システム設定

この章では、次の StarOS オプションを設定する手順について説明します。

「使用する前に」で説明したように、システムを最初に設定する手順が完了していることを前提としています。

重要 この項の設定例で使用されているコマンドは、最もよく使用されるコマンドやキーワードのオプションです。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。詳細については、『*Command Line Interface Reference*』を参照してください。

2 番目の管理インターフェイスの設定

管理入力/出力（MIO/UMIO）カードでのシステム管理インターフェイスの設定手順については、「はじめに」を参照してください。この項では、2 番目の管理インターフェースの構成方法について説明します。

2 番目の管理インターフェイスを設定するには、次の例を使用します。

```
configure
  context local
    interface interface_name
      ip address ipaddress subnetmask
      exit
    ip route 0.0.0.0 0.0.0.0 gw_address interface_name
    exit
  port ethernet slot#/port#
    bind interface interface_name local
    no shutdown
    media rj45
    end
```

注：

- **ポートイーサネット** *slot#* の場合、アクティブな MIO/UMIO が存在する実際のシャーシスロットを使用します。スロット番号 5 または 6 のいずれかになります）。
- IPv4 ドット付き 10 進表記または IPv6 コロンで区切られた 16 進表記を使用して IP アドレスを入力します。
- **ポートイーサネット** ポート番号の場合は、MIO/UMIO カードの物理ポート（ポート 1 または 2）を使用します。
- MIO/UMIO には、RJ-45（1000Base-T 銅線）インターフェイスが装備されています。RJ-45 インターフェイスは、CAT3 または CAT5 イーサネットケーブルを介してシステムを管理ネットワークに接続します。
- オプション：イーサネットポート構成モードで、**medium** コマンドを入力して、必要に応じてポート速度を設定します。このコマンドの詳細については、コマンドラインインターフェイスのリファレンスを参照してください。
- **{ ip | ipv6 } route** コマンドでは、ゲートウェイ IP アドレスではなく、他のキーワードオプションを使用できます。ネクスト**ホップ** IP アドレス、**ポイントツーポイント**、および**トンネル**が含まれます。

インターフェイスとポートの設定の確認と保存

次のコマンドを入力して、インターフェイスの設定が正しいことを確認します。

```
show ip interface
```

このコマンドの出力は、次に示すようになります。この例では、*mgmt2* という名前のインターフェイスがローカルコンテキストで設定されています。

```
Intf Name:       mgmt2
Intf Type:       Broadcast
Description:     management2
VRF:             None
IP State:        UP (Bound to 5/2)
IP Address:      192.168.100.3        Subnet Mask:     255.255.255.0
Bcast Address:   192.168.100.255      MTU:             1500
Resoln Type:     ARP                  ARP timeout:     60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
```

次のコマンドを入力して、ポートの設定が正しいことを確認します。

show configuration port *slot#/port#*

slot # は、物理ポートが設置されているラインカードのシャーシスロット番号です。slot# は 5 または 6 のいずれかです。*port#* はポートの番号です（1 または 2 のいずれか）。

次のコマンドでは、以下に示すような出力が生成されます。シャーシスロット 5 に取り付けられた MIO/UMIO/ のポート 2 の設定が表示されます。この例では、ポートは *mgmt2* というインターフェイスにバインドされています。

```
config
  port ethernet 5/2
    description management2
    no shutdown
    bind interface mgmt2 local
end
```

「設定の確認と保存」の章の説明に従って、設定を保存します。

インターフェイスとポートの設定の確認と保存

次の StarOS CLI コマンドを入力して、インターフェイスの設定が正しいことを確認します。

show ip interface

このコマンドの出力は、次に示すようになります。この例では、*mangement1* という名前のインターフェイスがローカルコンテキストで設定されています。

```
Intf Name:       LOCAL1
Intf Type:       Broadcast
Description:     management1
VRF:             None
IP State:        UP (Bound to 1/1 untagged, ifIndex 16842753)
IP Address:      192.168.100.3        Subnet Mask:     255.255.255.0
Bcast Address:   192.168.100.255      MTU:             1500
Resoln Type:     ARP                  ARP timeout:     60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
```

次のコマンドを入力して、ポートの設定が正しいことを確認します。

show configuration port *slot/port*

VPC-SI の場合、スロットは常に 1 です。port はポートの番号（1, 10 21）です。

この前のコマンドでは、次に示すような出力が生成されます。スロット 1 のポート 1 の設定が表示されます。

```
config
  port ethernet 1/1
    no shutdown
    bind interface LOCAL1 local
```

「設定の確認と保存」の章の説明に従って、設定を保存します。

システムタイミングの設定

システムには、統計カウンタ、アカウンティングレコード、ロギング、およびイベント通知のタイムスタンプを提供するクロックが備わっています。システムクロックの初期設定後に、1 つ または複数の Network Time Protocol（NTP）サーバーと通信するようにシステムを設定し、クロックが常に正確であることを確認できます。

停電が発生した場合、クロックは 1 ヵ月に ± 1 分の精度で最大 10 年間維持されます。これにより、電源が回復したときにシステムはセッションを処理し、正確なタイムスタンプでアカウンティング、ログ、およびイベントデータを生成できるようになります。

すべての VPC インスタンスは、ホストが配置されている IaaS データセンターで使用されているタイミング標準に合わせる必要があります。

タイミングソースの設定に加えて、システムのタイムゾーンを設定する必要があります。

システムクロックとタイムゾーンの設定

システムクロックとタイムゾーンを設定するには、次のコマンド例を使用します。

```
clock set date:time
configure
  clock timezone timezone [ local ]
  end
```

注：

- YYYY:MM:DD:HH:mm 形式 または YYYY:MM:DD:HH:mm:ss に日付、および時刻を入力します。
- サポートされているタイムゾーンの完全なリストについては、**clock timezone** コマンドのオンラインヘルプを参照してください。
- オプションの **local** キーワードは、指定されたタイムゾーンがローカルタイムゾーンであることを示します。
- サマータイムは、そのベースになるタイムゾーンに合わせて自動的に調整されます。

「設定の確認と保存」の章の説明に従って、設定を保存します。

クロックとタイムゾーンの設定の確認と保存

時間とタイムゾーンが正しく設定されていることを確認するには、次のコマンドを入力します。

```
show clock
```

出力には、設定した日付、時刻、およびタイムゾーンが表示されます。

ネットワーク時間プロトコルのサポートの設定

この項では、Network Time Protocol（NTP）を使用できるようにするためのシステムの設定に関する情報を提供し、手順を示します。

重要 NTPサポートを実装する前に、システムクロックとタイムゾーンを設定します。これにより、NTP サーバーで修正する必要がある期間が大幅に短縮されます。

（注） また、NTPはVPC VMを実行している市販（COTS）のすべてのサーバーでも設定する必要があります。StarOSのNTP設定は、COTSサーバーのNTP設定と一致している必要があります。

StarOS が提供するサービスの多くでは、NTP を介して取得する正確な時刻を保持する必要があります。StarOS で使用されている時間基準が正確でないと、サービスの信頼性が失われることがあります。このため、通常のシステム動作には NTP の設定が必要であることを前提とする必要があります。

システムは、NTP を使用して内部クロックを外部の時刻ソース（通常は GPS NTP ソース、あるいはその他の Stratum 2 または 3 サーバー、スイッチ、またはルータ）と同期します。

デフォルトでは、NTPは対外的には有効になっていないため、システムを最初にインストールした時点で設定する必要があります。有効にすると、アクティブな MIO/UMIO が外部ソースと同期されます。有効になっていない場合は、アクティブな MIO/UMIO は時刻ソースとしてローカルクロックを使用します。NTP サーバーまたはネットワークの停止が発生した場合、MIO/UMIO がすでに実行している場合は、時刻の精度を維持するために引き続き NTP が使用されますが、これはホールドオーバーモードで行われます。

CPUが搭載されたすべてのカードが内部的にアクティブなMIO/UMIOと同期します。これは、外部 NTP サーバーが設定されていない場合でも発生します。MIO/UMIO のスイッチオーバーが発生した場合、他のすべてのカードは、新しくアクティブになった MIO/UMIO との同期を自動的に開始します。

システムには次が必要です。

- NTP が有効になっていること。
- NTPが、ローカルコンテキスト内のみで使用されるように設定されていること。他のコンテキストを使用すると（enable は設定可能であるため指定できる）、問題が発生します。

- 少なくとも 3 台の外部 NTP サーバー用に NTP が設定されていること。サーバーが 3 台以上ある場合は、サーバーの異常や破損または誤設定が検出され、除外することができます。一般的に、サーバーの数が多いほど（理にかなった範囲で）良好な結果が得られます。

重要 **prefer** キーワードを使用して外部 NTP サーバーを設定しないでください。NTP クロック選択アルゴリズムには、最適なサーバーを選択する機能がすでに組み込まれています。通常、**prefer** を使用すると、NTP 自体が決定するよりも適切な選択が行われません。

重要 Cisco TAC から指示された場合を除き、**maxpoll**、**minpoll**、または **version** キーワードの設定は変更しないでください。

必要な NTP 関連付けパラメータを設定するには、次の例を使用します。

```
configure
  ntp
    enable
    server ip_address1
    server ip_address2
    server ip_address3
    end
```

注：

- デフォルトでは *context_name* は *local* に設定されます。これが推奨されている設定です。
- **server** コマンドには多数のオプションがあります。詳細については、『*Command Line Interface Reference*』の「*NTP Configuration Mode Commands*」の章を参照してください。
- IPv4 のドット付き 10 進表記または IPv6 のコロンで区切られた 16 進表記を使用して、NTP サーバーの IP アドレスを入力します。
- 最大 6 つの NTP サーバー IP アドレスを設定できます。

重要 少なくとも 3 台（できれば 4 台）の NTP サーバーを使用してシステムを設定します。

「設定の確認と保存」の章の説明に従って、設定を保存します。

ローカルソース使用した NTP サーバーの設定

NTP は、ネットワークピア、ローカルの外部クロック（GPS デバイスなど）、または外部ソースなしのローカルクロックを使用できます。

通常、外部ソースのないローカルクロックは、より適切なクロックが使用できない場合の最終手段です。ほとんどの場合はサイトの中間 NTP サーバー上に設定されます。そのため、WAN ネットワークが停止したときに、サイト内のホストは互いに同期し続けることができます。

これは、ntpd または多くの市販の NTP デバイスに設定できます。このクロックのストラタム番号は常に上位（8+）であるため、通常の状態（実際のソースが使用可能である場合）は、このローカルクロックは使用されません。

タグ付きインターフェイスでの NTP の設定

タグ付きインターフェイスで NTP を有効にするには、次の NTP 構成モード コマンドを使用します。

```
configure
  NTP
    [ no ] vlan  vlan_id
    end
```

注：

- **vlan** *vlan_id* ：vlan_id は ローカル コンテキスト インターフェイスがバインドされている VLAN です。設定後、NTP デーモンはタグ付きインターフェイスでリッスンを開始します。
- **no vlan** ：NTP 設定をデフォルトにリセットし、NTP デーモンがデフォルトのタグなしインターフェイスでリッスンを開始します。

ロード バランサの使用

NTP デーモンと NTP プロトコルは、設定された各サーバーが NTP を実行していることを前提としています。NTP クライアントが、一連の実際の NTP サーバーにパケットをリレーして配布するロードバランサと同期するように設定されている場合、ロードバランサはそれらのパケットを動的に配布し、NTP クライアントを混乱させる場合がありますNTP パケットは遅延とジッターに敏感です。ロードバランサを介してそれらをリレーすることは、NTP クライアントが混乱する可能性があり、サポートされている操作ではありません。

NTP の設定確認

NTP 設定が正しいことを確認します。Exec モードのプロンプトで次のコマンドを入力します。

```
show ntp associations
```

出力には、すべての NTP サーバーに関する情報が表示されます。2 つの NTP サーバーを展開する例については、次の出力を参照してください。

```
+----Peer Selection: ( ) - Rejected / No Response
|                    (x) - False Tick
|                    (.) - Excess
|                    (-) - Outlyer
```

```
|                    (+) - Candidate
|                    (#) - Selected
|                    (*) - System Peer
|                    (o) - PPS Peer
v
     remote            refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.81.254.202   .GPS.            1 u  160 1024  377   21.516    0.019   0.009
```

次の表では、**show ntp association** コマンドによって出力されるパラメータについて記述しています。

表 *1 : NTP* パラメータ

列のタイトル	説明
リモート	現在の NTP サーバーのリスト。これらの文字の 1 つは、各 IP アドレスの前にあり、サーバーの現在の状態を示します。 • ( ) Rejected/No response • X False tick • . Excess • - Outlyer • + Candidate • # Selected • * System peer • (o) PPS peer
refid	サーバーが同期している最後に報告された NTP の参照。
st	NTP サーバーのストラタムレベル。
t	通信タイプ：ブロードキャスト、マルチキャストなど
when	最終接続からの経過秒数。
poll	システムと NTP サーバー間の電話機の設定ユーティリティ。
reach	この NTP サーバーへの過去 8 回のポーリングで受信された応答を示す、到達可能性シフトレジスタの 8 進値。
delay	システムと NTP サーバー間で交換されるメッセージのラウンドトリップ遅延（ミリ秒単位）。
offset	システムクロックを NTP サーバーと同期させるために調整する必要があるミリ秒数。
ジッター	システムと NTP サーバー間のジッター（ミリ秒単位）。

ソフトウェア RSS の設定

Cisco Unified Computing System（USC）の NIC は、ハードウェアベースの受信側スケーリング（RSS）をサポートしています。ただし、RSS は IP トラフィックでのみサポートされています。MPLS、GTP、L2TP、GRE などの他のネットワークプロトコルでは、すべてのトラフィックが単一のキューにルーティングされます。

ASR 5500VPC-SI は、処理のために使用可能な vCPU コアに MPLS トラフィックを配信するソフトウェア RSS 機能を提供します。これにより、リソース使用率が増加し、スループットが向上します。

ソフトウェア RSS 機能は、Cisco UCS NIC ハードウェア RSS サポートを補足することができます。これは、ハードウェア NIC でサポートされていない一部のトラフィック（このリリースでのみ MPLS トラフィック）を配信することを意味します。ASR 5500VPC-SI は、包括的な RSS カバレッジを提供することもできます。つまり、すべてのトラフィックを配信します。このオプションは、RSS をサポートしていないハードウェアが使用されている場合に適用されます。

iftask sw-rss コマンドで RSS を使用するように設定します。

```
config
   iftask sw-rss {comprehensive | supplemental}
```

すべての着信トラフィックに対して RSS を設定するには、**comprehensive** キーワードを使用します。**supplemental** キーワードを使用して、ハードウェア RSS 機能でサポートされていないプロトコル（このリリースでのみ MPLS トラフィック）で RSS を設定します。

DI ネットワーク RSS の暗号化

機能の概要と変更履歴

要約データ

該当製品または機能エリア	すべて
該当プラットフォーム	VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*VPC-DI* システム管理ガイド

マニュアルの変更履歴

重要　リリース 21.2 および N5.1 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
Distributed Instance Network（DI ネットワーク）の RSS トラフィックのデフォルト設定は現在は無効になっていますが、新しい CLI コマンドを使用して有効にすることができます。以前のリリースでは、この機能は自動的に有効になっており、設定できませんでした。	21.8
最初の導入。	21.2 よりも前

変更された機能

以前の動作：21.8 よりも前のリリースでは、仮想化 StarOS インスタンスの内部分散インスタンスネットワーク（DI ネットワーク）上のすべてのトラフィックに対して Receive Side Scaling（RSS）がデフォルトで有効になっていました。

新しい動作：リリース 21.8 以降では、RSS はデフォルトで無効になっており、新しい CLI を介して有効にすることができます。

コマンドの変更

iftask di-net-encrypt-rss

この新しい CLI コマンドは、DI ネットワーク上の暗号化トラフィックでの RSS の有効化を制御するために追加されました。

```
configure
   [no] iftask di-net-encrypt-rss
   end
```

（注）　デフォルト設定では無効になっています。

SF ブート設定ポーズの設定

特定の状況下では、VPC-DI 展開内で、すべての SF が起動プロセスを完了する前に CF がブート設定を適用します。

次の構成モードコマンドを実行すると、**wait cards active** 指定されたすべてのカードが動作可能になるか、タイムアウト期間が経過するまで（いずれかの基準が最初に満たされるまで）設定が一時停止されます。一時停止は、ローカル管理コンテキストの作成と ntp/snmp 設定の直後に行われます。

このコマンドは、シャーシのロードまたはリロード後に SF がオンラインになっており、それらの SF に関する設定が適用されない（その結果、失われる）シナリオを修正します。

```
configure
   [ no ] wait cards active { all | number } [ standby number ] timeout
seconds
   end
```

注：

- **all**：すべてのアクティブモードカードが動作ステータスを達成するまで一時停止します。
- *number*：指定した数のアクティブモードカードが動作ステータスになるまで一時停止します。*number* は、アクティブモードカードの数によって 0 になります。
- **standby** *number*：（オプション）指定した数の非アクティブモードカードが動作ステータスになるまで待機します。

  number は、0 またはアクティブモード SF 用に設定されていないサービススロットの数です。
- **timeout** *seconds*：指定されたカードセットが動作ステータスになるまで、1 ～ 3600 秒待ちます。この状態が満たされた場合に、待機が終了します。それ以外の場合は、タイムアウト期間が経過すると待機が終了します。

次のコマンド例では、すべてのアクティブカードと 1 つのスタンバイカードがアクティブになるまで、最大 120 秒待機するようにシステムに指示します。

wait cards active all standby 1 timeout 120

CLI タイムスタンプの有効化

CLI で実行されるすべてのコマンドのタイムスタンプ（日付と時刻）を表示するには、Exec モードのルートプロンプトで次のコマンドを入力します。

```
timestamps
```

日付と時刻は、このコマンドを実行するとすぐに表示されます。

「設定の確認と保存」の章の説明に従って、設定を保存します。

CLI 確認プロンプトの設定

Exec モードとグローバル構成モードのさまざまなコマンドによって、コマンドを実行する前にユーザーに確認のプロンプト（[Are you sure? [Yes|No]:]）が表示されます。

この項では、次の設定について説明します。

- 現在の CLI セッション（Exec モード）またはすべての CLI セッションとユーザー（グローバル構成モード）のコマンドを自動的に確認する。

- Exec モードの **configure** コマンドと **autoconfirm** コマンドに対してのみ確認を要求する。
- Exec モード設定コマンドの確認を選択的に要求する。

自動確認の有効化

autoconfirm コマンドを使用して、設定コマンドの確認プロンプトを無効にできます。**autoconfirm** コマンドは、Exec モードおよびグローバル構成モードで使用できます。自動確認機能を有効にすると、設定コマンドプロンプトに「Yes」の応答が自動的に提供されます。これには、**リロードや**シャットダウンなどの重要なコマンドが含まれます。デフォルトでは自動確認機能は無効になっています。

Exec モードでは、自動確認は現在のインタラクティブ CLI セッションにのみ適用されます。

グローバル構成モードでは、すべての CLI ユーザーのすべての CLI セッションに自動確認が適用されます。

```
configure
   autoconfirm
   end
```

自動確認を有効にした後に無効にするには、**no autoconfirm** コマンドを使用します。

重要 コマンドガードが有効になっている場合、自動確認はコマンドガードを無効にします。

自動確認は「ease-of-use」機能として意図されています。「Are you sure?」という答えがあることを前提としています。[Y/N]" プロンプトは「Yes」になり、プロンプトをスキップします。この使用は、ユーザーがこれらの「safety-net」プロンプトを必要としないエキスパートであることを意味します。

autoconfirm コマンドと configure コマンドに対する確認の要求

autoconfirm（Exec モードとグローバル構成モード）コマンドと、グローバル構成モードの **commandguard** コマンドを介した **configure**（Exec モード）コマンドに対する確認プロンプトが必要な場合があります。

重要 autoconfirm が有効になっている場合、Exec モードとグローバル構成モードの両方で autoconfirm が無効になるまで commandguard は有効になりません。

次のコマンドシーケンスは、commandguard 機能を有効にします。

```
configure
   commandguard
   end
```

commandguard を有効にすると、次の例に示すように確認プロンプトが表示されます。

```
[local]host_name# configure
Are you sure? [Yes|No]: yes
[local]host_name(config)#
```

commandguard がいったん有効になった後に無効にするには、**no commandguard** コマンドを使用します。

commandguard のステータスは、**show configuration** コマンドで出力されます。

特定の Exec モードのコマンドに対する確認の要求

commandguard コマンドのキーワードを使用すると、自動確認が有効になっている場合でも、Exec モード構成コマンドの特定のカテゴリに対して必須のプロンプトを適用できます。

コマンド構文は次のとおりです。

```
configure
   commandguard exec-command exec_mode_category
   end
```

注：

- **exec-command** *exec_mode_category* は、Exec モード構成コマンドの次のいずれかのカテゴリを指定します。
  - card
  - clear
  - copy
  - debug
  - delete
  - filesystem
  - hd
  - reload
  - rename
  - shutdown
  - task
  - upgrade
- 複数の **commandguard exec-command** *exec_mode_category* コマンドを入力できます。
- 自動確認が有効になっているかどうかに関係なく、指定したカテゴリワードで始まる Exec モードのすべてのコマンドに確認のプロンプトを表示します。
- **no commandguard exec-command** *exec_mode_category* コマンドを使用して、特定のカテゴリの確認プロンプトをオフにすることができます。
- Exec モードコマンドに対する **commandguard exec-command** で自動確認をオーバーライドした場合、StarOS はコマンドを実行しようとしたときに自動確認がオーバーライドされた理由を示す情報メッセージを表示します。
- **-noconfirm** キーワードをサポートする Exec モード構成コマンドに対する確認プロンプトのオーバーライドを選択できます。

たとえば、**commandguard exec-command card** が有効になっている場合、確認プロンプトは次のように表示されます。

```
[local]host_name# card busy-out 1
Info: commandguard prevents autoconfirm of this command
Are you sure? [Yes|No]: yes
[local]host_name#
```

システム管理ユーザーの設定

はじめに、システムのコンテキストレベルのセキュリティ管理者を設定する方法について説明します。

この項では、次の権限を持つ追加の管理ユーザーを設定する手順について説明します。

- **セキュリティ管理者**：読み取り/書き込み権限を持ち、管理者、演算子、およびインスペクターで使用できるものを含め、すべての CLI コマンドを実行できます。
- **管理者**：読み取り/書き込み権限を持ち、CLI で任意のコマンドを実行できます。ただし、セキュリティ管理者だけが設定できるセキュリティ関連のコマンドは実行できません。管理者は、システム設定を構成または変更したり、オペレータやインスペクタで使用可能なコマンドを含め、すべてのシステムコマンドを実行したりできます。
- **オペレータ**：Execモードコマンドのより大きなサブセットに対する読み取り専用権限を持ちます。これらは、インスペクタモードの一部であるすべてのコマンドと、システムモニタリング、統計情報、および障害管理機能の一部を実行できます。オペレータには、構成モードを開始する機能がありません。
- **インスペクタ**：いくつかの読み取り専用 Exec モードコマンドに制限されます。これらのほとんどは、さまざまな統計情報や条件を表示するための **show** コマンドです。インスペクタは、**show configuration** コマンドを実行できず、設定モードを開始する権限もありません。

設定手順は、管理ユーザーのタイプ（コンテキストレベルまたはローカルユーザー）に従って分類されます。

重要 これらのユーザー権限とタイプの違いについては、「はじめに」を参照してください。

ユーザー名の文字制限

ユーザー名には、英数字（a-z、A-Z、0-9）、ハイフン、下線、およびピリオドだけを含めることができます。ハイフン文字を最初の文字にすることはできません。これは、AAA ユーザー名とローカルユーザー名に適用されます。

これらの標準規格に準拠していないユーザー名を作成しようとすると、「Invalid character」というメッセージが表示されます。有効な文字「0123456789.-_abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ」です。

コンテキストレベルの管理ユーザーの設定

このユーザータイプはコンテキストレベルで設定され、ログイン時にユーザー名とパスワードを検証するために AAA サブシステムに依存します。これは、設定ファイルを介してローカルに設定された管理ユーザーアカウント、または外部 RADIUS サーバーまたは TACACS+ サーバーの両方に当てはまります。これらのユーザータイプのパスワードは一度割り当てられ、設定ファイルでアクセスできます。

この項では、コンテキストレベルの管理ユーザータイプを設定するための情報と手順について説明します。

アカウントごとまたは認証方式ごとにシミュレーションのCLIセッションの最大数を設定することができます。セキュリティ設定と属性に影響を与えたり、システムのサービス、安定性、およびパフォーマンスに悪影響を及ぼす可能性がある特定のアカウントを保護します。同時CLIセッションの最大数は、新しいローカルユーザーログインと新しいAAAコンテキストベースのログインを試行するときに設定できます。セッションの最大数が0に設定されている場合は、ログインタイプに関係なくユーザーが認証されます。CLIタスクが開始されると、カウントを識別するためのチェックが完了します。この場合、CLIは、そのユーザーのセッション数が 0 よりも大きい 1 であると判断し、出力にエラーメッセージを表示し、starCLIActiveCount オブジェクトおよび starCLIMaxCount SNMP MIB オブジェクトと、starGlobalCLISessionsLimit アラームおよび starUserCLISessionsLimit SNMP MIB アラームを生成します。

ローカルユーザーのユーザー名におけるグローバル構成モードのコマンドの **max sessions** キーワードは、ローカルユーザーに使用可能な同時セッションの最大数を設定します。

最大セッションにおけるコンテキスト構成モードのコマンドを使用すると、管理ユーザーは、対応するユーザーに許可される最大同時セッション数を設定できます。

これらのコマンドの詳細については、『*Command Line Interface Reference* 』を参照してください。

警告期間中のパスワード変更オプション

警告期間中でも、パスワードを変更できます。たとえば、次にサンプル出力を示します。

```
When in warning period
1.Warning: Your password is about to expire in 3 days.
         We recommend you to change password.
         Logins are not allowed without acknowleding this.
         Do you want to change it now ? [y/n] (times out in 30 seconds) : n
# <you are logged in>
2.Warning: Your password is about to expire in 3 days.
         We recommend you to change password.
         Logins are not allowed without acknowleding this.
         Do you want to change it now ? [y/n] (times out in 30 seconds) : y
Auto generated password : <Jc42Q8hU>
Do you want to use auto-generated password? [y/n]: n
New password:
Repeat new password:
# <you are logged in>
```

コンテキストレベルのセキュリティ管理者の設定

追加のセキュリティ管理者を設定するには、次の例を使用します。

```
configure
  context local
    administrator user_name { [ encrypted ] [ nopassword ] password password
 }
     end
```

注：

- 追加のキーワードオプションを使用して、アクティブな管理者を識別したり、管理者に時間しきい値を設定したりできます。**administrator** コマンドの詳細については、『*Command Line Interface Reference*』を参照してください。
- **nopassword** オプションを使用すると、関連付けられたパスワードを使用せずに管理者を作成できます。認証の唯一の手段として ssh 公開キー（SSH 構成モードの **authorized key** コマンド）を使用する場合は、このオプションを有効にします。このオプションを有効にすると、管理者パスワードを使用してユーザーアカウントにアクセスできなくなります。

「設定の確認と保存」の章の説明に従って、設定を保存します。

コンテキストレベルの管理者の設定

次の例を使用して、コンテキストレベルの設定管理者を設定します。

```
configure
  context local
    config-administrator user_name { [ encrypted ] [ nopassword ] password
 password }
     end
```

注：

- 追加のキーワードオプションを使用して、アクティブな管理者を識別したり、管理者に時間しきい値を設定したりできます。**config-administrator** コマンドの詳細については、『*Command Line Interface Reference*』を参照してください。
- **nopassword** オプションを使用すると、関連付けられたパスワードを使用せずに設定管理者を作成できます。認証の唯一の手段として ssh 公開キー（SSH 構成モードの **authorized key** コマンド）を使用する場合は、このオプションを有効にします。このオプションを有効にすると、設定管理者パスワードを使用してユーザーアカウントにアクセスできなくなります。

「設定の確認と保存」の章の説明に従って、設定を保存します。

コンテキストレベルのオペレータの設定

次の例を使用して、コンテキストレベルのオペレータを設定します。

```
configure
  context local
```

```
operator user_name { [ encrypted ] [ nopassword ] password password }
end
```

注：

- 追加のキーワードオプションを使用して、アクティブな管理者を識別したり、管理者に時間しきい値を設定したりできます。オペレータコマンドの詳細については、『**Command Line Interface Reference**』を参照してください。
- **nopassword** オプションを使用すると、関連付けられたパスワードなしでオペレータを作成できます。認証の唯一の手段として ssh 公開キー（SSH 構成モードの **authorized key** コマンド）を使用する場合は、このオプションを有効にします。このオプションを有効にすると、オペレータパスワードを使用してユーザーアカウントにアクセスできなくなります。

「設定の確認と保存」の章の説明に従って、設定を保存します。

コンテキストレベルのインスペクタの設定

次の例を使用して、コンテキストレベルのインスペクタを設定します。

```
configure
  context local
    inspector user_name { [ encrypted ] [ nopassword ] password password
}
    end
```

注：

- 追加のキーワードオプションを使用して、アクティブな管理者を識別したり、管理者に時間しきい値を設定したりできます。**Inspector** コマンドの詳細については、『*Command Line Interface Reference*』を参照してください。
- **nopassword** オプションを使用すると、関連付けられたパスワードを使用することなくインスペクタを作成できます。認証の唯一の手段として ssh 公開キー（SSH 構成モードの **authorized key** コマンド）を使用する場合は、このオプションを有効にします。このオプションを有効にすると、インスペクタパスワードを使用してユーザーアカウントにアクセスできなくなります。

「設定の確認と保存」の章の説明に従って、設定を保存します。

LI 管理者の設定

重要 セキュリティ上の理由から、**li-administration** アカウントは、一般的なシステム管理ではなく、合法的傍受（LI）機能でのみ使用するよう制限する必要があります。セキュリティ管理者と管理者のみが、LI 権限をプロビジョニングできます。司法当局（LEA）の基準に従ってセキュリティを確保するために、LI 管理ユーザーは、セキュアシェル（SSH）プロトコルのみを使用してシステムにアクセスする必要があります。LI 権限は、システム全体の単一コンテキスト内で使用するように設定することもできます。詳細については、『*Lawful Intercept Configuration Guide*』と合法的傍受のプロビジョニング （21 ページ）を参照してください。

次の例を使用して、コンテキストレベルの LI 管理者を設定します。

```
configure
   context context_name
     administrator user_name { [ encrypted ] [ nopassword ] password password
 li-administrator}
     end
```

LI管理者とびLI以外の管理者は、合法的傍受のCLIコマンドを設定できます。ただし、グローバル構成モードの **require segregated li-configuration** コマンドが有効になっている場合は、信頼できるビルドと通常のビルドに暗号化された合法的傍受のCLIコマンドを表示できます。詳細については、『*Lawful Intercept Configuration Guide*』とシステムと LI 設定の分離 （18 ページ）を参照してください。

システムと LI 設定の分離

合法的傍受（LI）の設定には、機密情報が含まれています。通常のビルドのデフォルトでは、li-administration 権限のない管理者が LI 設定コマンドを表示できます。ただし、LI 設定コマンドの表示は、システム設定の残りの部分から制限したり、分離したりすることができます。

グローバル構成モードの **require segregated li-configuration** コマンドによって、システムおよび合法的傍受の CLI の表示は永続的に分離されます。合法的傍受のキーワードを指定した CLI コマンドは暗号化され、li-administration 権限を持つ管理者によってのみ表示できます。

重要 信頼できるビルドでは、LIの分離はオンになっており、無効にすることはできません。**require segregated li-configuration**コマンドは非表示です。

システム設定から LI 設定を分離すると、StarOS に次の影響があります。

- li-administration 権限を持つ管理者のみが、**show configuration** コマンドの出力で合法的傍受の CLI コマンドを確認できます。
- **save configuration** コマンドを実行すると、合法的傍受のCLI設定コマンドが自動的に暗号化されます。
- CLI コマンドを介して保存された構成ファイルをロードすると（たとえば、**configure** <*url*>）、暗号化済み合法的傍受の CLI コマンドは、LI 権限を持つ管理者に対してのみ復号および実行されます。LI 権限のない管理者の場合は、暗号化済み合法的傍受の CLI コマンドは復号および実行されません。
- 起動設定がロードされているシステム起動中に、暗号化済み合法的傍受の設定が復号され、サイレントにロードされます。つまり、合法的傍受のCLI設定はコンソールポートに表示されません。
- Exec モードの **configure** コマンドは、LI 管理者が保存された構成ファイルから、暗号化された合法的傍受の設定のみをロードできるようにするキーワードをサポートするようになりました（たとえば、**configure encrypted** <*url*> など）。**暗号化された**キーワードは、LI 管理者のみが実行できます。

- 暗号化済み合法的傍受の設定（分離されたLI）を使用してシステムを実行している場合、**show boot initial config** コマンドの出力には、最初の起動時に2番目のパスを実行する必要があるかどうかを示す行が含まれています。この行には、暗号化済み合法的傍受の設定が処理された場合は「encrypted li」と表示されます。その行に「encrypted li errors」と表示されている場合は、2番目のパスが正しく動作しなかったか、予期されていないまたは本来の情報ではない出力が提供されています。
- li-administration 権限を持つユーザーは、**show logs encrypted-li** コマンドを使用して、暗号化済み合法的傍受の設定におけるブート設定の出力を表示できます。

グローバル構成モードの **require segregated li-configuration** コマンドと関連コマンドの詳細については、『*Lawful Intercept Configuration Guide*』の付録「*Lawful Intercept CLI Commands*」を参照してください。

（注） 『*Lawful Intercept Configuration Guide*』は、www.cisco.com では利用できません。このガイドのコピーを入手するには、シスコのアカウント担当者にお問い合わせください。

リリース 21.4 以降（信頼できるビルドのみ）：

- ユーザーは、それぞれのコンテキストインターフェイスを使用してのみシステムにアクセスできます。
- ユーザーが別のコンテキストインターフェイスを使用してそれぞれのコンテキストにログインしようとすると、そのユーザーは拒否されます。
- ユーザーが「authorized-keys」または「allowusers」のいずれかのコンテキストに設定されているかどうかに関係なく、この機能では、独自のコンテキストインターフェイス以外のコンテキストインターフェイスを介してログインを試行すると、これらのユーザーは拒否されます。
- ローカル以外のコンテキストに設定されているユーザーは、ログインを試行するコンテキストを指定する必要があります。例：

  ssh username@ctx_name@ctx_ip_addrs

コンテキストレベルの管理ユーザー設定の確認

設定が正常に行われたことを確認するには、次のコマンドを入力します。

show configuration context local

このコマンドは、このセッション時にローカルコンテキスト内で変更したすべての設定パラメータを表示します。次に、このコマンドの出力例を示します。この例では、*testadmin* という名前のセキュリティ管理者が設定されています。

```
config
  context local
    interface mgmt1
      ip address 192.168.1.10 255.255.255.0
    #exit
```

```
    subscriber default
    #exit
    administrator testadmin encrypted password fd01268373c5da85
    inspector testinspector encrypted password 148661a0bb12cd59
exit
  port ethernet 5/1
    bind interface mgmt1 local
  #exit
```

ローカルユーザーの管理ユーザーの設定

ローカルユーザータイプは、ANSI T1.276-2003 のパスワードセキュリティ保護をサポートしています。パスワード、パスワード履歴、ロックアウト状態などのローカルユーザーアカウント情報は、/flash で維持されます。この情報は、AAA ベースの認証の対象となる個別のローカルユーザーデータベースにただちに保存され、システムの残りの部分では使用されません。そのため、設定されているローカルユーザーアカウントは、システム設定の残りの部分では表示されません。

重要 ローカルユーザーデータベースが無効になっています。グローバル構成モードの **local-user** コマンドと Exec モードの **show local-user** コマンド、および **update local-user** コマンドは使用できません。信頼できるビルドの詳細については、「システム操作と設定」の章を参照してください。

次の例を使用して、ローカルユーザーの管理ユーザーを設定します。

```
configure
   local-user username name
   end
```

注：

- 追加のキーワードオプションを使用して、アクティブな管理者を特定したり、管理者に時間のしきい値を設定したりできます。*local-user username* コマンドの詳細については、『**Command Line Interface Reference**』を参照してください。

ローカルユーザーデータベースの詳細については、ローカルユーザーデータベースの更新とダウングレード （21 ページ）を参照してください。

ローカルユーザー設定の確認

設定が正常に行われたことを確認するには、次のコマンドを入力します。

```
show local-user verbose
```

このコマンドは、設定されたローカルユーザーの管理ユーザーに関する情報を表示します。次に、このコマンドの出力例を示します。この例では、*SAUser* という名前のローカルユーザーが設定されています。

```
Username:                SAUser
  Auth Level:            secadmin
  Last Login:            Never
```

```
Login Failures:         0
Password Expired:       Yes
Locked:                 No
Suspended:              No
Lockout on Pw Aging:    Yes
Lockout on Login Fail: Yes
```

ローカルユーザーデータベースの更新

次の Exec モードコマンドを実行して、ローカルユーザー（管理）設定を更新します。このコマンドは、管理ユーザーを作成、削除、または編集した直後に実行する必要があります。

update local-user database

ローカルユーザーデータベースの更新とダウングレード

PBKDF2（パスワードベースのキー派生関数バージョン 2）を使用し、入力されたデータ、ソルト、および反復回数に基づいて、特定の長さのキーを取得します。ローカルユーザーアカウントのパスワードは、ランダムに生成されたソルトと多くの反復回数を備えたPBKDF2方式を使用してハッシュされ、パスワードストレージの保護が強化されます。

リリース20.0にアップグレードする場合、ローカルユーザーデータベース内の既存のユーザーパスワードはMD5からPBKDF2ハッシングに自動的にアップグレードされません（ハッシュされたパスワード値のみが保存されます）。ハッシュ関数は一方向であるため、保存されたハッシュ値からユーザーパスワードを取得することはできません。したがって、既存のハッシュパスワードを強力なハッシュパスワードに自動的に変換することはできません。

データベースを更新するには、セキュリティ管理者がExecモードの**update local-user database** CLIコマンドを実行する必要があります。このコマンドを実行すると、StarOSは/flashディレクトリからデータベースを読み取り、データベースを新しい形式で再構築してディスクに書き込みます。

一時停止されたユーザーを再アクティブ化するには、セキュリティ管理者が次の手順を実行します。

- Execモードの **password change local-user** *username* コマンドを使用して、一時停止されたユーザーの一時パスワードを設定します。
- 構成モードの **no suspend local-user** *username* コマンドを使用して、ユーザーの一時停止フラグをリセットします。

合法的傍受のプロビジョニング

合法的傍受（LI）機能を使用すると、ネットワークオペレータは、ターゲットのモバイルユーザー間の制御メッセージとデータメッセージを代行受信できます。司法命令や令状とともに、法執行機関（LEA）はネットワークオペレータに対し特定のモバイルユーザーの代行受信の開始を求めます。

合法的傍受を行うために従うべき規範は国によって異なります。『*LI Configuration Guide*』では、この機能の仕組みと、合法的傍受をサポートしているStarOSの各サービスでのこの機能

の設定方法とモニター方法について説明しています。このガイドは、www.cisco.com では入手できません。入手するには、シスコのアカウント担当者にご連絡ください。

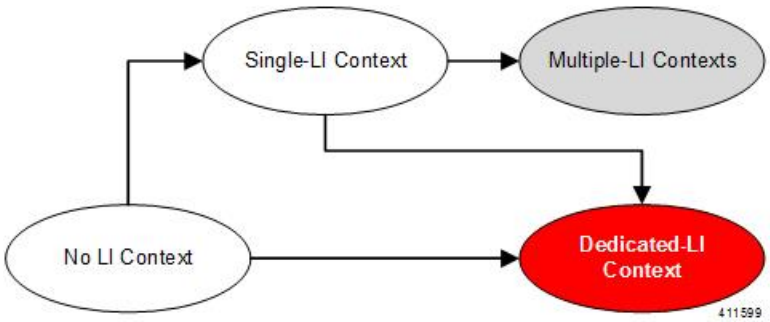
合法的傍受のプロビジョニングに関するセキュリティ関連の制限事項については、「システムセキュリティ」の章の「合法的傍受の制約事項」の項を参照してください。

LI は、1 つ以上の StarOS コンテキスト内でプロビジョニングできます。**li-administration** 権限を持つ管理ユーザーは、LI機能をサポートするコンテキストに関連付けられています。この管理者は、LI 機能をプロビジョニングする CLI 設定コマンドにアクセスできます。

StarOS システム設定内では、いくつかのタイプの LI 設定がサポートされています。

- **LI コンテキストなし**：すべてのコンテキストに対して LI 設定が入力されていません。
- **単一の LI コンテキスト**：LI 設定は 1 つのコンテキスト内に入力されているが、他のコンテキスト内では入力されていませんでした。この状態では、別のコンテキストが LI 設定で設定されている場合に、1 つの LI コンテキストを複数の LI コンテキストに変換できます。または、コンテキスト構成モードの **dedicated-li** コマンドを入力して、このコンテキストを専用 LI コンテキストに変換することもできます。
- **複数の LIは コンテキスト**：LI 設定を使用して 2 つ以上のコンテキストが設定されています。複数の LI コンテキスト設定は、他のどのタイプの LI 設定としても再設定できません。
- **専用 LI コンテキスト**：既存のシステム設定が LI コンテキストなしか 1 つの LI コンテキストのシステムの場合は、コンテキスト構成モードの **dedicated-li** コマンドを入力することで、専用 LI コンテキストシステムに変換できます。専用 LI コンテキストは、LI 設定へのアクセスを、それを必要とする 1 つの VPN コンテキストに制限します。専用 LI コンテキストシステムとして設定されると、その他のどのタイプの LI コンテキストシステムにも再設定できません。専用 LI コンテキストの作成を試みる前に、『*Lawful Intercept Configuration Guide*』を参照してください。

図 *1: LI* コンテキストの設定



リリース 21.4 以降（信頼できるビルドのみ）：

- ユーザーは、それぞれのコンテキストインターフェイスを使用してのみシステムにアクセスできます。
- ユーザーが別のコンテキストインターフェイスを使用してそれぞれのコンテキストにログインしようとすると、そのユーザーは拒否されます。

- ユーザーが「authorized-keys」または「allowusers」のいずれかのコンテキストに設定されているかどうかに関係なく、この機能では、独自のコンテキストインターフェイス以外のコンテキストインターフェイスを介してログインを試行すると、これらのユーザーは拒否されます。
- ローカル以外のコンテキストに設定されているユーザーは、ログインを試行するコンテキストを指定する必要があります。例：

  ssh username@ctx_name@ctx_ip_addrs

指定されたルートディレクトリへのユーザーアクセスの制限

デフォルトでは、FTP/SFTP アクセス権を持つ管理者ユーザーは、/mnt/user/ ディレクトリの下にある任意のファイルにアクセスし、変更を加えることができます。次のディレクトリに「オールオアナッシング」ベースでアクセスが許可されます。/flash、/cdrom、/hdraid、/records、/usb1、/usb2

管理者または設定管理者は、ファイルディレクトリとアクセス権限を使用して SFTP サブシステムのリストを作成できます。ローカルユーザーが作成されると、管理者は SFTP サブシステムを割り当てます。ユーザーの承認レベルがセキュリティ管理者または管理者でない場合、ユーザーは読み取り専用権限を持つサブシステムにのみアクセスできます。このディレクトリは、ユーザーのルートディレクトリとして使用されます。この情報は、openssh sftp サーバーに渡される環境変数として設定されます。

SFTP ルートディレクトリは、ローカルユーザー、管理者、および設定管理者と関連付ける前に作成する必要があります。複数の SFTP ディレクトリを作成できます。各ディレクトリは、1 人以上のユーザーに割り当てることができます。

SFTP ルートディレクトリの設定

subsystem sftp コマンドを使用すると、SFTP ルートディレクトリおよび関連付けられているアクセス権限レベルを割り当てることができます。

```
configure
   context local
      server sshd
        subsystem sftp  [ name sftp_name root-dir pathname mode { read-only
 | readwrite } ]
```

注：

- *sftp_name* は、このサブシステムを一意に識別する英数字の文字列です。
- *pathname* は、SFTP ファイルの転送先となるルートディレクトリを指定します。次のオプションがあります。
  - /hd-raid/records/cdr
  - /flash

SFTP ルートディレクトリとローカルユーザーの関連付け

local-user username コマンドを使用すると、管理者は SFTP ルートディレクトリを指定されたユーザー名に関連付けることができます。

```
configure
  local-user username user_name authorization-level level ftp sftp-server
 sftp_name password password
  exit
```

SFTP ルートディレクトリと管理者の関連付け

administrator コマンドを使用すると、管理者は、指定された管理者に SFTP ルートディレクトリを関連付けることができます。

```
configure
   context local
     administrator user_name password password ftp sftp-server sftp_name
     exit
```

SFTP ルートディレクトリと設定管理者の関連付け

config-administrator コマンドを使用すると、管理者は、指定された設定管理者に SFTP ルートディレクトリを関連付けることができます。

```
configure
   context local
    config-administrator user_name password password ftp sftp-server sftp_name
     exit
```

システム管理ユーザー用の TACACS+ の設定

ここでは、ASR 5500VPC-SI の TACACS+（Terminal Access Controller Access Control System+）AAA（認証、許可、およびアカウンティング）サービスの機能と設定について説明します。

動作

TACACS+は、セキュアな暗号化されたプロトコルです。管理ユーザーアカウントデータベースを使用してプロビジョニングされた TACACS+ サーバーにリモートでアクセスすることで、ASR 5500VPC-SI システムはシステム管理ユーザーに TACACS+ AAA サービスを提供できます。TACACS+ は、UDP ではなく TCP を使用する TACACS プロトコルの拡張バージョンです。

システムは、TACACS+ ネットワークアクセスサーバー（NAS）として機能します。NAS として、承認されたシステム管理ユーザーに代わって、システムが TACACS+ AAA サービスを要求します。正常に認証されるには、システムがアクセスするのと同じローカルコンテキストとネットワーク内にTACACS+ サーバーが存在する必要があります。

システムは、TACACS+マルチ接続モードをサポートしています。マルチ接続モードでは、セッションごとに TACACS+ サーバーへの個別のプライベート TCP 接続が開き、維持されます。TACACS+ セッションが終了すると、サーバーへの接続が終了します。

TACACS+ は、ASR 5500VPC-SI 上のシステム全体を網羅する機能です。TACACS+ AAA サービスの設定は、TACACS 構成モードで実行されます。TACACS+ 機能の有効化は、グローバル構成モードで実行されます。システムでは、最大 3 台の TACACS+ サーバーの設定がサポートされます。

システムで設定して有効にすると、TACACS+ 認証が最初に試行されます。デフォルトでは、TACACS+ 認証が失敗すると、システムは RADIUS などの TACACS+ 以外の AAA サービスを使用してユーザーの認証を試行します。

アカウントごとまたは認証方式ごとにシミュレーションの CLI セッションの最大数を設定することができます。セキュリティ設定と属性に影響を与えたり、システムのサービス、安定性、およびパフォーマンスに悪影響を及ぼす可能性がある特定のアカウントを保護します。同時 CLI セッションの最大数は、新しい TACACS+ ユーザーログインを試行するときに設定できます。最大セッション機能を使用するには、TACACS + サーバー属性オプションのオプションを使用することを**推奨します**。2 番目の方法は、**user-id** コマンドに **maxsess** キーワードを指定して StarOS CLI 構成モードの TACACS+ モードを使用することです。セッションの最大数が 0 に設定されている場合は、ログインタイプに関係なくユーザーが認証されます。CLI タスクが開始されると、カウントを識別するためのチェックが完了します。この場合、CLI は、そのユーザーのセッション数が 0 よりも大きい 1 であると判断し、出力にエラーメッセージを表示し、starCLIActiveCount オブジェクトおよび starCLIMaxCount SNMP MIB オブジェクトと、starGlobalCLISessionsLimit アラームおよび starUserCLISessionsLimit SNMP MIB アラームを生成します。

max-sessions TACACS+ 構成モード コマンドは、TACACS+ で使用可能なセッションの最大数を設定します。また、 **user-id** TACACS+ 構成モード コマンドの **default** オプションは、特定の TACACS+ ユーザー識別子にデフォルトの属性を設定します。これらのコマンドの詳細については、『*Command Line Interface Reference* 』を参照してください。

重要 ユーザーは、StarOS と TACACS+ サーバーの両方の設定で使用可能なシミュレーション CLI セッションの最大数を定義できます。ただし、このオプションを使用しないことを強く推奨します。

重要 TACACS+ アカウンティング（CLI イベントロギング）は、権限レベルが 15 と 13 に設定されている合法的傍受ユーザーに対しては生成されません。

ユーザーアカウントの要件

TACACS+ AAA サービスを設定する前に、次の TACACS+ サーバーと StarOS ユーザーアカウントのプロビジョニング要件に注意してください。

TACACS+ ユーザーアカウントの要件

TACACS+ サーバーは、次の TACACS+ ユーザーアカウント情報を使用してプロビジョニングする必要があります。

- 既知の管理ユーザーのリスト。
- 各ユーザーのプレーンテキストまたは暗号化されたパスワード。
- 各ユーザーが属するグループの名前。
- ユーザーグループのリスト。
- 各グループで許可/拒否される TACACS+ の特権レベルとコマンド。

重要 TACACS+ の権限レベルは、ネットワークの TACACS+ サーバーデータベースに属性値ペア（AVP）として保存されます。ユーザーは、権限レベルに関連付けられた一連のコマンドに制限されます。次の表で、TACACS+ の権限レベルを StarOS CLI の管理ロールと責任にマッピングする方法を説明します。

CLI 管理ロールへの TACACS+ 権限レベルのデフォルトマッピングを表示するには、Exec モードの **show tacacs priv-lvl** コマンドを実行します。デフォルトのマッピングは、StarOS リリースとビルドタイプによって異なります。

Tacacs+ の権限レベルをデフォルトの StarOS 認証値から再設定するには、TACACS+ 構成モードの **priv-lvl** コマンドと **user-id** コマンドを使用します。詳細については、『*Command Line Interface Reference*』の「*TACACS+ Configuration Mode Commands*」の章を参照してください。

重要 FTP はサポートされていません。

StarOS ユーザーアカウントの要件

システムへの管理アクセスが許可されている TACACS+ ユーザーには、StarOS で次のユーザーアカウント情報が定義されている必要があります。

- ユーザ名
- パスワード
- 管理ロールと権限

重要 システムでユーザーと管理者の権限を定義する手順については、「システム管理ユーザーの設定」を参照してください。

TACACS+ AAA サービスの設定

この項では、システム上の管理ユーザーに TACACS+ AAA サービスを設定する方法について説明します。

⚠

注意 TACACS+ AAA サービスを初めて設定する場合は、管理者ユーザーが StarOS にログインするために TACACS+ 以外のサービスを使用する必要があります。そうしないと、TACACS+ ユーザーはシステムへのアクセスが拒否されます。

TACACS+ 以外のサービスを使用してシステムにログインします。

システムで TACACS+ AAA サービスを設定するには、次の例を使用します。

```
configure
   tacacs mode
      server priority priority_number ip-address tacacs+srvr_ip_address
      end
```

（注）

- **server priority** *priority_number*：TACACS+ サーバーが TACACS+ 認証を試行する順序を指定する 1 ～ 4 の整数である必要があります。優先順位は 1 が最も高く、4 が最も低くなります。優先順位の数値は、設定されている TACACS+ サーバーに対応します。
- **ip-address**：有効な TACACS+ サーバーの IPv4 アドレスである必要があります。これを使用し、TACACS+ AAA サービスを介してこのシステムにアクセスする管理ユーザーを認証します。
- デフォルトでは、TACACS+設定によって、認証、許可、およびアカウンティングの各サービスが提供されます。

StarOS で TACACS+ を有効にします。

```
configure
   aaa tacacs+
   end
```

詳細については、コンソールの TACACS+ 認証の無効化 （29 ページ）を参照してください。

「設定の確認と保存」の章の説明に従って、設定を保存します。

👉

重要 すべての TACACS+ 構成モードのコマンドとオプションの詳細については、『*Command Line Reference*』の「*TACACS Configuration Mode Commands*」の章を参照してください。

非ローカル VPN 認証のための TACACS+ の設定

デフォルトでは、TACACS+ 認証はローカルコンテキストへのログインに関連付けられています。TACACS+認証は、非ローカルコンテキストVPNログイン用に設定することもできます。TACACS+ は、以下で説明するオプションを使用して設定し、有効にする必要があります。

stop キーワードオプションは、TACACS+ 構成モードの **on-unknown-user** コマンドで使用できます。TACACS+ がコマンドキーワードオプションで有効になっている場合、ユーザーがログインを試行する VPN コンテキスト名は、ユーザー名文字列で指定された VPN 名と一致している必要があります。コンテキスト名が一致しない場合、ログインは失敗して終了します。

このオプションを指定しないと、ログインシーケンスは代替ログイン方式を介して別のコンテキストで認証を試行します。たとえば、**on-unknown-user stop** の設定がない場合、管理者アカウントは、非ローカルの VPN コンテキストを介してローカルコンテキストにログインできます。ただし、**on-unknown-user stop** の設定では、ローカルコンテキストのログインは試行されず、管理者アカウントのログイン認証は失敗します。

```
configure
   tacacs mode
      on-unkown-user stop ?
      end
```

TACACS+ の設定の確認

この項では、TACACS+ 設定の確認方法について説明します。

システム CLI からログアウトし、TACACS+ サービスを使用して再度ログインします。

重要 StarOS で TACACS+ AAA サービスを設定して有効にすると、システムは最初に TACACS+ AAA サービスを介して管理ユーザーを認証しようとします。デフォルトでは、TACACS+ 認証が失敗した場合、システムは TACACS+ AAA 以外のサービスを使用して認証を続行します。

Exec モードのプロンプトで、次のコマンドを入力します。

```
show tacacs [ client | priv-lvl | session | summary ]
```

show tacacs コマンドの出力には、ユーザー名、ログイン時刻、ログインステータス、現在のセッション状態、権限レベルなどのサマリー情報がアクティブな TACACS+ セッションごとに表示されます。 オプションのフィルタキーワードによって、追加情報が表示されます。

次に、このコマンドの出力例を示します。この例では、*asradmin* という名前のシステム管理ユーザーが、TACACS+ AAA サービスを介してシステムに正常にログインしています。

```
active session #1:
   login username               : asradmin
   login tty                    : /dev/pts/1
   time of login                : Fri Oct 22 13:19:11 2011
   login server priority        : 1
   current login status         : pass
   current session state        : user login complete
   current privilege level      : 15
   remote client application    : ssh
   remote client ip address     : 111.11.11.11
   last server reply status     : -1
total TACACS+ sessions          : 1
```

重要 すべての TACACS+ メンテナンスコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

TACACS+ サーバーでの IPv6 アドレスサポート

認証方式の分離

コンソールポートにアクセスし、SSH/telnet セッション（vty 回線）を確立するための個別の認証方式を設定できます。

TACACS+ をグローバルに設定すると、コンソールおよび vty 回線へのアクセスは両方ともその方式を使用して認証されます。

コンソールポートは StarOS への最後のリゾートアクセスであるため、コンソールのローカル認証を設定し、vty 回線に TACACS+ を使用することができます。

重要 この機能は、AAA（認証、許可、およびアカウンティング）サービス、およびローカルユーザーに対して拡張されます。たとえば、ローカルユーザーは、vty 回線を介してのみアクセス権を持つコンソールアクセスおよび AAA（VPN コンテキスト）ユーザーのみを持つことができます。

認証方式（コンソールと vty 回線）を分離するには、認証のタイプに基づいてユーザーのコンソールアクセスを無効にする必要があります。

コンソールの TACACS+ 認証の無効化

グローバル構成モードの **aaa tacacs+** コマンドの **noconsole** キーワードは、コンソール回線での TACACS+ 認証を無効にします。

```
configure
  aaa tacacs+ noconsole
  exit
```

デフォルトでは、TACACS+ サーバー認証は、コンソールまたは vty 回線からのログインに対して実行されます。**noconsole** を有効にすると、コンソール回線のローカルデータベース認証を優先して TACACS+ 認証がバイパスされます。vty 回線では、TACACS+ は有効のままになります。

重要 **aaa tacacs+ noconsole** が設定されている場合は、有効なログイン情報を持つローカルユーザーがコンソールポートにログインできます。**on-authen-fail stop** と **on-unknown-user stop** が TACACS+ 構成モードでイネーブルになっている場合でも、コンソールポートにログイン可能です。ユーザーが TACACS+ ユーザーでない場合、vty 回線でログインできません。

コンソールの AAA ベースの認証を無効化

グローバル構成モードの **local-user allow-aaa-authentication** コマンドの **noconsole** キーワードは、コンソール回線での AAA ベースの認証を無効にします。

```
configure
  local-user allow-aaa-authentication noconsole
  exit
```

ローカルユーザー認証は、AAA ベースの認証と **local-user allow-aaa-authentication noconsole** が有効になる前に常に実行されるため、**no local-user allow-aaa-authentication** が設定されている場合と同じに動作します。VTY 回線には影響しません。

重要 このコマンドは、ローカルで使用されているデータベースが使用できないため、信頼できるビルドには適用されません。

コンテキストレベルで TACACS+ 認証を無効化

グローバル構成モードで **aaa tacacs+**を有効にすると、TACACS+ 認証はすべてのコンテキスト（ローカルおよび非ローカル）に自動的に適用されます。一部のネットワーク展開では、特定のコンテキストに対して TACACS+ サービスを無効にすることができます。

コンテキスト内で TACACS+ サービスを無効にするには、**no aaa tacacs+** コンテキスト設定コマンドを使用します。

```
configure
  context ctx_name
    no aaa tacacs+
```

以前に無効にされていたコンテキスト内で TACACS+ サービスを有効にするには、**aaa tacacs+** コンテキスト設定コマンドを使用します。

重要 コンテキストレベルでサービスを選択的に無効にするには、その前に、グローバル構成モード（すべてのコンテキスト）で AAA TACACS+ サービスを有効にする必要があります。グローバルに有効になっていない場合は、コンテキストレベルで TACACS+ サービスを選択的に有効にすることはできません。

コンソール/VTY 回線でのローカルユーザーログインの制限

StarOSユーザーを作成するときのセキュリティ管理者は、そのユーザーがコンソールを使用してログインするか、またはVTY回線を使用してログインするかを指定できます。グローバル構成モードの **local-user username** コマンドの **[noconsole | novty]** キーワードはこれらのオプションをサポートしています。

```
configure
  local-user username <username> [ noconsole | novty ]
  exit
```

noconsole キーワードを指定すると、ユーザーはコンソールポートにログインできなくなります。**novty** キーワードを指定すると、ユーザーはSSHまたはtelnetセッションを介してログインできなくなります。どちらのキーワードも指定されていない場合は、コンソールとVTY回線の両方へのアクセスが許可されます。

重要 **noconsole** キーワードまたは **novty** キーワードの使用は、新しいローカルユーザーデータベース形式でのみサポートされています。**update local-user database** を実行していない場合は、これらのキーワードを有効にする前に実行する必要があります。そうしないと、**noconsole** キーワードと **novty** キーワードはローカルユーザーデータベースに保存されません。システムの再起動後も、すべてのユーザーがコンソールとVTY回線にアクセスできます。詳細については、ローカルユーザーデータベースの更新とダウングレード （21 ページ）を参照してください。

重要 このコマンドは、ローカルで使用されているデータベースが使用できないため、信頼できるビルドには適用されません。

AAA ベースのユーザーのコンソールアクセスの制限

AAAベースのユーザーは、通常、VTY回線を介してログインします。ただし、一部のユーザーはコンソール回線にだけアクセスするように制限することもできます。ローカルユーザーデータベースを使用しない場合（または信頼できるビルドを実行している場合）は、他のAAAベースのユーザーについてはコンソール回線へのアクセスを制限することでこれを行う必要があります。コンソール回線にアクセスできないすべてのレベルの管理者ユーザーに対して **noconsole** キーワードを有効にします。

noconsole キーワードは、次に示すコンテキスト構成モード コマンドで使用できます。

```
configure
  context <ctx_name>
   administrator <username> { encrypted | nopassword | password } noconsole

   config-administrator <username> { encrypted | nopassword | password }
 noconsole
   inspector <username> { encrypted | nopassword | password } noconsole
```

```
operator <username> { encrypted | nopassword | password } noconsole
exit
```

noconsole キーワードを指定すると、コンソール回線へのユーザーアクセスが無効になります。デフォルトでは、**noconsole** は有効になっていないため、すべての AAA ベースのユーザーがコンソール回線にアクセスできます。

重要 **local-user allow-aaa-authentication noconsole** コマンドが優先されます。この場合、すべての AAA ベースのユーザーがコンソール回線にアクセスできません。

設定変更の確認

Exec モードの **show configuration** コマンドを使用して、認証方式の分離に関連した変更を確認できます。設定変更を保存した後、**show configuration | grep noconsole** および **show configuration | grep novty** を実行します。これらのコマンドの出力には、実行したすべての変更が示されます。

シャーシキーの設定

シャーシキーは、システムごとに設定する必要があります。このキーは、構成ファイルにある暗号化されたパスワードを復号するために使用されます。

概要

シャーシキーは、設定ファイル内の暗号化されたパスワードを暗号化および復号するために使用されます。2 つ以上のシャーシが同じシャーシキー値で設定されている場合、暗号化されたパスワードは、同じシャーシキー値を共有するシャーシのいずれかで復号できます。そのため、特定のシャーシキー値は、異なるシャーシキー値で暗号化されたパスワードは復号できません。

シャーシキーは、ファイルに保存され、設定ファイル内の機密データ（パスワードや秘密など）を保護するためのマスターキーとして使用されるシャーシ ID を生成するために使用されます。

シャーシ ID はシャーシキーの SHA256 ハッシュです。シャーシキーは、CLI コマンドまたはクイック セットアップウィザードを使用してユーザーが設定できます。シャーシ ID が存在しない場合、シャーシ ID を生成するにはローカル MAC アドレスを使用します。

ユーザーはクイック セットアップ ウィザードまたは CLI コマンドを使用して、シャーシキーを明示的に設定する必要があります。設定されていない場合、ローカル MAC アドレスを使用してもデフォルトのシャーシ ID は生成されません。シャーシキー（つまり、シャーシ ID）がない場合、機密データは保存された設定ファイルには表示されません。シャーシ ID は、ユーザーが入力したシャーシキーおよび32バイトのセキュアな乱数による SHA256 ハッシュ（base36

形式で暗号化）です。これにより、キーセキュリティを得るためにシャーシキーとシャーシ ID には 32 バイトのエントロピーが確保されます。

シャーシ ID を使用できない場合、設定ファイル内の機密データの暗号化と復号は機能しません。

新しいシャーシキーの値の設定

CLI コマンド

重要 **chassis key value** コマンドと **chassis keycheck** コマンドが実行できるのは、セキュリティ管理者権限を持つユーザーのみです。

新しいシャーシキーを入力するには、Exec モードの **chassis key value** *key_string* コマンドを使用します。

key_string は、1 ～ 16 文字の英数字文字列です。シャーシキーは、パスワードのように一方向の暗号化された値として保存されます。このため、シャーシキーの値がプレーンテキスト形式で表示されることはありません。

Exec モードの **chassis keycheck** *key_string* コマンドは、入力した *key_string* に基づいて一方向の暗号化されたキー値を生成します。生成された暗号化キーの値は、以前に入力したシャーシキー値の暗号化されたキー値と比較されます。暗号化された値が一致すると、コマンドは成功し、キーチェックに合格します。比較に失敗した場合は、キーチェックが失敗したことを示すメッセージが表示されます。デフォルトのシャーシキー（MAC アドレス）が現在使用されている場合、比較するシャーシキー値がないため、このキーチェックは常に失敗します。

複数のシャーシが同じシャーシキー値を共有しているかどうかを確認するには、**chassis keycheck** コマンドを使用します。

重要 既存のシャーシ ID ファイルが存在しない場合、**chassis keycheck** コマンドは非表示になります。

詳細については、『*Command Line Interface Reference*』の「*Exec Mode Commands*」の章を参照してください。

シャーシ ID は、より安全なアルゴリズムを使用して、シャーシキーから生成されます。結果として得られる 44 文字のシャーシ ID は、同じファイルに保存されます。

シャーシ ID ファイルがすでに存在しているシャーシでは、何も変更されません。ただし、両方の管理カードにシャーシ ID ファイルがなくなった場合、既存のすべての設定ファイルが無効になります。元の値と同じ新しいシャーシキーを入力しても、シャーシ ID の生成には新しい方法が使用されているため、問題は解決しません。

⚠

注意 新しいシャーシキーを設定した後、リロードを開始する前に設定を保存する必要があります。「設定の確認と保存」の章を参照してください。

クイック セットアップ ウィザード

シャーシ ID ファイルが存在しない場合、クイック セットアップ ウィザードにより、ユーザーにシャーシキーを入力するように求めるプロンプトが表示されます。シャーシキーが入力されていない場合、デフォルトのシャーシ ID は生成されません。

クイック セットアップ ウィザードを実行するには、Exec モードの **setup** コマンドを実行します。

```
[local]host_name# setup
1. Do you wish to continue with the Quick Setup Wizard[yes/no]: y
2. Enable basic configuration[yes/no]: y
3. Change chassis key value[yes/no]: y
4. New chassis key value: key_string
```

MIO/UMIO ポートの冗長性の設定

MIO カードのポート冗長性は、システムの外部で発生するネットワーク障害の影響を最小限に抑えるため、冗長性レベルを高めます。たとえば、スイッチまたはルータのポート障害、ケーブルの切断、またはリンクダウンエラーの原因となるその他の外部障害などがあります。

⚠

注意 システムカードとポートレベルの冗長性メカニズムが適切に機能するようにするには、任意のシステムポートに直接接続されているデバイスのスパニングツリープロトコルを無効にします。スパニングツリープロトコルをオフにしないと、冗長性メカニズムまたはサービスの停止に障害が発生する可能性があります。

デフォルトでは、障害発生時にポートレベルの冗長性が提供されます。または、**ポートスイッチを**コマンドに発行することもできます。このモードでは、アクティブおよびスタンバイの MIO/UMIO カードのポートに同じ MAC アドレスが設定されていますが、いずれかのポートだけがアクティブになっていても、いずれかのポートで競合が発生することはありません。これにより、ポートのフェールオーバー時に MAC アドレスを転送し、無償 ARP を送信する必要がなくなります。代わりに、イーサネットポートの場合、送信元 MAC アドレスを含む 3 つのイーサネット ブロードキャスト パケットが送信されるため、外部ネットワーク機器（スイッチ、ブリッジ、またはその他のデバイス）がトポロジ変更後に情報を再学習できます。ただし、カードの削除が検出されると、特定のポートで発生した MAC アドレスの変更により、システムはネットワークに ARP を送信します。

ポートの冗長性により、フェールオーバーが発生すると、特定のポートのみがアクティブになります。たとえば、次のようになります。ポート 5/1 に障害が発生した場合、ポート 6/1 はアクティブになりますが、スロット 5 のラインカード上の他のすべてのアクティブポートは同じ

アクティブ状態のままになります。ポートフェールオーバーの状況では、**show port table** コマンドを使用して、両方のカードでポートがアクティブであり、両方のカードがアクティブであることを確認します。

冗長ペアの 1 つであるポートを管理上無効にする場合は注意が必要です。冗長ペアは、アクティブポートとスタンバイポートの両方で構成されます（たとえば、5/1 と 6/1）5/1 がアクティブな場合、CLI を使用して5/1 を管理上無効にしても 6/1 はアクティブになりません。1 つのポートでのアクションが両方に対して同じ影響を与えるため、5/1 と 6/1 の両方を無効にします。『*System Interface and Port Configuration Procedures*』の「*Creating and Configuring Ethernet Interfaces and Ports*」を参照してください。

自動カードレベルの冗長性では、MIO/UMIO フェールオーバーにポートレベルの冗長性はありません。スタンバイ MIO/UMIO がアクティブになり、そのカード上のすべてのポートがアクティブになります。システムは、障害が発生した MIO/UMIO によって使用されるすべての MAC アドレスと設定パラメータを、冗長な同等のものに自動的にコピーします。MIO のポートは元の MAC アドレスを保持し、システムは障害が発生した MIO/UMIO の設定パラメータを冗長な同等のものに自動的にコピーします。

ポートの冗長性は、リバーティブまたは非リバーティブに設定できます。リバーティブ冗長性サービスは、サービスが復元されたときに元のポートに戻されます。

この機能を使用するには、特定のネットワークトポロジを適切に動作させる必要があります。ネットワークには、システムが接続されている冗長スイッチングコンポーネントまたはその他のデバイスが必要です。次の図は、冗長スイッチングトポロジの例と、システムがさまざまな外部ネットワークデバイスのシナリオにどのように対応しているかを示しています。

図 *2 : MIO/UMIO* ポート冗長性を使用したネットワークトポロジの例

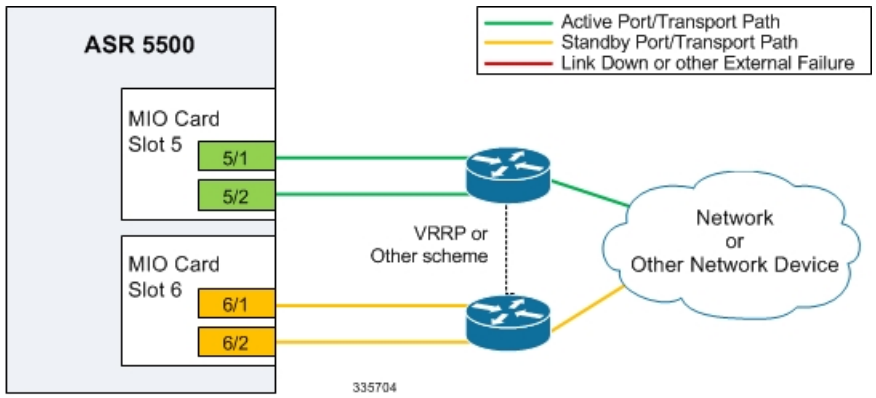
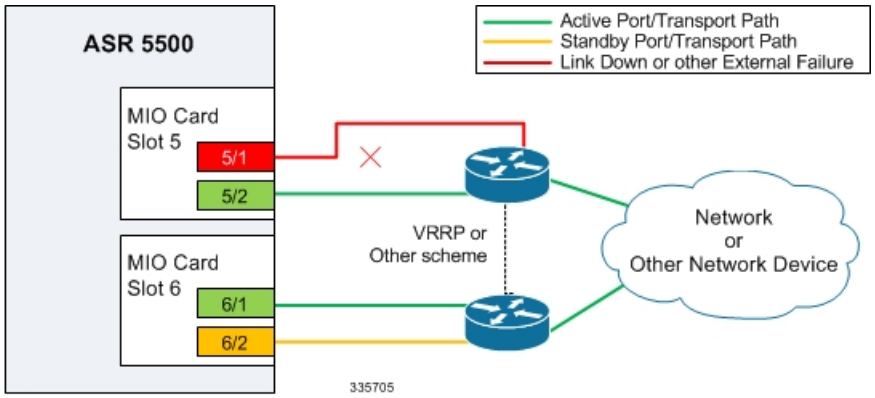
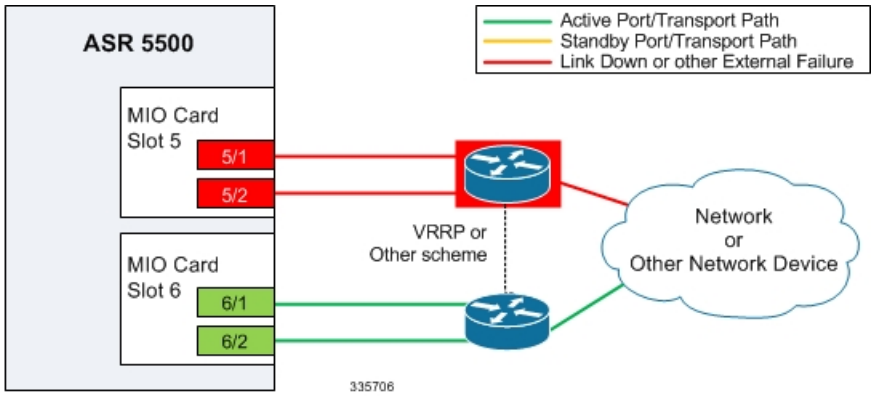


図 *3:* ケーブル故障時のポート冗長フェールオーバーのシナリオ



上の例では、イーサネットケーブルが切断されているか、または取り外されているため、リンクがダウンしています。このイベントが発生すると、ポートモードの冗長性が有効になっているシステムでは、リンクダウン状態が認識され、ポート 6/1 がアクティブポートになります。一部のポート冗長方式を使用するスイッチングデバイスは、障害を認識し、スロット 6 の MIO/UMIO が接続されているセカンダリスイッチ上のポートを有効にして、データのリダイレクトと転送を可能にします。

図 *4:* 外部ネットワークデバイス障害の場合のポート冗長性フェールオーバーのシナリオ



上記の例では、スイッチに障害が発生すると、そのスイッチに接続されているすべてのポートでリンクがダウン状態になります。この障害により、スロット 6 のラインカード上のすべての冗長ポートがアクティブ状態に移行し、冗長スイッチを使用します。

MIO/UMIO ポートの冗長性の自動リカバリを設定

ポートの自動リカバリ機能を設定できます。ポート障害が発生し、優先ポートがサービスに戻された場合（リンクが稼働している場合）、制御が自動的にそのポートに戻されます。デフォルトでは、ポートは非リバーティブ状態になっています。これは、ポートが優先されないことを意味します。元のポートへの使用を戻すには、手動のポートスイッチが必要です。

重要 この機能は、（**preferred slot** キーワードを介して）ポート単位で適用されます。これにより、個々の MIO カードで使用する特定のポートを設定することができます。たとえば、スロット 5 の MIO/UMIO の優先ポートとしてポート 10 ～ 19 を設定し、スロット 6 の MIO/UMIO の優先ポートとしてポート 20 ～ 29 を設定できます。

次の例を使用して、復元する優先ポートを設定し、問題が解消された場合のサービスへの自動復帰を設定します。

```
configure
   port ethernet slot#/port#
     preferred slot slot#
     end
```

注意

- 優先順位を指定する場合、指定されたカードに冗長性が復元されます。優先順位を指定しない場合、冗長性は復元されません。
- 優先させる追加のポートごとに、手順を繰り返します。

「設定の確認と保存」の章の説明に従って、設定を保存します。

ポートの冗長性の自動リカバリに関する検証

次のコマンドを入力して、ポート情報を確認します。

show port info *slot#/port#*

slot# は、物理ポートが存在する MIO/UMIO カードのシャーシスロット番号です。

port # は、MIO/UMIO の物理ポートです。

次に、スロット 5 の MIO/UMIO のポート 1 に対するこのコマンドの出力例を示します。

```
[local]host_name# show port info 5/1
Port: 5/1
  Port Type                : 1000 Ethernet
  Role                     : Management Port
  Description              : (None Set)
  Redundancy Mode          : Port Mode
  Redundant With           : 6/1
  Preferred Port           : Non-Revertive
  Physical ifIndex         : 83951616
  Administrative State     : Enabled
  Configured Duplex        : Auto
  Configured Speed         : Auto
  Configured Flow Control  : Enabled
  Interface MAC Address    :  02-05-47-B8-2F-41
  Fixed MAC Address        :  02-05-47-B8-2F-41
  Link State               : Up
  Link Duplex              : Full
  Link Speed               : 1000 Mb
  Flow Control             : Disabled
  Link Aggregation Group   : None
  Logical ifIndex          : 83951617
  Operational State        : Up, Active
```

データ処理カードの可用性の設定

「システムの動作と設定の概要」の「システムの起動プロセスの概要」の項で説明したように、システムを初めて起動すると、インストールされているすべての DPC/UDPC または DPC2/UDPC2 がスタンバイモードになります。これらのカードの一部をアクティブ化して、セッション処理に使用するように設定して使用する必要があります。DPC/UDPC または DPC2/UDPC2 のうちの 1 枚は、冗長性を確保するためにスタンバイモードのままになる場合があります。

この項では、DPC/UDPC または DPC2/UDPC2 をアクティブ化して、それらの冗長性を指定する方法について説明します。

重要 システムハードウェアの設定と冗長性については、『*ASR 5500 Installation Guide*』を参照してください。

次のコマンドを入力して、すべての DPC タイプの動作ステータスを確認します。

```
show card table
```

このコマンドは、スロット番号、動作ステータス、およびカードがシングルポイント障害（SPOF）であるかどうかによって、システムに取り付けられている DPC のタイプを一覧表示します。

次の例を使用して、DPC/UDPC または DPC2/UDPC2 の可用性を設定します。

```
configure
  card slot#
    mode { active | standby }
    end
```

注：

- カードをアクティブ化する場合は冗長性を確保するために、少なくとも 1 枚の DPC/UDPC または DPC2/UDPC2 をスタンバイモードにしておくことを忘れないでください。
- アクティブ化するシャーシ内の他のすべての DPC/UDPC または DPC2/UDPC2 に対して、この手順を繰り返します。

「設定の確認と保存」の章の説明に従って、設定を保存します。

カード設定の確認

設定が正しかったことを確認します。次のコマンドを入力します。

```
show card table
```

アクティブにしたすべての DPC/UDPC または DPC2/UDPC2 の動作ステータスが [Active] になっている必要があります。

FSC ファブリックの自動リセットの有効化

デフォルトでは、スイッチファブリック内で過剰な数の破棄されたファブリック出力パケットが発生した場合、ファブリック ストレージ カードを手動でリセットしてファブリックをリカバリする必要があります。

過剰な数の破棄されたファブリック出力パケットが検出された場合に、必要に応じて FSC の自動リセットを有効にすることができます。

グローバル構成モードの **fabric fsc-auto-recover** コマンドは、過剰な数の破棄されたファブリック出力パケットを検出したときに、自動 FSC リセットを有効または無効にします。

次のコマンドシーケンスは、この機能を有効にします。

```
configure
   fabric fsc-auto-recovery { disable | enable } [ max-attempts [
number_attempts | unlimited ] ]
   end
```

max-attempts [*number_attempts* **| unlimited]** は、StarOS が各 FSC のリセットを試行する回数を 1 ～ 99 の整数または無制限で指定します（FSC がリセットされるまで停止しません）。デフォルトの設定は 1 秒です。

重要 この機能を有効にするには、最初にグローバル構成モードの **fabric egress drop-threshold** コマンドを介して、ファブリック出力ドロップしきい値を設定する必要があります。

ASR 5500 のリンク集約の設定

Link Aggregation Group（LAG）は、IEEE 802.3ad で定義されているリンクの集約について、ピアが設定された物理ポートを介してLink Aggregation Control Protocol（LACP）経由で制御パケットを交換することによって動作します。LAG は、物理ポート上で制御パケットを直接送受信します。

LAG は最大 32 個のメンバーポートを持つことができます。これは MIO/UMIO/MIO2 カードが 2 枚あることを前提として、MIO/UMIO/MIO2 カードから 16 個のポートを持つことになります。

リンク集約（トランキングまたは□ボンディングとも呼ばれる）は、デバイス間のパラレルネットワークリンクを単一のリンクとして組み合わせることにより、より高い総帯域幅、自動ネゴシエーション、および回復を提供します。大きなファイルは、いずれかのリンクを介して送信されることが保証されます。これにより、不正なパケットに対処する必要がなくなります。

LAG およびマスターポート

論理ポートの設定（VLANおよびバインド）は、LAGのマスターポートで定義されます。カードの削除や障害が原因でマスターポートが削除された場合、使用可能な冗長マスターポートがない限り、別のメンバーポートがマスターポートになります（結果として、VPNバインドの変更および停止が発生します）。

重要 VPN バインドに対して VLAN を作成できるマスターポートは、常にアクティブ/マスター MIO/UMIOで設定する必要があります。スロット 5 の MIO/UMIO とスロット 6 の MIO/UMIO の間の冗長性により、両方のポートが自動的にマスターになり、同じ VLAN が設定されてアクティブになります。

LAG およびポートの冗長性

ASR 5500 LAG の実装は、次を前提としています。

- MIO/UMIO のスロット 5 と MIO/UMIO のスロット 6 の LAG ポートは 2 つのイーサネットスイッチに接続されている。
- MIO/UMIO のスロット 5 と MIO/UMIO のスロット 6 の LAG ポートは同時に両方ともアクティブになる。
- MIO/UMIO のスロット 5 と MIO/UMIO のスロット 6 のポートは、互いに冗長となっている。

LAG 内のすべてのポートは、特定のアクティブポート数または帯域幅のしきい値を超えたときに、別の MIO/UMIO に自動切り替えできます。

LAG および複数のスイッチ

この機能は、MIO 上のサブスクライバ トラフィック ポートをイーサネットスイッチ上のポートに接続します。ポート障害/スイッチは、指定されたしきい値を超えたときに、LAG 内のすべてのポートを他のMIO/UMIOに切り替えるよう強制します。これは、ポートの冗長性を得るために自動スイッチ機能と同様に動作します。LACP は ASR 5500 とイーサネットスイッチの間で動作し、正常性ステータスなどの情報に関連する部分を交換します。

次の表に、MIO/UMIO カードの一般的な LAG 機能の概要を示します。

表 *2 : MIO/UMIO LAG* 機能

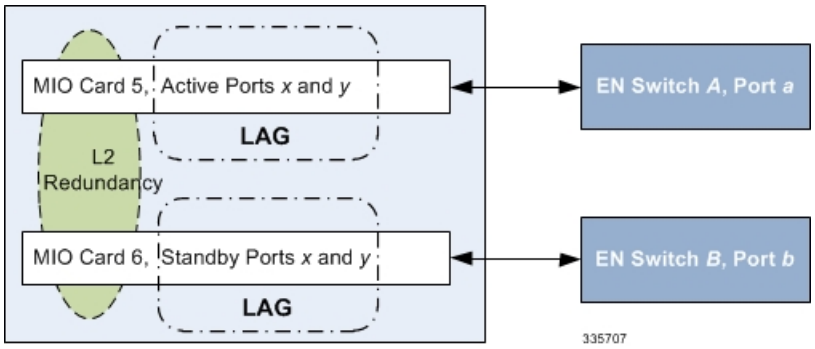
ASR 5500	LAGID	イーサネットスイッチ A	イーサネットスイッチ
MIO/UMIO ポート 11	1	Port 1	----
MIO/UMIO ポート 12	1	Port 2	----
MIO/UMIO ポート 13	1	----	Port 1

L2 冗長性を備えた複数のスイッチ

LACP パケットを渡すためにスタンバイポートを必要とせずに、LACP の実装を処理するために、冗長カード上で 2 つの異なる LACP インスタンスを開始します。2 つの LACP インスタンスとポートリンクステートがモニターされ、自動スイッチを開始するかどうか（自動 L2 ポートスイッチを含む）が決定されます。

次の図は、L2 冗長性を備えた 2 つの MIO/UMIO ドーターカードポート間で確立された LAG を示しています。

図 *5 : L2* 冗長性を備えた *LAG*、*2* つのイーサネットスイッチ



スタンバイポートがリンクアップしている場合でも、L2 冗長性を備えた LACP の実装でトラフィックを渡すことはできません。たとえば、2 つの異なるイーサネットスイッチが 2 つの MIO/UMIO カードに接続され、すべてのポートが同じ LAG にある場合、ポートの障害は、アクティブなポート番号の比率が反転（アップよりダウンのポートが多い）するまでLAGスイッチがトリガーされることはありません。

自動スイッチのためのポートの状態

ポートは4つの状態のいずれかに分類され、自動スイッチを開始するかどうかを決定します。次の表を参照してください。

カウンタでは、State(x) は、その状態のカードのポート数を表します。

表 *3 :* 自動スイッチポートの状態

状態（State）	カウンタ	説明
リンク	L(x)	物理リンクアップ
Standby	S(x)	リンクアップしてもスタンバイモード
Waiting	W(x)	リンク集約制御プロトコルのネゴシエーションの待機
集約データ	A(x)	形成された集約

Hold Time

LAG マネージャは別の LACP インスタンスに切り替えると、しばらくの間はリンクと LACP ネゴシエーションを安定させるために別の変更を検討しません。この「ホールド時間」は設定可能です。

また、LAG マネージャは、管理者が手動でポートを切り替えてカードスイッチをトリガーした場合のホールド時間を開始または延長します。

優先スロット

優先スロットとして、LAG グループごとに優先されるカードを定義できます。優先 MIO/UMIO スロットが指定されている場合は、初期タイムアウト期間として選択され、スイッチ選択のランダム性は低下します。

このモードでは、ポート設定は許可されていません。

自動スイッチの基準

次の基準によってカード x からカード y への切り替えを決定し、手動による介入を許可するとともに、より適切な帯域幅を提供します。条件の評価は、保留期間外で行われます。

A（y）= 1、少なくとも 1 つのポートがカード y の集約状態にあり、次のいずれかの条件が満たされると、ポートはカード x からカード y に自動的に切り替えられます（優先順）。

- L（x）L（y）の場合、カード *x* の方が、カード *y* よりリンクアップのポートが少ない
- S（x）S（y）の場合、カード *x* のスタンバイ状態のポート数の方が、カード *y* より多い
- W（x）W（y）の場合、カード *x* の待機状態のポート数の方が、カード *y* より多い
- A（x）A（y）の場合、カード *x* の集約状態にあるポート数の方が、カード *y* より少ない
- カード *y* が優先されます
- カード *y* が選択されています

リンク集約制御

集約グループ内の 1 つのポートがマスターとして設定されるため、集約グループ内のすべてのトラフィック（制御トラフィックを除く）が論理的にこのポートを通過します。LAG を有効にするときは、まずマスターポートでリンク集約を設定し、LAG を無効にするときにマスターポートの設定を解除することを推奨します。

次のコマンドは、マスターとしてポート *slot#/port#* を使用して、リンクアグリゲーショングループ *N* を作成します。1 つのグループに対して許可されるマスターポートは 1 つだけです。*N* は [1 ～ 255] の範囲内である必要があります。

```
configure
   port ethernet slot#/port#
```

```
link-aggregation master group N
exit
```

重要 Link Aggregation Control Protocol（LACP）は、マスターポートが有効になっている場合にのみ実行を開始します。

マスターポートが割り当てられている場合にのみ、リンクアグリゲーショングループ番号*N*のメンバとしてポートを追加するには、次のコマンドを使用します。それ以外の場合は、マスターポートが割り当てられたときにグループに追加されます。

```
port ethernet slot#/port#
   link-aggregation member group N
   exit
```

重要 VPN はマスターポートのみをバインドでき、VLAN はマスターポートでのみ作成できます。リンク集約メンバポートにバインドしようとすると、エラーメッセージが生成されます。

リンクアグリゲーションに参加する各システムには、2 バイトのプライオリティ（最小番号[0]が最も高いプライオリティを持つ）と、最初のポートの MAC アドレスから取得した 6 バイトの MAC アドレスで構成される一意のシステム ID があります。次のコマンドは、システム ID を形成するために使用されるシステムプライオリティを設定します。*P* は、[0x0000..0xFFFF]の 16 進数です。デフォルトは 0x8000 です。

```
card slot#
   link-aggregation system-priority P
```

システム内のポートにはキーが割り当てられています。グループ番号は、キーに直接マッピングされ、同じキーを持つポートだけを集約できます。リンクの両側のポートは、異なるアグリゲーションキーを使用します。

2 つのピアのシステム ID、ポートキー、およびポート ID は、リンクアグリゲーショングループ識別子（LAGID）を形成します。同じ LAGID を持つリンクを集約できます。システムは、最初に各ポートを独自の集約（ポートごとに個別のキーを必要とする）、または同じ集約内のすべてのポート（すべてのポートに対して 1 つのキー）で設定することがよくあります。LACP によるネゴシエーションでは、実際の集約が適用されます。

システムは、システム ID、ポートキー、およびポート ID に関する情報を、LACP を使用して物理リンクを介してピアと交換します。

LACP パケットは、低速プロトコル形式で定義されます。各システムは、自身の（「アクター」）情報と、そのピア（「パートナー」）に関する最後に受信した情報を、物理リンクを介して送信します。

LACP パラメータを設定するには、次のコマンドを使用します。LACP は、アクティブモードで動作して LACP パケットを定期的に送信するか、またはパッシブモードで、受信した LACP パケットにのみ応答することができます。

LACP は、auto（30s）または fast（1s）レートのいずれかでパケットを送信できます。このリリースのデフォルトは、[**Active**] と [**Auto**) です。次の設定例を参照してください。

```
config
   port ethernet slot#/port#
      link-aggregation lacp { active | passive } [ rate { auto | fast
} | timeout { long | short } ]
```

ピアは、状態が変化したとき、または受信したLACPパケットから自身の状態に関する差異が検出された場合に、LACP パケットを送信します。

MIO/UMIO 冗長ペアの対応するポートは、同時にアクティブにすることはできません。冗長ポートは同じ MAC アドレスを共有するため、フェールオーバーが解決されると、元のポートはリンクアグリゲーショングループに再参加します。

最小リンク

最小リンクオプションでは、集約に使用可能な最小数のリンクがある場合にのみ、リンク集約グループ（LAG）が作動状態（使用可能）になることを指定します。これにより、最小量の帯域幅が使用可能であることが保証されます。

この機能を有効にした場合、LAG 内のリンクの数が設定された最小リンク値を下回ると LAG は使用できなくなります。現在アクティブなバンドル内のリンク数が設定された最小リンク値を下回ると、別の LAG バンドルへのスイッチオーバー（使用可能な場合）が自動的に発生します。

この機能を有効にするには、グローバル構成モードの **link-aggregation** コマンド内に **min-link** キーワードオプションを使用します。

```
configure
   port ethernet slot/port
      link-aggreagation master ( global | group } number
         min-link number_links
         end
```

冗長性のオプション

L2 冗長性では、グループ全体で使用するために、マスターポートで次のオプションを設定します。

```
link-aggregation redundancy standard [hold-time sec ] [preferred slot {
 card_number | none }
```

標準の冗長性では、グループ内のすべてのカードが 1 つのグループとして扱われます。

2 つのイーサネットスイッチによる水平リンク集約

LAG に異なるスイッチにそれぞれ接続するポートセットが 2 つ含まれている場合、オペレータはポートを切り替えるときに、（接続先スイッチに接続されている）スロット/ポートを指定できます。

Exec モードの **link aggregation port switch to** *slot/port* コマンドは、このオプションを設定します。*slot/port* は、接続先スイッチに接続されている有効なポートです。このオプションの設定には、次の基準が適用されます。

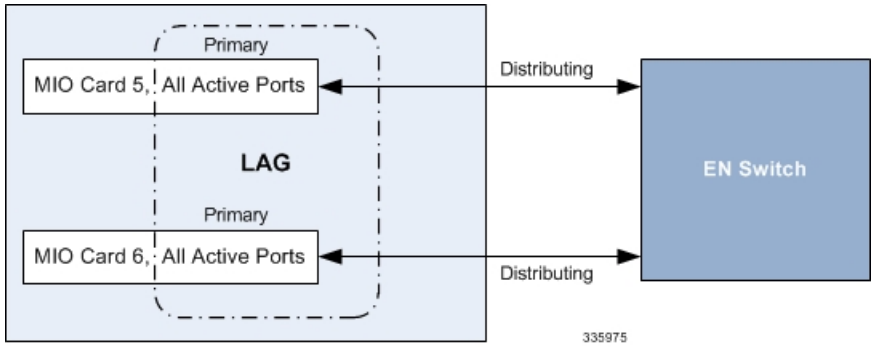
- *slot/port* は LAG をサポートしている必要があります。
- *slot/port* は LAG を使用して設定する必要があります。
- *slot/port* はすでにアクティブに配信していてはなりません。
- *slot/port* は、標準モードでリンク集約パートナーをネゴシエートしている必要があります。
- *slot/port* のパートナーは、標準モードで同等以上である必要があります。
- *slot/port* のパートナーバンドルには、標準モードで同等以上の帯域幅がある必要があります。
- 標準モードでは、*slot/port* への切り替えがホールド時間内の優先順位に違反しないようにする必要があります。

非冗長（アクティブ-アクティブ）LAG

LAG は、両方の MIO/UMIO カードのポートが同じスイッチに接続されている非冗長モードで展開できます。

次の図に示すように、両方のカードで使用されている LAG 内のすべてのポートは、非冗長モード（アクティブ/アクティブ）で機能します。

図 *6* : 単一の *LAG* グループを使用した非冗長 *LAG* 設定



上記の設定では、単一のプライマリ LAG があります。すべてのポートは、トラフィックを分散するポートの単一のバンドルとして機能します。

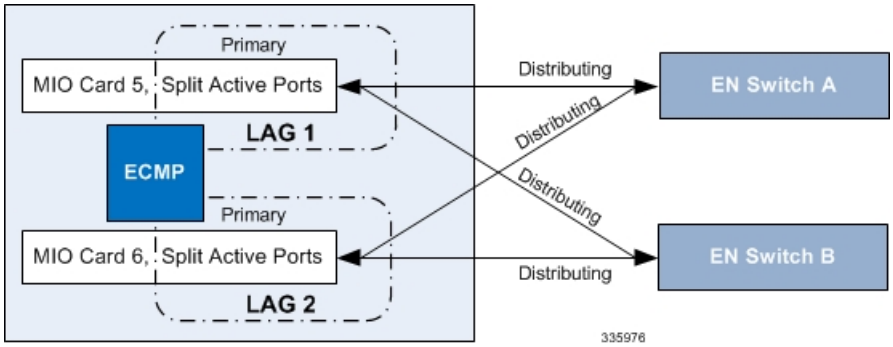
重要 イーサネットポート構成モードの **shutdown** コマンドを使用して、この LAG 設定で MIO/UMIO カードのいずれかのポートをシャットダウンする場合、デフォルトでは、他の MIO/UMIO カードのペアリングされたポートもシャットダウンされます。Exec モードの **port { disable | enable } ethernet** *slot/port* コマンドを使用して、この LAG 設定で MIO/UMIO のポートを選択的に無効にすることができます。

重要 この動作モードでは、自動の ASR 5500 ポートの冗長性が失われます。

冗長性を実現するには、2 つ目の非冗長 LAG を設定する必要があります。ECMP（等コストマルチパス）のルーティングなど上位層のロード バランシング メカニズムを使用して、2 つの LAG グループにトラフィックを均等に分散させることができます。

1 つの MIO/UMIO に障害が発生した場合、両方の LAG グループからの半分のポートが、他の MIO/UMIO からのトラフィックの流通に使用できるようになります。

図 *7: ECMP* を使用した非冗長 *LAG* 設定



2 番目の LAG グループの設定は必須ではありませんが、このモードの LAG で冗長性を実現するための通常のアプローチです。

ただし、集約ポートがキャパシティの 50% を超えてロードされ、MIO/UMIO の障害とスイッチオーバーが発生した場合、ASR 5500 で設定されたポート容量がオーバーサブスクライブされ、不確定な数量のセッションがドロップされ、トラフィックが失われます。

データ プレーンのコンバージェンスの短縮

グローバル構成モードの **fast-data-plane-convergence** コマンドを使用すると、アグレッシブ MicroBFD タイマーを使用したアクティブ/アクティブ LAG 設定での既存のセッションを迅速にリカバリできます。この機能は、アクティブ/スタンバイ LAG 設定で有効にすることができますが、スイッチオーバー時間の短縮は保証できません。

この機能により、外部スイッチでの障害の誤検出と、別の ASR 5500 での誤検出 ICSR フェールオーバーがなくなります。

```
configure
  fast-data-plane-convergence
```

重要 アクティブ/アクティブ LAG グループは、アグレッシブ microBFD タイマー（150 * 3 など）とともに設定する必要があります。MIO カードのリカバリ時に、BGP セッションが設定に基づいてフラップする場合があります。これらのイベント時のトラフィック損失を回避するには、適切なホールド/キープアライブタイマーと再起動タイマーを使用して BGP グレースフルリスタートを設定する必要があります。『*Command Line Interface Reference*』の「*BGP Configuration Mode Commands*」の章に記載されている **bgp graceful-restart** コマンドの説明を参照してください。

リンク集約のステーテス

リンク集約のステータスを確認するには、次のコマンドを使用します。

- **show port table**
- **show port info** *slot/port*

show port table コマンドの出力で LAG の物理ポートのステータスを表示するには、1 文字を使用します。次の表を参照してください。

表 *4 : LAG* ポートのステータス

ディスプレイ	説明
LA+	ポートは配信（送受信データ）に積極的に使用されます。
LA-	ポートは LACP のネゴシエーションに失敗しました。
LA ～（チルダ）	ポートは LACP をネゴシエートしましたが、別のピアが選択されました。
LA*	ポートは LACP を（再）ネゴシエートしています。
LA#	最小リンク条件が満たされていないため、ポートはダウンしています。

逆多重化カードの設定

逆多重化カードとして機能するように、DPC/UDPC または DPC2/UDPC2、または MIO/UMIO を専用にします。逆多重化は、1つの逆多重化タスクの総称です。これらは、コールセットアップ（シグナリングパケット）を解析し、コールを内部的に配信するためのタスクです。そのため、存在するサービスとほぼ同数のタスクが逆多重化カードで実行しています。

各コンテキストの vpnmgr も逆多重化カード上で実行されます。vpnmgr タスクの数はコンテキストの数に対応しています。vpnmgr は、モバイル機器、IP ルーティング（BGP、OSPF など）および関連付けられているさまざまなタスクに IP アドレスを割り当てます。

概要

DPC/UDPC または DPC2/UDPC2、または MIO/UMIO をデマルチプレクサカードとして指定すると、セッション処理のためのリソースが解放され、システムのスループットが向上する可能性があります。ただし、他のシステムリソースの制限により、サブスクライバの総キャパシティのサポートが増加することはありません。

この機能はデフォルトでは無効になっていますが、グローバル構成モードの **require demux** を使用して有効にすることができます。これは、限られた数の製品でのみサポートされています。詳細については製品のアドミニストレーションガイドを参照してください。

また、この機能をサポートするには、グローバル構成モードの **require session recovery** コマンドを使用してセッションリカバリを有効にする必要もあります。

重要 デマルチプレクサカードとセッションリカバリを有効にした後にこの機能を有効にするには、設定を保存し、ASR 5500 を再起動する必要があります。

注意 MIO/UMIO機能でデマルチプレクサを有効にすると、システム内のリソース割り当てが変更されます。これは、ICSR 設定内の StarOS バージョン間のアップグレードまたはダウングレードに直接影響を与えます。ICSR 展開をアップグレードまたはダウングレードする前に、Cisco TAC に連絡して手順についてのサポートを受けてください。

MIO Demux の制約事項

MIO/UMIO を demux カードとして有効にする場合は、次の制約事項が適用されます。

- サービスまたはコンテキストがシステム上で作成される前に、**require demux management-card** コマンドを設定する必要があります。このコマンドは、シャーシに対して動作モードが選択された後は実行されません。
- 現在、demux 機能の MIO/UMIO カードの指定をサポートしているのは、次のサービスのみです。ePDG（StarOS リリース 21.2 以降）、GGSN、 HeNBGW（StarOS リリース 21.2 以降、SaMOG（StarOS リリース 21.2 以降）、SGW、PGW、HA、SAE-GW、および L2TP LNS. これらのサービスは、コンシューマゲートウェイとして展開されている場合にのみサポートされます。
- SGSN、MME、HNBGW、HeNBGW（StarOS リリース 21.1 以前）、SaMOG（StarOS リリース 21.1 以前）、 PDG、PDIF、ePDG（StarOS リリース 21.1 以前）、IPSG、PDSN、HSGW、L2TP LAC、NEMO、FA、および WSG はサポートされていません。企業ゲートウェイまたは社内ゲートウェイ（GGSN、HA、PGW など）もサポートされていません。
- 多数のトンネルを必要とする設定については、MIO/UMIO で demux 機能を有効にしないでください。

- MIO/UMIO で実行されている demux 機能を使用して ASR 5500 を起動した後、サポートされていないサービスを設定することはできません。最大 8 つの Demux マネージャがサポートされます。8 つを超える Demux マネージャを追加しようとすると、すべてブロックされます。
- 多数の VPN マネージャ、VRF、および/または Demux マネージャを必要とするサービスや製品では、MIO/UMIO で Demux 機能を有効にしないでください。
- MIO/UMIO で実行されている demux 機能では、ASR 5500 は最大 10 のコンテキスト、コンテキストごとに 64 のインターフェイス、およびシステムごとに 250 の VRF をサポートします。
- ICSR のアップグレードには、互換性のある設定と Method of Procedure（MOP）が必要です。

この機能を実装するには、CEPS（1 秒あたりのコールイベント）とサブスクライバの数が一定のままで、データレートだけが増加することを前提としています。これにより、CPU 要求が MIO/UMIO で増加しないことが保証されます。

（注） demux カードのバックグラウンドでプロセスのクラッシュが発生した場合、カードの計画済み移行または未計画の移行が失敗します。

重要 MIO/UMIO 機能の Demux を有効にする場合のシステム設定への影響を評価する際に追加のサポートが必要な場合は、Cisco TAC にお問い合わせください。

構成

DPC/UDPC を demux カードとして設定するには、次の CLI コマンドを入力します。

```
config
  require demux processing-card
  end
```

DPC/2UDPC2 を demux カードとして設定するには、次の CLI コマンドを入力します。

```
config
  require demux processing-card
  end
```

MIO/UMIO を demux カードとして設定するには、次の CLI コマンドを入力します。

```
config
  require demux management-card
  end
```

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。