コマンドを使用します。less-than グループ メンバーは、エントリに指定されたポート番号より小さい（および同等ではない）ポート番号と一致します。ポート オブジェクト グループから less-than グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **lt** *port-number*

no {*sequence-number* | **lt** *port-number*}

構文の説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号は、オブジェクト グループ内でグループ メンバーの順序を保ちます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合、デバイスは最大シーケンス番号より 10 大きい番号を現在のオブジェクト グループに割り当てます。
port-number	このグループ メンバーと一致するトラフィックが、この番号以下となるポート番号。有効な値は 0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

IP ポート オブジェクト グループには方向性がありません。**lt** コマンドを、送信元ポートと宛先ポートのどちらと一致させるか、またはインバウンドとアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは必要ありません。

例

次に、ポート 1 ～ 49151 間で送信されるトラフィックに一致するグループ メンバーで port-group-05 という名前の IP ポート オブジェクト グループを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# lt 49152
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to（等しい）グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに greater-than（より大きい）グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに not-equal-to（等しくない）グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。