ターミナル サービス（TS）エージェントの概要

- シスコ ターミナル サービス（TS）エージェントについて （1 ページ）
- サーバおよびシステム環境要件 （2 ページ）
- Firepower Management Center での TS エージェントに関する問題のトラブルシューティング （4 ページ）
- TS エージェントに関する問題のトラブルシューティング （7 ページ）
- ユーザエージェントに関する問題のトラブルシューティング （9 ページ）
- 解決済みの問題 （9 ページ）
- TS エージェントの履歴 （10 ページ）

シスコターミナルサービス（TS）エージェントについて

シスコ ターミナル サービス（TS）エージェントを使用すると、Firepower Management Center または ISE/ISE-PIC では、Microsoft Windows ターミナル サーバによってモニタされるユーザトラフィックを一意に識別できるようになります。TSエージェントがない場合、システムは、Microsoft Windows ターミナルサーバからのすべてのトラフィックを、1 つの IP アドレスから発信された単一のユーザセッションとして認識します。

（注） 潜在的な問題を回避するとともに、ご使用のソフトウェアが最新であることを確保するため、シスコは、TS エージェントの最も新しくリリースされたバージョンを使用することを推奨します。最新バージョンを確認するには、https://www.cisco.com/c/en/us/support/index.htmlシスコサポートのサイトを参照してください。

TS エージェントは、Microsoft Windows ターミナルサーバにインストールおよび設定されると、一定のポート範囲を個別のユーザセッションに割り当て、その範囲内のポートをユーザセッションにおける TCP および UDP 接続に割り当てます。システムは、ネットワーク上のユーザによる個別の TCP および UDP 接続を識別するために一意のポートを使用します。ポート範囲

は、Least Recently Used ベースで割り当てられます。つまり、ユーザセッションの終了後、同じポート範囲が新しいユーザセッションにすぐに再利用されることはありません。

（注） ICMP メッセージは、ポートマッピングなしで渡されます。

コンピュータのシステム コンテキスト内で実行されるサービスによって生成されるトラフィックは、TS エージェントによって追跡されません。特に、サーバ メッセージ ブロック（SMB）トラフィックはシステム コンテキスト内で実行されるため、TS エージェントは、SMB トラフィックを識別しません。

TS エージェントは、TS エージェントホストごとに最大 199 の同時ユーザセッションをサポートします。単一のユーザが複数の同時ユーザ セッションを実行している場合、TS エージェントは、個別のユーザセッションのそれぞれに一意のポート範囲を割り当てます。あるユーザがセッションを終了すると、TS エージェントは、そのポート範囲を別のユーザ セッションに使用できます。

各 FMC は、同時に接続する最大 50 の TS エージェントをサポートします。

お使いのサーバにインストールされる TS エージェントには、3 つの主要コンポーネントがあります。

- インターフェイス：TS エージェントを設定し、現在のユーザ セッションをモニタするアプリケーション
- サービス：ユーザのログインおよびログオフをモニタするプログラム
- ドライバ：ポート変換を行うプログラム

TS エージェントは次のいずれかに使用できます。

- Firepower Management Center 上の TS エージェント データは、ユーザ認識やユーザ コントロールに使用できます。Firepower システムでの TS エージェント データの使用に関する詳細については、『Firepower Management Center Configuration Guide』を参照してください。

（注） TS エージェントをユーザ認識やユーザコントロールに使用するには、データの送信先を Firepower Management Center のみに設定する必要があります。詳細については、TS エージェントの設定 を参照してください。

サーバおよびシステム環境要件

お使いのシステム上で TS エージェントをインストールして実行するには、次の要件を満たす必要があります。

（注） 潜在的な問題を回避するとともに、ご使用のソフトウェアが最新であることを確保するため、シスコは、TS エージェントの最も新しくリリースされたバージョンを使用することを推奨します。最新バージョンを確認するには、https://www.cisco.com/c/en/us/support/index.htmlシスコ サポートのサイトを参照してください。

サーバ要件

64 ビット Microsoft Windows ターミナル サーバの次のバージョンのいずれかに TS エージェントをインストールします。

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

（注） TS エージェントのインストールには、サーバ上に 653 KB の空き領域が必要です。

（注） TS エージェントサーバで Web トラフィックをプロキシするアンチウイルスソフトウェアを使用している場合、通常、ユーザトラフィックはシステムユーザに割り当てられ、FMC はそれらのユーザを不明なユーザとして認識します。この問題を回避するには、Web トラフィックのプロキシを無効にします。

TS エージェントは、サーバにインストールされるターミナル サービス ソリューションのうち、以下のものと同時に使用することができます。

- Citrix Provisioning
- Citrix XenDesktop
- Citrix XenApp
- Xen Project Hypervisor
- VMware vSphere Hypervisor/VMware ESXi 6.0
- Windows ターミナル サービス または Windows リモート デスクトップ サービス（RDS）

このバージョンの TS エージェントでは、ポート変換およびサーバ システム間の通信に、単一のネットワーク インターフェイス コント ローラ（NIC）を使用することができます。サーバに有効な NIC が 2 つ以上存在する場合、TS エージェントは、設定の際に指定されたアドレスに対してのみポートの変換を実行します。有効な NIC には必ず、IPv4 もしくは IPv6 のアドレ

スが 1 つだけ、または各タイプのアドレスが 1 つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。

（注） サーバに接続されているデバイスのいずれかでルータ アドバタイズメントが有効になっていると、それらのデバイスがサーバ上の NIC に複数の IPv6 アドレスを割り当て、TS エージェントで使用する NIC を無効にしてしまう可能性があります。

Firepower システムの要件

このバージョンの TS エージェントは、バージョン 6.4 以降の Firepower システムを実行するスタンドアロンまたは高可用性の Firepower Management Center との接続をサポートします。

Firepower Management Center での TS エージェントに関する問題のトラブルシューティング

Firepower Management Center での TS エージェントに関する問題の詳細については、次の項を参照してください。

このリリースで解決された既知の問題の詳細については、解決済みの問題 （9 ページ）を参照してください。

Firepower Management Center がシステム プロセスについてはユーザ情報を表示しない

システム コンテキスト内で実行されるサービスによって生成されるトラフィックは、TS エージェントによって追跡されません。特に、次の点に注意してください。

- サーバメッセージブロック（SMB）トラフィックはシステムコンテキスト内で実行されるため、TS エージェントは SMB トラフィックを識別しません。
- 一部のアンチウイルス アプリケーションは、Web トラフィックをオンプレミスまたはクラウドゲートウェイにプロキシして、クライアントコンピュータに到達する前にウイルスを捕捉します。ただし、これは、アンチウイルスソフトウェアが通常はシステムアカウントを使用することを意味します。この場合、FMC はユーザを不明なユーザと見なします。この問題を解決するには、Web トラフィックプロキシを無効にします。

TS エージェント ユーザのタイムアウトが期待されるときに発生しない

サーバと Firepower Management Center の時計を同期させる必要があります。

TS エージェントがユーザ セッション ポートの変換を実行しない

TS エージェントは、次の場合はポート変換を実行しません。

- ユーザ セッションが、設定されている [最大ユーザ セッション（Max User Sessions）] の値を超えている。たとえば、[最大ユーザ セッション（Max User Sessions）] が 29 に設定

されている場合、TS エージェントは、30 番目のユーザ セッションに対しては、ポート変換を実行しません。

- 使用可能なポートがすべて使用中。たとえば、[ユーザ ポート（User Ports）] の [範囲（Range）] の値がユーザ セッションごとに 1000 ポートに指定されている場合、TS エージェントは、1001 番目の TCP/UDP 接続に対しては、ユーザが別の TCP/UDP 接続を終了してポートを開放するまで、ポート変換を実行しません。
- ユーザセッションに関連付けられたドメインがない。たとえば、サーバ管理者のセッションが、ローカル システムには認証されたものの外部の Active Directory サーバには認証されなかった場合、サーバ管理者は、サーバにログインしますがネットワークおよびTSエージェントにはアクセスできず、TS エージェントは、そのユーザ セッションにポートを割り当てません。

TS エージェントがポート変換を期待されるように実行しない

サーバの IP アドレスを手動で編集する場合、TS エージェント上で [サーバ NIC（Server NIC）] を編集する必要があります。その後で、TS エージェント設定を保存し、サーバを再起動します。

ユーザ セッションが Firepower Management Center に期待されるように報告されない

別の Firepower Management Center に接続するように TS エージェント設定を更新する場合は、新しい設定を保存する前に、現在のすべてのユーザセッションを終了する必要があります。詳細については、現在のユーザ セッションの終了を参照してください。

クライアント アプリケーションのトラフィックがユーザ トラフィックとして Firepower Management Center に報告される

サーバにクライアント アプリケーションがインストールされており、そのアプリケーションが、[システム ポート（System Ports）] の範囲外のポートを使用するソケットにバインドするよう設定されている場合、[除外ポート（Exclude Port(s)）] フィールドを使用して、そのポートを変換から除外する必要があります。そのポートを除外しないと、そのポートが [ユーザ ポート（User Ports）] の範囲内である場合、TS エージェントは、そのポートでのトラフィックを、関係のないユーザ トラフィックとして報告する可能性があります。

これを防ぐには、クライアント アプリケーションを、[システム ポート（System Ports）] の範囲内のポートを使用するソケットにバインドするように設定します。

サーバ アプリケーションのタイムアウト、ブラウザのタイムアウト、または TS エージェントと Firepower Management Center の間の接続障害

TS エージェント サーバ上のアプリケーションが TCP/UDP 接続を終了したものの、それに関連するポートが完全に閉じられていない場合、TS エージェントは、そのポートを変換に使用できません。サーバがポートを完全に閉じる前に TS エージェントがそのポートを変換に使用しようとすると、接続は失敗します。

（注） 完全に閉じられていないポートを特定するには、`netstat` コマンド（サマリー情報用）または `netstat -a -o -n -b` コマンド（詳細情報用）を使用できます。これらのポートのステータスは、`TIME_WAIT` または `CLOSE_WAIT` です。

この問題が発生する場合は、問題によって影響を受ける TS エージェント ポートの範囲を大きくします。

- 正しく閉じられていないポートが [ユーザ ポート（User Ports）] の範囲内である場合、サーバ アプリケーションまたはブラウザのタイムアウトが発生します。
- 正しく閉じられていないポートが [システム ポート（System Ports）] の範囲内である場合、TS エージェントと Firepower Management Center の間で接続障害が発生します。

TS エージェントと Firepower Management Center の間の接続障害

設定中に [テスト（Test）] ボタンをクリックしたときに TS エージェントが Firepower Management Center との接続を確立できなかった場合は、次のことを確認してください。

- 50 を超える TS エージェントクライアントが同時に FMC への接続を試行していないことを確認します。
- 入力した [ユーザ名（Username）] と [パスワード（Password）] が、REST VDI ロールの作成で説明するように、REST VDI 特権を有する Firepower Management Center ユーザの正しいクレデンシャルであるか確認します。

  TS エージェントからのユーザ認証が成功したかを確認するには、Firepower Management Center で監査ログを表示します。
- ハイ アベイラビリティ設定で、設定の直後にセカンダリの Firepower Management Center への接続が失敗した場合、それは、想定されている動作です。TS エージェントは、アクティブな Firepower Management Center と常に通信します。

  セカンダリがアクティブな Firepower Management Center となっている場合、プライマリの Firepower Management Center への接続は失敗します。

システム プロセスまたはサーバ上のアプリケーションが誤動作している

お使いのサーバ上のシステム プロセスが [システム ポート（System Ports）] の範囲にないポートを使用またはリッスンしている場合、そのポートは、[除外ポート（Exclude Port(s)）] フィールドを使用して手動で除外する必要があります。

お使いのサーバ上のアプリケーションが Citrix MA クライアントのポート（2598）または Windows ターミナル サーバのポート（3389）を使用またはリッスンしている場合、それらのポートが [除外ポート（Exclude Port(s)）] フィールドで除外されていることを確認してください。

Firepower Management Center に TS エージェントからの不明なユーザが表示される

Firepower Management Center が TS エージェントからの不明なユーザを表示するのは、次の状況です。

- TS エージェントのドライバコンポーネントがクラッシュすると、ダウンタイム中に発生したユーザセッションは、Firepower Management Center のログに不明なユーザとして記録されます。
- 一部のアンチウイルス アプリケーションは、Web トラフィックをオンプレミスまたはクラウドゲートウェイにプロキシして、クライアントコンピュータに到達する前にウイルスを捕捉します。ただし、これは、アンチウイルスソフトウェアが通常はシステムアカウントを使用することを意味します。この場合、FMC はユーザを不明なユーザと見なします。この問題を解決するには、Web トラフィックプロキシを無効にします。
-
- ハイ アベイラビリティ設定でプライマリの Firepower Management Center がダウンすると、フェールオーバー中の 10 分のダウンタイムの間に TS エージェントによって報告されるログインは、次のように処理されます。
  - Firepower Management Center で以前に見られたことのないユーザについて TS エージェントがユーザセッションデータを報告した場合、そのデータは、Firepower Management Center には、不明なユーザ アクティビティとして記録されます。
  - Firepower Management Center で以前に見られたことがあるユーザの場合、データは正常に処理されます。

  ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

サーバの NIC リストに NIC が表示されない

サーバに接続されているデバイスで、ルータ アドバタイズメント メッセージを無効にする必要があります。ルータ アドバタイズメントが有効になっていると、デバイスがサーバ上の NIC に複数の IPv6 アドレスを割り当て、TS エージェントで使用する NIC を無効にしてしまう可能性があります。

有効な NIC には必ず、IPv4 もしくは IPv6 のアドレスが 1 つだけ、または各タイプのアドレスが 1 つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。

TSエージェントに関する問題のトラブルシューティング

Firepower Management Center のテスト接続が失敗する

（ドメインユーザではなく）ローカルユーザとして TS エージェントサーバにログインしている場合、TS エージェントと Firepower Management Center とのテスト接続が失敗します。これは、デフォルトでは、TS エージェントがシステムプロセスにネットワーク上での通信を許可しないために発生します。

この問題を回避するには、次の手順を実行します。

- TS エージェントの設定フィールドの説明に従って、[設定（Configure）] タブページの [不明なトラフィック通信（Unknown Traffic Communication）] をオンにしてトラフィックを許可します。
- ローカルユーザとしてではなく、ドメインユーザとして TS エージェントコンピュータにログインします。

TS エージェントがアップグレード時に再起動を要求する

マシンの IP アドレスが変更されない場合でも、アップグレード後に TS エージェントが IP アドレスの変更を報告し、サーバの再起動を要求することがあります。これは、TS エージェントが IP アドレスと次のレジストリキーの値の違いを検出するために発生します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TSAgent\{IPv4 | IPv6}
```

設定されたプライマリアダプタの IP アドレスとキー値が異なる場合、TS エージェントが変更を報告し、設定を保存してコンピュータを再起動するように指示されます。

これは、たとえば、コンピュータが再イメージ化またはバックアップから復元され、DHCP が新しい IP アドレスを割り当てた場合に発生することがあります。

エラーは無視できますが、いずれにしても、アップグレード後にコンピュータを再起動する必要があります。

Citrix Provisioning クライアントが起動に失敗する

Citrix Provisioning Server 用に設定した UDP ポートを無視するように TS エージェントを設定する必要があります。

TS エージェントの [予約ポート（Reserve Port(s)）] フィールドで指定する値は、Citrix Provisioning の [最初と最後の UDP ポート番号（First and Last UDP port numbers）] のポートのいずれかと一致する必要があります。

⚠

注意 正しいポートを指定しないと、クライアントの起動に失敗します。

TS エージェントの IP アドレスを保存する際の例外

まれに、無効な IP アドレスを使用して TS エージェント設定を保存しようとすると、例外が表示されます。無効な IP アドレスは、次のいずれかになります。

- ネットワーク上の別のデバイスと同じ IP アドレス。
- TS エージェント アプリケーションが開いているときに、Windows で変更した静的 IP アドレス。

例外は次のとおりです。

- `System.ArgumentException`：同じキーを持つ項目がすでに追加されています。（`An item with the same key has already been added.`）
- `System.NullReferenceException`：オブジェクト参照がオブジェクトのインスタンスに設定されていません。(`Object reference not set to an instance of an object.`)

回避策：TS エージェントサーバの IP アドレスを有効な IP アドレスに設定し、TS エージェントの設定を保存して、サーバを再起動します。

ユーザエージェントに関する問題のトラブルシューティング

TS エージェントとユーザエージェントの両方を使用する場合、ユーザエージェントから TS エージェントの IP アドレスを除外することによって、重大ではないエラーのログを回避できます。TS エージェントとユーザ エージェントの両方によって同じユーザが検出されると、重大ではないエラーがログに書き込まれます。

これを防ぐには、TS エージェントの IP アドレスがユーザエージェントによってログに記録されないようにします。詳細については、Firepower ユーザ エージェント コンフィギュレーション ガイド [英語] を参照してください。

解決済みの問題

解決済みの問題

不具合 ID 番号	説明
CSCvp10012	TS エージェントがインストールされている場合、Windows Server が応答しなくなることがなくなりました。
CSCvn28482	TAC ダンプの実行時に TS エージェントが応答しなくなることがなくなりました。さらに、ドライバフィルタを含む XML ファイルがダンプに追加されました。

TS エージェントの履歴

機能	バージョン
• Citrix Provisioningのサポートが追加されました。 • TS エージェントの [予約ポート（Reserve Port(s)）] フィールドで指定する値は、Citrix Provisioning の [最初と最後の UDP ポート番号（First and Last UDP port numbers）] のポートのいずれかと一致する必要があります。 **注意** 正しいポートを指定しないと、クライアントの起動に失敗します。	1.3

機能	バージョン
• サーバ上の IP アドレスの変更を検出し、設定を保存して再起動するように求めます。TS エージェントの設定フィールド を参照してください。 • 以前のバージョンをアンインストールせずに、このバージョンにアップグレードできます。TS エージェントのインストールまたはアップグレード を参照してください。 • [除外ポート（Exclude Port(s)）] 設定フィールドの名前が [予約ポート（Reserve Port(s)）] に変更されました。TS エージェントの設定フィールド を参照してください。 • エフェメラルポートのサポート。TS エージェントの設定フィールド を参照してください。 • [モニタ（Monitor）] タブページでは、特定のセッションで TCP または UDP ポートの 50% 以上が使用されている場合に警告が表示されます。TS エージェントに関する情報の表示 を参照してください。 • Least Recently Used ベースで割り当てられたユーザセッションポートの範囲。シスコ ターミナル サービス（TS）エージェントについて （1 ページ） を参照してください。 • トラブルシューティング情報を XML ファイルにエクスポートできます。TS エージェントに関する情報の表示 を参照してください。 • Firepower Management Center にユーザセッションを再ストリーミングできます。TS エージェントに関する情報の表示 を参照してください。 • TS エージェントがアンインストールされると、すべてのユーザセッションを終了しようとします。TSエージェントのアンインストール を参照してください。	1.2
• 最大ユーザセッションのデフォルトの最大数が 200 から 30 に変更されました。 • ポート範囲が 200 以上から 5000 以上に変更されました。 これらの変更については、すべてTS エージェントの設定フィールドで説明されています。	1.1

機能	バージョン
TS エージェント 導入された機能。TS エージェントを使用すると、管理者はポートマッピングを使用してユーザアクティビティを追跡できます。TS エージェントは、ターミナルサーバにインストールされると、一定のポート範囲を個別のユーザセッションに割り当て、その範囲内のポートをユーザセッションにおける TCP および UDP 接続に割り当てます。システムは、ネットワーク上のユーザによる個別の TCP および UDP 接続を識別するために一意のポートを使用します。	1.0