Symantec™ Product Authentication Service™ 管理者ガイド

Linux、Microsoft Windows および UNIX

4.3

symantec.

Symantec Product Authentication Service 管理者ガイド

Documentation version 1.6

Symantec Corporation
http://www.symantec.com

サード パーティ（第三者）製ソフトウェアの権利に関する通知

本製品には、特定のサード パーティ製ソフトウェアが配布、組み込み、または同梱されている場合があります。また、本製品のインストールおよび使用にともない、サード パーティ製ソフトウェアの使用を推奨する場合があります。同サード パーティ製ソフトウェアのライセンスは、著作権の保有者により別途付与されます。サード パーティ製ソフトウェアの使用については、それらのライセンス規約に従ってください。この章には、サード パーティ製ソフトウェアの使用条件を含むライセンスに関する情報および原著作者の権利表示が記載されています。Symantec Corporation は、これらのサード パーティ製ソフトウェアに対する表明や保証を一切いたしません。Symantec Corporation は、これらのサード パーティ製ソフトウェアのサポートを行わず、その使用に関連する責任を負わないものとします。

テクニカルサポート

製品のサポートを受けるには、http://support.veritas.com ページへアクセスし「Phone Support」または「E-mail Support」をクリックします。このページから TechNote、Software Alerts、ソフトウェアのダウンロード、ハードウェア互換性リスト、VERITAS Email Notifications サービス などにアクセスすることもできます。「Knowledge Base Search」機能を使用し、製品ドキュメントのリリースなどの製品情報へアクセスすることができます。

目次

はじめに

第 1 章 今回のリリースの新機能

第 2 章 Symantec Product Authentication Service の概要

第 5 章　コマンドライン インタフェース

はじめに

このマニュアルは、Symantec Product Authentication Service の管理者を対象としています。また、このマニュアルの読者が、コンピュータの一般的なセキュリティ システムとそれらに関連する概念について基本的に理解していることを想定しています。

「はじめに」の内容は次のとおりです。

このマニュアルの内容

次の表に、このマニュアルに含まれる章および付録を示します。

表 -1　　このマニュアルの内容

タイトル	説明
第 1 章「今回のリリースの新機能」	4.3 の新機能
第 2 章「Symantec Product Authentication Service の概要」	Symantec Product Authentication の理解に必要なコンポーネント、アーキテクチャ、プリンシパルおよび概念の概要
第 3 章「Symantec Product Authentication Service のインストール」	Symantec Product Authentication Service のインストールに関する参照情報
第 4 章「管理コンソール」	管理コンソールへのアクセスおよび使用方法
第 5 章「コマンドライン インタフェース」	コマンドライン インタフェースへのアクセスおよび使用方法
第 6 章「その他の管理作業」	コンソールまたはコマンドライン インタフェース以外の管理作業
付録 A「デバッグおよびログ」	Symantec Product Authentication Service のデバッグおよびログ
付録 B「LDAP プラグインの詳細情報」	LDAP プラグインについての詳細情報 (第 2 章「Symantec Product Authentication Service の概要」で必要なほぼすべての情報が記載されています)

アクセシビリティ

Symantec 社製品は、米国リハビリテーション法第 508 条に定義されている、ソフトウェアについてのアクセシビリティの要件を満たしています。

- http://www.access-board.gov/508.htm

主なグラフィカル ユーザー インタフェース (GUI) 操作およびメニュー項目すべてに対して、キーボードのショートカットを使用できます。Symantec 社製品は、オペレーティング システムのアクセシビリティ設定および様々な補助技術に対応しています。また、すべてのマニュアルはアクセシビリティに対応した PDF ファイルで提供されており、オンライン ヘルプは対応するビューアで表示される HTML で提供されています。

表記規則

この項では、このマニュアルで使用する表記規則について説明します。

表記規則

表 -2 表記規則

書体	使用方法
固定幅フォント （太字）	入力する文字。例：ディレクトリを変更するには、**cd** と入力します。
固定幅フォント	パス、コマンド、ファイル名または出力。例：デフォルトのインストール ディレクトリは、/opt/VRTSxx です。
固定幅フォント （斜体）	プレースホルダの文字列または変数。例：*filename* は、ご使用のファイル名に置き換えてください。

注意および警告

メモ：これはメモです。製品の使用をより簡単にしたり、問題の回避に役立つ情報への注意を促します。

注意：これは注意です。データが損失する可能性のある状況について警告します。

キーの組合せ

キーボード コマンドには、同時に 2 つ以上のキーを使用するものもあります。たとえば、[Ctrl] キーを押しながら、別のキーを押します。キーボート コマンドは、プラス記号でキーをつなげて示されます。次に例を示します。

[Ctrl]+[t] を押す

1

今回のリリースの新機能

Symantec Product Authentication Service バージョン 4.3 の新機能は、次のとおりです。

- Generic Security Service 認証プラグインのサポート
- リモート識別情報 : リモート ブローカで特定の CLI を使用できるようになったため、新しいパラメータが追加されました。次に例を示します。
  - `vssat setuptrust`
  - `vssat listpd`
  - `vssat createpd`
  - `vssat addprpl`
- 新しい API サブルーチンによって提供される、Symantec Product Authentication Service のリモート管理の拡張機能
- 新しい CLI コマンド
  - `vssat showispbxexchflag`: ブローカに PBX Exchange Installed 属性が設定されているかどうかを表示します。(5-48 ページの「showispbxexchflag」を参照。)
  - `vssat setispbxexchflag`: PBX Exchange Installed 属性を有効または無効のいずれかの状態に設定します。(5-30 ページの「setispbxexchflag」を参照。)
  - `vssat showcredinfo`: ターゲット マシン上で、リモートから提供された識別情報のプリンシパルおよびドメイン情報を表示します。(5-43 ページの「showcredinfo」を参照。)

2

Symantec Product Authentication Service の概要

この章では、Symantec Product Authentication Service の概要について説明します。内容は次のとおりです。

基本的な用語

用語集は、このマニュアルの最後にあります。この章では、用語集では説明できなかった Symantec Product Authentication Service の基本を理解するために必要な概念について、さらに詳細に説明します。

認証 (Authentication)

識別情報の検証。これは、次のように行われます。

どなたですか？

私は Pat です。

証明してください。

はい。ここに私を証明するマテリアルがあります。

確認しました。これは、あなたが Pat であると確認したことを示す証明書です。この証明書とあなたの秘密鍵を組み合わせると、有効な製品クレデンシャルになります。

認可 (Authorization)

基本的にはアクセス制御。つまり、誰が何に対して何をすることが許可されているかを判断することです。これは、次のように行われます。

私は Pat であると証明されています。Pat として、製品リソース Y に対して X を実行することを要求します。

あなたが Pat であることを確認しました。規則を参照して、あなたが製品リソース Y に対して X を実行することが許可されているかどうかを確認します。

セキュリティ ポリシー (Security Policy)

製品がユーザーの環境でどのように使用されるべきか、どのように誤用される可能性があるか、アクセス規則のどの範囲を製品によって有効にするかを考慮して、十分に検討して決定した一連の事項。

ポリシーの許容範囲を設定するときは、次の事項を考慮する必要があります。

- その製品を使用する必要があるのは誰 / 何か
- あるリソースに対するある作業の実行を許可される必要があるのは誰 / 何か

Secure Sockets Layer プロトコル (Secure Sockets Layer Protocol)

Secure Sockets Layer (SSL) は、Netscape 社が開発した公開鍵プロトコルで、クライアントとサーバーが Web を介してセキュリティ保護された通信を行うために使用されます。たとえば、クレジット カードなどの機密データをインターネット上で転送するためによく使用されます。

その名が示すように、SSL は、通信パケットのネットワーク層で動作します。これは、TCP/IP 層の上層で、HTTP などの上位アプリケーション プロトコルが使用する領域の下に位置します。

各暗号化トランザクションは、SSL を使用して、40 ビットまたは 128 ビットのセッション鍵を生成します。セッション鍵は、長いほどセキュリティが強化されます。

SSL 接続を使用すると、クライアントとサービスの間のすべての通信は送信側で暗号化され、受信側で復号化されます。このプロトコルは、クライアント認証とサービス認証の両方を提供できます。

SSL と Symantec Product Authentication Service

SSL テクノロジは、Symantec アプリケーション クライアント、認証ブローカおよび Symantec アプリケーション サービスの間でセキュリティ保護された通信を提供します。

認証プロセス中、クライアントは SSL 層を使用して認証ブローカと通信し、製品クレデンシャルを要求します。プリンシパルが認証されると、Symantec アプリケーション クライアントと Symantec アプリケーション サービスとの間に SSL 接続が確立されます。クライアントとサービスは、SSL 接続を介して対話し、クライアントが通信を終了するまで、必要なだけメッセージが送受信されます。

Symantec Product Authentication Service の特徴と目的

Symantec Product Authentication Service には、次の役割があります。

- ユーザー識別情報の検証と、その情報を利用した認可およびアクセス制御の基準を作成する
- メッセージの完全性および機密性の保持されたサービスによって、Symantec アプリケーション クライアントと Symantec アプリケーション サービス間の通信チャネルを保護する

Symantec Product Authentication Service は様々な認証メカニズムを使用可能なため、既存の認証ドメインから将来導入される認証ドメインまで、さらに、複数のオペレーティング システム環境間の認証をサポートします。

セキュリティ管理者は、必要に応じて、Symantec アプリケーションにシングル サインオン サービスを提供するように認証を構成することもできます。この場合、ユーザーは 1 つの Symantec アプリケーションにログオンするだけで、最初のログオンによって取得したクレデンシャルを使用して、他のアプリケーションも使用できるようになります。

SSPI プラグインによるシングル サインオン認証

Windows のセキュリティ サポート プロバイダー インターフェース (SSPI) は、Microsoft 社のプラットフォーム上で動作するアプリケーション間で使用する、認証および通信の一連のセキュリティ サービスを提供します。

Symantec Product Authentication Service は、SSPI プラグインとともに動作して、Microsoft 社のプラットフォームと統合されたログオンを可能にします。ユーザーは、別のパスワードを入力する必要がありません。

たとえば、ユーザーが、NT ドメインのアカウント / パスワードを使用して Windows マシンにログオンしているとします。Symantec Product Authentication Service は、SSPI を使用してクレデンシャルを取得します。この SSPI 接続は、Symantec アプリケーション クライアントから認証ブローカへのものです。Symantec アプリケーション クライアントから Symantec アプリケーション サービスへの通信には、相互に認証された SSL が使用されます。認証ブローカの認証では、Symantec Product Authentication Service はプリンシパルが属するすべての OS グループを取得します。

認証プリンシパル

認証プリンシパルは、一意の識別情報によって Symantec Product Authentication Service の認証を受けることができるエンティティです。通常、認証プリンシパルは人間のユーザーを表します。ただし、識別情報は人間ではなく、コンピュータ、サービス、またはコマンドライン インタフェース (CLI) などのプロセスにも関連付けられます。

Symantec 社のリソース管理アプリケーションの多くは、それ自身が認証プリンシパルになります。つまり、実行中のオペレーティング システムのログイン アカウントとは別な識別情報を利用して個別の識別情報に基づいて認証されます。認証を受けるものについて説明するときは、(セキュリティ プリンシパルと区別して) 認証プリンシパルという用語を使用します。

コンポーネントの概要

Symantec Product Authentication Service は、次のコンポーネントから構成される分散アプリケーションです。

- 認証ブローカ (サーバー)
- 認証クライアント (ランタイム)
- 認証プラグイン
- 管理 UI (CLI および GUI)
- 製品グループによって使用される SDK (Java、C API)

コンポーネントおよび構成要素の説明

この項では、Authentication の設定でのコンポーネントおよび構成要素について説明します。

- アプリケーション ホスト
  Symantec アプリケーションが実行されているマシン。
- 認証ブローカ
  ルート ブローカよりレベル (層) が 1 つ下の中間登録局および認証局として機能するコンポーネント。認証ブローカは、クライアント (ユーザー、サービスなど) の認証を行い、製品クレデンシャルを付与することができます。ただし、他のブローカを認証することはできません。他のブローカの認証は、ルート ブローカで実行する必要があります。
- 認証ライブラリ
  Symantec アプリケーション クライアントにリンクするコンポーネント。認証の要求を行うプログラムの呼出しを実装します。概念上、このライブラリは通信のセキュリティを保護する認証とは区別されていますが、実際には、2 つのコンポーネントは 1 つのライブラリにまとめられています。
- 認証メカニズム
  ドメインで定義された特定の名前空間内のプリンシパルに対して認証を行う方法。たとえば、Kerberos ドメインでは、Kerberos ticket およびパスワードが使用されます。UNIX プラットフォームの場合、Kerberos ドメインは GSS-API を介して使用されます。認証メカニズムは、認証アルゴリズムのすべての細目 (API、プロトコル、トークン形式、トークン コンテンツの構文、データベース オブジェクト形式など) をカプセル化します。関連する構成要素は、メカニズムごとに異なります。

- 認証プラグイン
  認証ブローカによって、特定のドメイン内で識別情報を検証するために使用されるコンポーネント。認証プラグインは、サポートされている認証メカニズムごとに存在します。たとえば、あるプラグインで NIS の識別情報とパスワードの組合せの検証を NIS データベースに対して行うことが可能な一方で、別のプラグインではプリンシパルの認証を行う際に Kerberos ticket を利用できます。
  すべてのプラットフォーム用にそれぞれのプラグインを用意する必要はありません。指定された Symantec アプリケーション クライアントが必要とする認証は、通常、1 つまたは 2 つのドメインに対してのみです。従って、必要なプラグインも 1 つまたは 2 つ程度 (前述のパスワード プラグインのように、単一のプラグインで両方のドメインで利用できない場合) です。たとえば、UNIX マシンで実行されている認証ブローカでは Microsoft 固有の認証プラグインを使用する必要はありません。

- 通信ライブラリ
  Symantec Product Authentication Service の一部。Symantec アプリケーション クライアントと Symantec アプリケーション サービス間で、あらかじめ認証処理で取得した Symantec クレデンシャルを使用してセキュリティ保護された通信を提供します。概念上、このライブラリは識別情報の認証とは区別されていますが、実際には、2 つのコンポーネントは 1 つのライブラリにまとめられています。

- リソース管理アプリケーション
  Symantec Product Authentication Service および Symantec Product Authorization Service によってリソースが保護されている Symantec 社製品のこと。

- ルート ブローカ
  自己署名した証明書を持つ最上位にある認証ブローカ。ルート ブローカは、有効と判断されるブローカの名前だけを保持する 1 つのプライベート ドメインを持ちます。ルート ブローカ自身の名前は、完全修飾されたドメイン名 (FQDN) としてそのプライベート ドメインに格納されます。

- Symantec アプリケーション サービス
  Symantec アプリケーション クライアントから要請されてサービスを提供するプログラム。

- Symantec アプリケーション クライアント
  Symantec アプリケーション サービスと呼ばれる別プログラムが提供するサービスまたは機能にアクセスするプログラム。セキュリティ保護されたアプリケーション クライアントには、VERITAS Volume Manager GUI などがあります。Symantec アプリケーション クライアントは、Symantec

Authentication を使用して、そのクライアントのユーザーの ID を検証します。

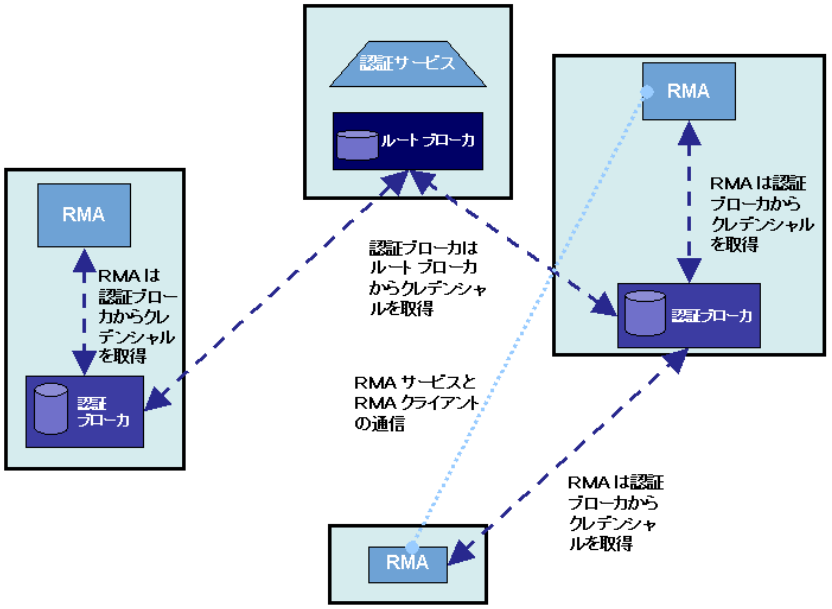
- インタフェース
  セキュリティ管理者が、Symantec Product Authentication Service の様々な機能を管理するために使用するコンポーネント。CLI と管理コンソールの 2 つのインタフェースがあります。
- SDK
  社内のソフトウェア グループによって使用されるソフトウェア開発者キット。Java および C API で構成されます。

構成要素およびアーキテクチャの図

次の図に、コンポーネント全体での動作の仕方を示します。最初の図 (図 2-1「構成要素およびアーキテクチャの図」) の動作の仕方は、次のとおりです

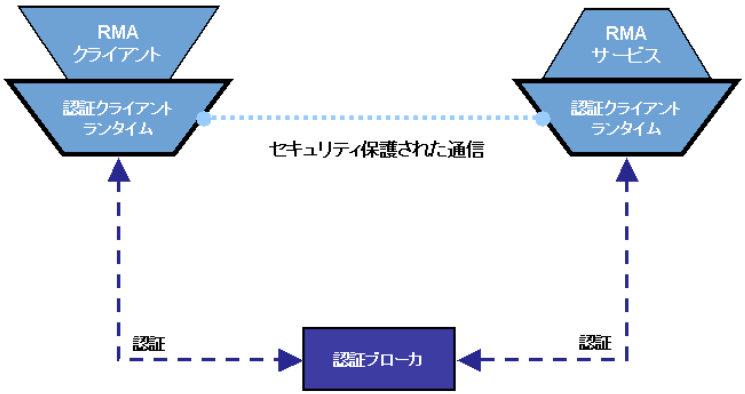
- ルート ブローカは、認証ブローカを認証しています。
- 認証ブローカは、リソース管理アプリケーション (RMA) を認証しています。
- Symantec アプリケーション サービスは、アプリケーション ホスト上で動作していて、そのクライアントの 1 つと通信しています。

図 2-1　　構成要素およびアーキテクチャの図



2 番目の図 (図 2-2「リソース管理アプリケーションおよび AT」) は、RMA クライアント マシンと RMA サービス マシンの両方に認証クライアントがインストールされている必要があることを示します。

図 2-2　　リソース管理アプリケーションおよび AT



ルート ブローカおよび認証ブローカの詳細については、2-8 ページの「ブローカの種類」の図を参照してください。

ブローカの種類

認証を理解するには、ルート ブローカと認証ブローカの 2 種類のブローカを区別する必要があります。

ルート ブローカ

Symantec Product Authentication Service では、最初に設定されたブローカをルート ブローカと呼びます。これは、認証の階層ツリーの最上位に位置します。ルート ブローカは、非常に特殊なもので、単に「認証ブローカ」と呼ばれることはありません。常にルートまたはルート ブローカとして区別されます。

ルート ブローカは、認証ブローカより信頼性があり、高い権限を持っています。

- ルート ブローカは、自己署名した証明書で自身を検証します。
- ルート ブローカは、他のブローカを認証できます。
- ルート ブローカは、認証ブローカだけを含む PDR を持っています。

図 2-3　　ルート ブローカ ホスト

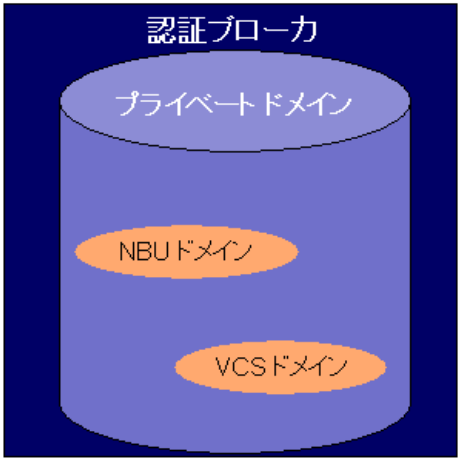
認証ブローカ

ルート以外に、多数の認証ブローカが存在する場合があります。認証ブローカは、認証の階層ツリーの中でルート ブローカより 1 つ下のレベル (層) に位置します。各認証ブローカは、クライアント (ユーザー、サービスなど) を認証することができる中間登録局および認証局として機能します。

認証ブローカは、次の 2 つの主要なサブコンポーネントで構成されます。

- 登録局は、認証プリンシパルが正当な利用者かどうかを判断します。
- 認証局は、登録局による妥当性の確認に基づき、要求された認証プリンシパルに対する製品クレデンシャルを発行します。

図 2-4 認証ブローカの例



各認証ブローカは、プライベート ドメイン リポジトリを持ち、このブローカで使用するように選択されたサービスおよびリソース管理アプリケーション ユーザーを格納しています。この図は、NBU および VCS のドメインを示しています。また、認証ブローカは様々なプラグインも持っています。

場合によっては、専用のマシン上に認証ブローカが存在する場合もあります。多くの場合、認証ブローカは、アプリケーション ホスト上に存在します。

ルート ブローカと認証ブローカの違いの概要

ルート ブローカは、次の点で認証ブローカと異なります。

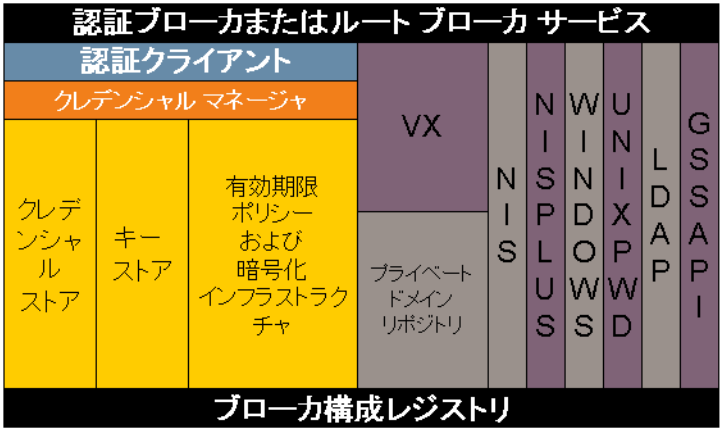
- ルート ブローカは自己署名した証明書を持ち、認証ブローカはルートによって署名された証明書を持ちます。
- ルート ブローカは、他の認証ブローカを認証できます。通常の認証ブローカは、クライアントおよびサービスを認証できますが、他の認証ブローカを認証できません。
- ルート ブローカは、特別な形式のプライベート ドメインを持っています。

注意 : ルート ブローカの管理者は、ルート ブローカのプライベート ドメインに認証ブローカだけを配置する必要があります。ルート ブローカ自身の名前は、完全修飾されたドメイン名 (FQDN) としてそのプライベート ドメインに格納されます。

ブローカのアーキテクチャの詳細

次の図に、ブローカ サービスのアーキテクチャの詳細を示します。

図 2-5　　認証ブローカまたはルート ブローカ サービス



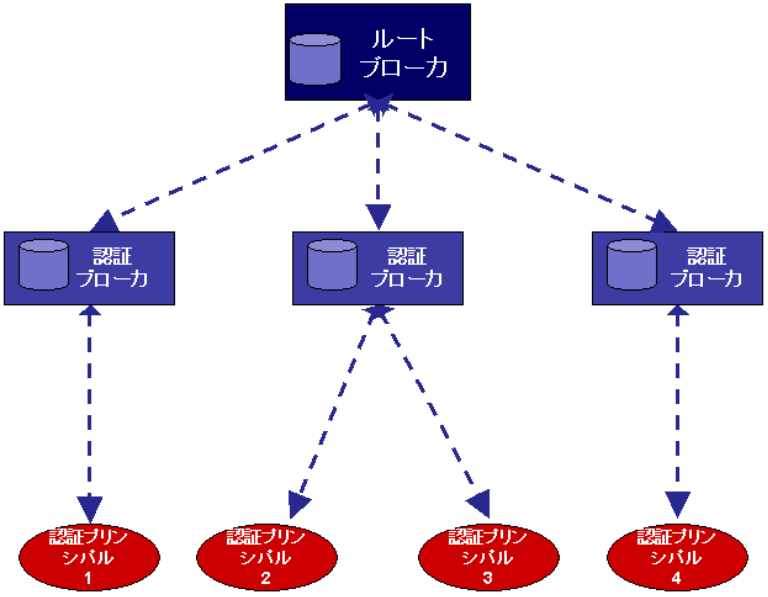
認証ブローカ ツリー (証明書の階層)

Symantec Product Authentication Service は、3 つのレベル (層) で構成される証明書の階層を実装しています。これを、認証ブローカ ツリーと呼びます。次に 3 つのレベル (層) を示します。

- レベル 1: ルート ブローカ
  ルート ブローカは、各認証ブローカ ツリーの中で、認証ブローカのルート認証局および登録局として機能します。ルート ブローカは、認証ブローカだけを含むプライベート ドメインを 1 つ持っています。
- レベル 2: 認証ブローカ
  その他の認証ブローカは、プライベート ドメインを持たないか、1 つ以上持っていて、そのメンバーの種類は、ユーザー、サービス、コマンドライン インタフェースと様々です。これらは、各識別情報に属性を持たせることによって、プライベート ドメイン リポジトリ (PDR) 内で識別されます。
- レベル 3: アプリケーション クライアントおよびアプリケーション サービス

次に図を示します。

図 2-6 認証ブローカのツリーの図



認証ブローカによって使用されるポート

すべての認証サーバー (ルート ブローカ、認証ブローカ、ルート＋認証ブローカ) は、IANA に登録済みのポート 2821 で待機します。このポート番号は、コマンドライン インタフェースで vssat コマンドを使用して変更できます。(5-7 ページの「vssat の使用」を参照。) ルート ブローカ、認証ブローカ、またはルート＋認証ブローカに接続する場合は、ポート番号に 2821 を指定する必要があります。管理コンソールおよびコマンドライン インタフェースの管理コマンドでは、認証サービスに接続時のポート番号がデフォルトでは 2821 に設定されています。

認証ブローカは、PBX サービスからの要求を受け取るように構成することもできます。このような構成の場合は、共通の PBX ポート 1556 でも要求を受け取ります。

クライアントが使用するブローカを識別する方法

セキュリティ管理者は、クライアントが認証を受けるために問い合わせる認証ブローカをドメインごとに選択できます。ドメイン ブローカのマッピングは、各ドメインで利用する認証ブローカを示す情報の集まりです。次に例を示します。

- nis+ クライアントである場合は、認証ブローカ A を使用
- unixpwd クライアントである場合は、認証ブローカ B を使用

Symantec アプリケーション クライアントが識別情報および Symantec アプリケーション サービスによって信頼された認証ブローカの位置を取得するには、次の 2 つの方法があります。

- ローカル構成から取得する。
- Symantec サービスから提供される情報を使用する。たとえば、VERITAS Enterprise Administrator サービスは、クライアントに、同じ場所またはリモートにあるブローカに関する情報を知らせることができます。

クレデンシャルと証明書

クレデンシャルと証明書は、混同しやすい用語です。これらは同義ではありません。

- 証明書は、電子パスポートまたは ID カードの一種で、所有者の識別情報を保証して、プリンシパルの名前をユーザーの公開鍵に関連付けるものです。
- 製品クレデンシャル (略してクレデンシャルとも呼ばれる) は、認証されたプリンシパルとして認識される資格です。これには証明書が含まれますが、プリンシパルの秘密鍵も含まれている必要があります。両方がそろっていないと、クレデンシャルにはなりません。

メモ : 名前に credential (クレデンシャル) と付いている API サブルーチンは、certificate (証明書) と称した方が正確であるように思われる場合も多数あります。これは、認証ライブラリが、ユーザーが PKI 証明書の複雑さを理解しなくても API を効果的に使用できるようになっているためです。

製品クレデンシャル

製品クレデンシャルは、有効な識別情報として認識されるために必要な資格です。製品クレデンシャルには、プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された (1) プリンシパルの秘密鍵と (2) 特殊な拡張定義を含む X.509v3 証明書が必要です。製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作する、Symantec Product Authentication Service が使用可能なすべての Symantec アプリケーションに対して有効なシングル サインオン証明書です。

製品クレデンシャルが必要な場合

Symantec 社のすべてのリソース管理アプリケーションには 2 つのコンポーネントがありますが、その両方とも有効なクレデンシャルによって認証される必要があります。

- Symantec アプリケーション クライアント
  Symantec アプリケーション クライアント (略してクライアントとも呼ばれる) は、Symantec 社のサービスまたは別のプログラムによって提供されるサービスまたは機能にアクセスするプログラムです。
- Symantec アプリケーション サービス
  Symantec アプリケーション サービス (略してサービスとも呼ばれる) は、要求されたサービスを提供するプログラムです。

クライアントおよびサービスは、認証を求めるときは、どちらもクライアントとして動作します。クレデンシャルは、アプリケーション クライアントあるいはアプリケーション サービスのどちらに付与されるかによって異なります。通常、サービスに付与されるクレデンシャルは、クライアントに付与されるものより長い期間有効です。

製品クレデンシャルの拡張属性

製品クレデンシャルの拡張属性には、プリンシパルのグループ メンバーシップおよびクレデンシャルが付与されるマシンの IP アドレスがあります。これらの拡張属性を使用すると、通信ライブラリが、所定の通信セキュリティ ポリシーを適用するようになります。たとえば、Symantec Execs と呼ばれるグループに属するプリンシパルがあるとします。ポリシーによって、このグループのメンバーへのすべての通信を 128 ビット暗号化アルゴリズムまたはそれ以上の方法で暗号化し、他のグループのメンバーへの通信とは区別することができます。

証明書の署名者

プリンシパルが正当な利用者であることを示す証明書は、認証局の各階層で署名されます。ルート ブローカのルート認証局は、階層の最上位に位置するエンティティで、そのため最も信頼できる認証局です。ルート自身を証明する証明書は自己署名されており、ルート証明書と呼ばれます。

アプリケーション プログラム環境には、認証ライブラリが有効なクレデンシャルの署名者として受け入れる、一連のルート証明書が含まれています。この情報は、事前に設定しておくことも、Symantec アプリケーション サービスから取得することもできます。プリンシパルには、このルート証明書をレジストリ構成の一部として格納できます。ただし、実際には、次にあげるいくつかの標準形式に従って、個別のファイルまたは一連のファイルに格納する方法が一般的です。

- 標準としての PKCS#12
- Java JSSE が使用する JKS
- OpenSSL および S/MIME 実装用の PEM

クレデンシャルの有効期間

クレデンシャルには、単一の有効期間はありません。

認証ブローカの管理者は、ID を作成するときに、サービス、コマンドライン インタフェース、ユーザーなど、どの種類のセキュリティ プリンシパルに使用する ID であるかを指定できます。この情報はプライベート ドメインに渡されて、エンティティが取得するクレデンシャルの有効期間に影響を与えます。

メモ: この ID 情報は、ルート以外の認証ブローカのプライベート ドメインに属する情報であるため、ルート ブローカのプライベート ドメインに置かれることはありません。状況によって、管理者は、プライベート ドメインの代わりに NT ドメインまたは NIS ドメイン (非プライベート ドメイン) を使用することもできます。管理者がこのドメインを使用する場合、認証サービスは、プリンシパルがサービスまたはユーザーのどちらであるかを判断できません。

Symantec アプリケーション サービスに対して発行される製品クレデンシャルは、Symantec アプリケーション クライアントに対するものより長い期間有効である方が都合がよいものです。これは、サービスが、できるだけ長い期間動作すべきものであるためです。

クレデンシャルの有効期間は、クレデンシャルが発行されたマシン上でその情報が存続する期間を決定します。X.509 証明書に関連する公開鍵テクノロジには、クライアントだけに保存される秘密鍵があります。これに関連するクレデンシャルおよび秘密鍵はディスク上に保存されて、Symantec Product Authentication Service 内部の独自の難読化メカニズムを使用して、難読状態が維持されます。

特殊なクレデンシャル

次の 2 つの特殊なクレデンシャルがあります。

- プロキシ クレデンシャル
  プロキシ権限を付加した特殊な長期間のクレデンシャルで、Web コンソールを構成するときに、コンソール ユーザーの代わりに取得されます。このクレデンシャルのプロキシ権限によって、Web コンソール プロキシが実際のユーザーの代わりになります。
- 製品 Web クレデンシャル
  特殊なクレデンシャルで、ライブラリ内に対応する秘密鍵が存在しないことを Symantec Product Authentication Service に示します。製品 Web クレデンシャルは、プロキシ権限を持つ Web コンソールのクレデンシャルとともに使用する必要があります。

クレデンシャルのライフ サイクル

クレデンシャルの妥当性は制限されています。各クレデンシャルには、`notvalidBefore` および `notValidAfter` の時間が設定されています。これら 2 つの時間の間が有効期限となり、この期間は認証ブローカによって制御されます。

有効期限ポリシーは構成可能です。

クレデンシャルのライフ サイクルには、次の段階があります。

- 使用開始 : 管理コンソールまたは CLI からクレデンシャルがストアに追加されます。
- 使用中 : クレデンシャルが使用されます。
- 使用終了 : クレデンシャルの有効期限が切れるか、有効期限が管理コンソールまたは CLI から抹消されます。

場合によっては、クレデンシャルが更新され、新しいライフ サイクルが開始されます。

認証の起動

この項では、起動プロセスについて説明します。

認証サブシステムを起動するために実行される手順は、次のとおりです。

1. ルート ブローカがインストールされます。
2. ルート ブローカは、自身が使用する鍵ペアと自己署名した証明書を生成します。

メモ: 鍵ペアの生成は透過的に実行されます。

3 Symantec Product Authentication Service の管理者が、ルート ブローカの認証プライベート ドメイン リポジトリ内の認証ブローカの識別情報を構成します。

4 認証ブローカは、インストール時に、ルート ブローカのホスト名または IP アドレスおよびポートを設定します。

5 認証ブローカは、ルート ブローカに接続して、管理者から提供されたパスワードによって自身を識別します。

6 ルート ブローカは、認証ブローカの識別情報を検証して、認証ブローカ証明書を生成します。

7 ルート ブローカは、認証ブローカに至るまでの証明書を発行します。

8 認証ブローカは、認証プリンシパルを認証して証明書を発行します。つまり、認証ブローカは中間の認証局として機能します。

メモ: セキュリティ プリンシパルはルート ブローカの証明書を信頼する必要があり、ルート証明書は認証サービスのすべてのクライアントに配布される必要があります。

ルート証明書の配布

セキュリティ レベルが非常に高い場合は、ルート証明書を手動 (フロッピー ディスクなど) で配布することをお勧めします。それ以外の場合は、クライアントまたはアプリケーションが、信頼関係の確立用の API によってルート証明書をダウンロードします。

セキュリティ管理者は、ルート証明書の配布に関して、次のいずれかのセキュリティ レベルを設定できます。

- 高セキュリティ : これまで信頼できなかったルートがピアから取得された場合 (同じ署名のある証明書が信頼できるストア内に存在しない場合) に、ユーザーはハッシュの検証を求められます。
- 中セキュリティ : 最初の認証ルート ブローカが信頼され、プロンプトは表示されません。後続の認証ルート ブローカとの信頼関係の確立が試行されると、証明書が信頼できるストアに追加される前に、ユーザーはハッシュの検証を求められます。
- 低セキュリティ : 認証ブローカ証明書は常に信頼され、プロンプトは表示されません。

メモ: 信頼関係は継承できます。

認証および通信の手順

クライアントの認証、および Symantec アプリケーション サービスとの通信確立の手順には、次の 2 段階があります。

- 製品クレデンシャルの取得
- クレデンシャルの使用

製品クレデンシャルの取得

以降の手順が実行される前に、クライアントおよびサービスは、両方ともローカルに鍵ペアを生成します。それぞれの鍵ペアには、秘密鍵と公開鍵の両方が含まれています。

メモ: クライアントまたはサービスは、鍵ペアを生成するために特別な作業を実行する必要はありません。この処理は透過的に行われます。

この処理は、次のように行われます。

1. Symantec アプリケーション クライアントは、クライアントおよびサービスの両方の認証ライブラリを初期化する関数を呼び出します。この操作によって、認証ライブラリのインスタンスが作成されます。
2. Symantec アプリケーション クライアントは、信頼できる認証ブローカとサポートされるドメインのリストを取得するためのプログラム的な呼出し操作を実行します。
   リモート認証ブローカに問い合わせることなく、ローカル ホストのプリンシパルを検証する方法については、2-23 ページの「ローカル ホスト検証」を参照してください。
3. 認証ブローカとの間に、SSL 接続が確立されます。
   SSL とは Netscape 社が開発した公開鍵プロトコルです。クライアントとサーバーが Web を介してセキュリティ保護された通信を行うために使用されます。Symantec Product Authentication Service の場合、Secure Sockets Layer テクノロジは、Symantec アプリケーション クライアント、認証ブローカおよび Symantec アプリケーション サービスの間でセキュリティ保護された通信を提供します。
   認証ブローカに到達できない場合の動作を決定するのは、認証クライアント ライブラリのユーザー次第です。認証 API から戻されるエラー コードは、

実際のエラーを示しているので、ユーザーは再試行または他の方法によってエラーに対処できます。

4 ユーザーは、認証ブローカに認証マテリアルを送信します。
認証マテリアルとは、公開鍵、識別情報、パスワード、ドメイン、ドメインタイプなどです。マテリアルの実際の種類は、使用する認証メカニズムの種類によって異なります。メカニズムの種類は、ドメインによって入力パラメータとして示されます。メカニズムによっては、認証を完了するために、ブローカとの間で複数回の通信を行う必要があるものもあります。
ユーザーが情報を提供しないと (たとえば入力内容に NULL が存在する場合など)、認証ライブラリは、現在のインスタンスに既存の製品クレデンシャルを再利用するか、運用中の別なシングル サインオン クレデンシャルを使用してユーザーを認証する場合があります。

5 認証ブローカは、それ自身の認証プライベート ドメイン リポジトリを調査して、認証を求めるエンティティが有効と見なされるかどうかを確認します。

6 エンティティが有効と見なされる場合、認証ブローカはそれ自身の秘密鍵を使用して、認証を求めるエンティティの公開鍵に署名します。これを行うために、X509 証明書を作成します。

7 認証ブローカは、X509 証明書を、検証を求めるクライアントまたはサービスに返送します。

8 クライアント側では、この署名された証明書とクライアント自身の秘密鍵が製品クレデンシャルになります。

9 認証ブローカとの間の SSL 接続がクローズされます。

クレデンシャルを使用したセキュリティ保護されたセッションの確立

クライアントおよびサービスは、入手した製品クレデンシャルを使用して、セキュリティ保護されたセッションを確立します。

通信セキュリティの種類

Symantec アプリケーション クライアントと Symantec アプリケーション サービスとの通信のセキュリティ レベルを設定するため、Symantec Product Authentication Service は、アプリケーションから認証通信 API の関数 `vrtsAtSecConnAccept` に渡される明示的なパラメータを使用します。

データ通信のセキュリティには、次の 3 つの種類があります。

- 高セキュリティ (レベル 0): VRTSAT_COMM_VERIFY_ENCRYPT: 暗号化および署名されたデータ チャネルを提供します。ハンドシェーク フェーズで、相互の認証が実行されます。

- 中セキュリティ (レベル 1): VRTSAT_COMM_VERIFY_NONE: 暗号化および署名されたデータ チャネルを提供します。ハンドシェーク フェーズで、相互の認証は実行されません。このレベルは、信頼できる環境だけで使用する必要があります。
- 低セキュリティ (レベル 2): VERIFY_COMM_ENCRYPT_NONE: 署名されたチャネルだけを提供します。ハンドシェーク フェーズで、相互の認証が実行されます。このレベルは、盗聴が問題にならないポイントツーポイントリンクだけで使用できます。

メモ: ピアは、同じ通信レベルを使用する必要があります。

中セキュリティ以上のレベルを使用することをお勧めします。前述のすべてのレベルにおいて、ピアは両方とも有効なクレデンシャルを持っている必要があります。

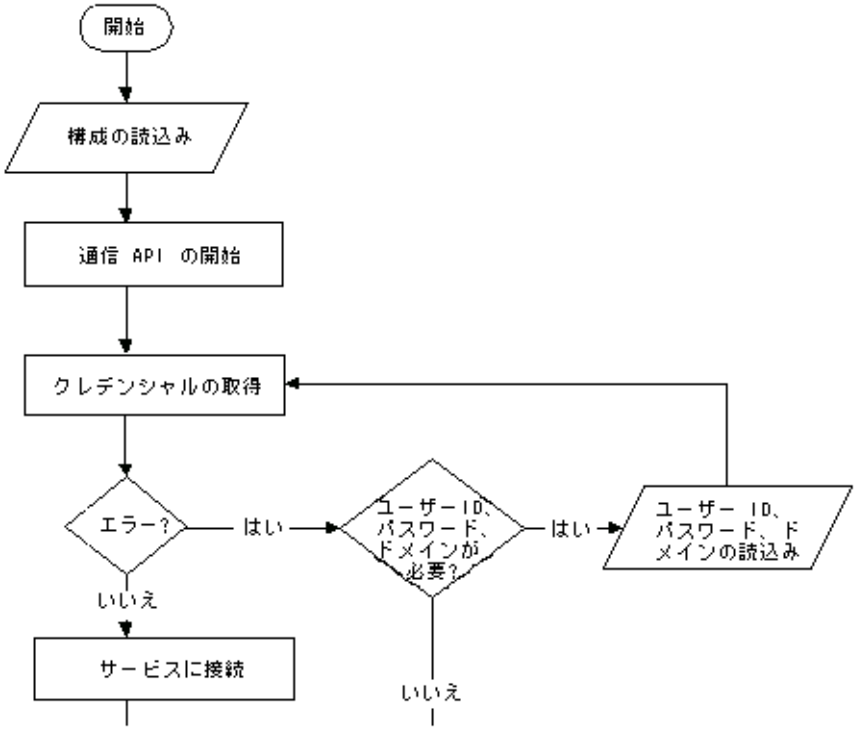
セキュリティ保護されたセッションを確立する方法

1. 通信 API を使用するエンティティは、次のようにセッションを開始します。
   a. クライアントは、API を使用してセッションを開始します。
   b. サービスは、API を使用して応答します。
2. 両方のピアが、それぞれの製品クレデンシャルを通信 API に渡します。
3. 通信 API は、ハンドシェークで 2 つのエンティティのクレデンシャルを交換し、相手が有効であることを検証します。
   これは、それぞれの相手のクレデンシャルに認証ブローカおよび認証ブローカが信頼するルート ブローカの署名があることを確認することによって実現します。
4. ハンドシェーク (相互の信頼を示す) が完了すると、セキュリティ保護されたセッションが形成されて、クライアントおよびサービスはデータを交換できるようになります。
5. アプリケーション クライアントが、Symantec アプリケーション サービスとのセキュリティ保護された接続を要求します。

処理の流れ図

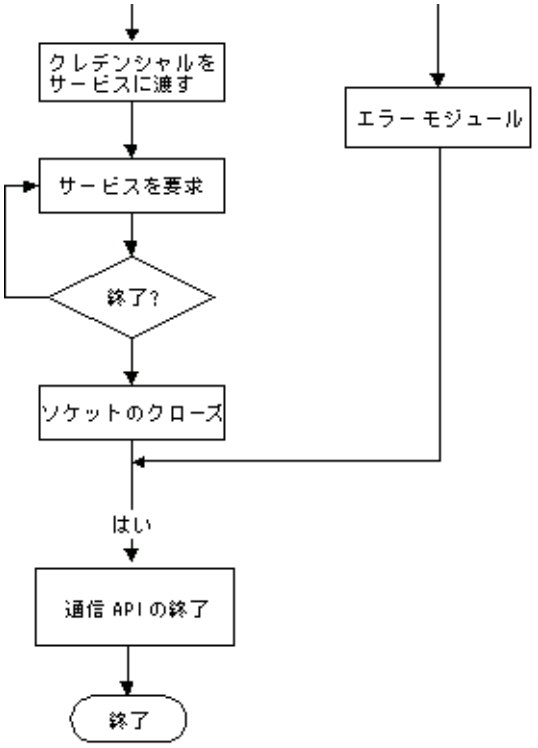
次に、通常のアプリケーション クライアントが Symantec Product Authentication Service を使用する際のプログラムの流れを、2 つの図に分けて示します。最初の図では、サービスに接続するまでを示します。

図 2-7　　認証を使用するクライアントの流れ図



2 つ目の流れ図では、サービスへの接続が確立された後の処理を示します。

図 2-8 認証を使用するクライアントの流れ図 (続き)



シングル サインオン認証

シングル サインオン認証を使用すると、Kerberos や Microsoft の統合的なログオンなどの既存のシングル サインオン メカニズムを利用できます。

シングル サインオンを使用する方法

1 ユーザーは、企業内のシングル サインオン システムに対して自身の認証を求めます。

2 検証されると、ユーザーはシングル サインオン クレデンシャルを取得します。

3 ユーザーは Symantec アプリケーションを起動します。

4 Symantec アプリケーションは、認証ライブラリに、シングル サインオン クレデンシャルを使用するように指示します。複数のシングル サインオン

クレデンシャルが有効である場合は、認証マテリアルに含まれるドメイン情報によってどれを使用するかが示されます。

5 シングル サインオン クレデンシャルが認証ブローカに送信されます。

6 認証ブローカは、シングル サインオン クレデンシャルを受け取って、企業内のシングル サインオン サービスを利用するように構成された、すべての Symantec Product Authentication Service 対応アプリケーションが使用する製品クレデンシャルを作成します。

Symantec アプリケーション クライアントは、企業内のシングル サインオン機能を利用するために、既存のシングル サインオン システムの形態、またはそのシステムが使用するクレデンシャルの形式を知る必要はありません。これらの情報を識別するのは、認証ライブラリの役割です。企業内のシングル サインオン サービスを使用するように構成またはプログラムされたアプリケーションは、ユーザー名およびパスワードの要求を行うプロンプトが不要なことを認識する必要があります。

ローカル ホスト検証

リソース管理アプリケーション (RMA) とは、Symantec Product Authentication Service によってリソースが保護されている Symantec 社製品のことです。アプリケーション ホストとは、Symantec 社の特定の RMA がインストールされたマシンを指します。

ローカル ホスト検証とは、リモート認証ブローカに問い合わせることなく、ローカル ホストのプリンシパルを検証する処理です。ローカル ホスト検証は、クライアント ライブラリそのものに実装されています。

次に、その処理を示します。

1 Symantec アプリケーション クライアントまたはサービスが、ローカル ホスト検証を要求します。認証クライアント ライブラリは、渡された識別情報の検証を試みます。この情報は、現在の識別情報のログイン コンテキストとして、または識別情報、ドメイン、ドメイン タイプとパスワードの組合せとして渡されます。

2 検証が成功すると、クライアント ライブラリは自己署名した証明書を生成します。

3 この証明書は、クライアントから、同じホスト上で動作しているアプリケーション サービスへ渡されます。

4 アプリケーション サービスは、`vrtsAtExtractInfo` API を使用して、プリンシパルの詳細情報を取得できます。

メモ: ローカル ホスト検証機能によって取得したクレデンシャルは、エンティティが低いセキュリティ レベルで動作している場合だけ、通信のセキュリティ保護のために使用されます。

この機能は、他のマシンに接続していないクライアントに使用することもあります。この場合、クレデンシャルが通信に使用されることはありません。認証が成功するかどうかのみに関与します。

Web コンソールを使用する場合の認証

Web コンソールを使用する場合の認証の手順は、前述の手順とは少々異なります。Web コンソールは、見た目も動作もデスクトップ コンソールと似ていますが、インターネットを介してアクセスできます。Web コンソールを使用する場合、クライアントはブラウザになりますが、ブラウザは製品クレデンシャルを保存することも表示することもできません。

そのため、Web コンソールでは製品 Web クレデンシャルと呼ばれる特殊なクレデンシャルを使用する必要があります。これは、プロキシ権限を持つクレデンシャルとともに使用します。

Web コンソールを使用する場合の構成方法については、『Symantec Product Authentication Service インストール ガイド』を参照してください。

認証メカニズム

各ドメインは、ユーザーの認証に、暗黙的な方法 (NIS+、認証プライベート ドメイン) または明示的な認証 API と、関連するプロトコルおよびアルゴリズムを使用します。

認証メカニズムは、ドメインで定義された名前空間内のユーザーに対して認証を行う方法です。認証メカニズムは、認証アルゴリズムのすべての細目 (API、プロトコル、トークン形式、トークン コンテンツの構文、データベース オブジェクト形式など) をカプセル化します。関連する構成要素は、メカニズムごとに異なります。

ドメインのマッピング

Symantec Product Authentication Service は、ドメインを 1 つの認証メカニズムに関連付けます。次に例を示します。

- Kerberos ドメインでは、Kerberos ticket およびパスワードが使用されます。UNIX プラットフォームの場合、Kerberos ドメインは GSS-API を介して使用されます。
- NT ドメインも Kerberos を基盤メカニズムとして使用できますが、ユーザーの名前空間は、UNIX によって使用される Kerberos ドメインの名前空間とは区別されます。その上、Windows 2000 では、Kerberos の機能は、UNIX の GSS-API ではなく SSPI インタフェースを介して実行されます。

これらのドメインは、それぞれ異なる認証プラグインにマップされます。

その逆はありません。つまり、各認証プラグインを、異なるドメインにマップする必要はありません。たとえば、Kerberos プラグインは、1 つの NT ネットワーク内の異なる多数のドメインに対応できます。

プラグイン

サポートされている各認証メカニズムには、プラグインがあります。プラグインとは、認証ブローカによって、特定のドメイン内で識別情報を検証するために使用されるコンポーネントです。各プラグインは、ドメイン タイプに 1 対 1 で対応します。

たとえば、あるプラグインで NIS の識別情報とパスワードの組合せの検証を NIS データベースに対して行うことが可能な一方で、別のプラグインではプリンシパルの認証を行う際に Kerberos ticket を利用できます。次に、プラグインのタイプを示します。

- nis - NIS v2 (以前は YP - イエロー ページと呼ばれていました)
- nisplus - NIS v3
- ldap - OpenLDAP および iPlanet による実装
- GSS - Generic Security Service Application Program Interface (GSS-API)
- nt - Windows NT ドメインおよび Active Directory (SSPI)
- vx - Symantec プライベート ドメイン

すべてのプラットフォーム用にそれぞれのプラグインを用意する必要はありません。指定された Symantec アプリケーション クライアントが必要とする認証は、通常、1 つまたは 2 つのドメインに対してのみです。従って、必要なプラグインも 1 つまたは 2 つ程度 (前述のパスワード プラグインのように、単一のプラグインで両方のドメインで利用できない場合) です。たとえば、UNIX マシンで実行

されている認証ブローカでは Microsoft 固有の認証プラグインを使用する必要はありません。

Symantec LDAP プラグイン

Symantec Product Authentication Service は、デフォルトで RFC 2307 のサポートを目的としたプラグイン モジュールを使用して、LDAP 認証をサポートしています。LDAP 認証プラグイン モジュールは、`authldap` と呼ばれる共有ライブラリで、認証ブローカに付属しています。

LDAP の導入に関する推奨事項

LDAP 認証プラグインを導入する場合の推奨事項は、次のとおりです。

- NIS データを LDAP ディレクトリに格納する場合、RFC 2307 で指定されているスキーマを使用する。
- 常にドメインごとに 1 つの LDAP ディレクトリ サーバーのみと通信するように構成する。
- Secure Sockets Layer (SSL) を有効にする。

LDAP の推奨事項の説明

Symantec Product Authentication Service では、プラグイン モジュールを使用した LDAP 認証がサポートされています。LDAP 認証プラグインは、常にドメインごとに 1 つの LDAP ディレクトリ サーバーのみと通信するように構成されます。

メモ: ユーザー名やパスワードなどのデータは、転送中は保護されないため、LDAP 認証プラグインを導入する場合は Secure Sockets Layer (SSL) を有効にすることをお勧めします。

LDAP プラグイン認証の有効化

ユーザー データおよびネットワーク データを LDAP (Lightweight Directory Access Protocol) ディレクトリを使用して管理している場合、Symantec Product Authentication Service の認証ブローカに LDAP 認証プラグインを使用してユーザー認証を実行することができます。

メモ: LDAP プラグインは主に UNIX ユーザーを対象にしています。Windows の Active Directory では検証されていません。

LDAP プラグインを有効化する基本的な手順

LDAP プラグインを有効にする基本的な手順は次のとおりです。

1. Symantec Product Authentication Service サーバーをシャットダウンします。
2. 次の場所に存在する VRTSatlocal.conf ファイルを特定します。
   - Windows の場合 : *<InstallDir>*/systemprofile
   - UNIX の場合 : /var/VRTSat/.VRTSat/profile
3. VRTSatlocal.conf ファイルの次の箇所を編集します。
   a. DomainInfos セクションを編集します。(2-27 ページの「DomainInfos セクションの編集」を参照。)
   b. ServerInfos セクションを編集します。(2-29 ページの「ServerInfos セクションの編集」を参照。)
4. Symantec Product Authentication Service サーバーを再起動します。マシンを再起動する必要はありません。

DomainInfos セクションの編集

LDAP サーバーは、1 つまたは複数のドメインを持つことができます。各ドメインには、1 つの User コンテナと 1 つの Group コンテナが含まれます。LDAP の各ドメインにアクセスするには、VRTSatLocal.conf ファイルに次のセクションが記入されている必要があります。

[Security¥Authentication¥Authentication Broker¥AtPlugins¥ldap¥**DomainInfos**¥ldap¥<Domain Name>]

VSS とは 1 つのドメインで、デフォルトではこのファイルに ....¥DomainInfos¥ldap¥VSS というセクションが含まれます。この VSS の部分は任意で編集できます。

アクセスされるすべての LDAP ドメインについて、このセクションを追加する必要があります。その各 DomainInfos セクションには、次の情報を記入する必要があります。3 つのフィールドは必須で、その他のフィールドは任意です。

すべての任意のフィールドには main セクション [Security¥Authentication¥Authentication Broker¥AtPlugins¥ldap] に設定されているデフォルト値があります。このデフォルト値を特定のドメインで無効にするには、そのドメインのセクションで新しい値を設定します。特定のドメインで設定した新しい値は、他のドメインの値には影響しません。

- (必須) 名前 : Server
  値 : ドメインを管理している LDAP ディレクトリ サーバーの名前または IP アドレス。この値は、LDAP サーバー セクション内の <Server Name> (後述) と同じである必要があります。
  説明 : たとえば "machinename.symantec.com" などです。
  "Server"="machinename.symantec.com"

- (必須) 名前 : GroupBaseDN
  値 : <Group コンテナのベース DN>
  説明 : ドメインの Group コンテナのベース DN です。
  "GroupBaseDN"="OU=group,dc=vss,dc=symantec,dc=com"

- (必須) 名前 : UserBaseDN
  値 : <User コンテナまたは People コンテナのベース DN>
  説明 : ドメインの User コンテナおよび People コンテナのベース DN です。
  "UserBaseDN"="OU=people,dc=vss,dc=symantec,dc=com"

- (任意) 名前 : GroupObjClass
  値 : <Group オブジェクト クラス名 >
  説明 : LDAP でのドメイン内の Group の保存方法を示す LDAP オブジェクト クラスの名前です。デフォルト値は "posixGroup" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。

- (任意) 名前 : UserObjClass
  値 : <User または People オブジェクト クラス名 >
  説明 : LDAP でのドメイン内の User または People の保存方法を示す LDAP オブジェクト クラスの名前です。デフォルト値は "posixAccount" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。

- (任意) 名前 : GroupAttr
  値 : <CN 属性名 >
  説明 : グループ名を格納するために使用する Group オブジェクト クラス内の属性の名前です。デフォルト値は "cn" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。

- (任意) 名前 : UserAttr
  値 : <UID 属性名 >
  説明 : 一意のユーザー識別子を格納するために使用する User オブジェクト クラス内の属性の名前です。デフォルト値は "uid" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。

- (任意) 名前 : GroupGIDAttr
  値 : <GroupObjClass の GID 属性名 >
  説明 : グループ ID を格納するために使用する Group オブジェクト クラス内の属性の名前です。デフォルト値は "gidNumber" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。
- (任意) 名前 : UserGIDAttr
  値 : <UserObjClass の GID 属性名 >
  説明 : ユーザーが属するグループのグループ ID を格納するために使用する User オブジェクト クラス内の属性の名前です。デフォルト値は "gidNumber" です。このデフォルト値を無効にした場合、新しい値はこの特定のドメインだけに影響します。

ServerInfos セクションの編集

LDAP サーバーは、1 つまたは複数のドメインを持つことができます。各ドメインには、1 つの User コンテナと 1 つの Group コンテナが含まれます。LDAP の各ドメインにアクセスするには、`VRTSatLocal.conf` ファイルに次のセクションが記入されている必要があります。

[Security¥Authentication¥Authentication Broker¥AtPlugins¥ldap¥ServerInfos¥<Server Name>]

このセクションには、次の情報を記入する必要があります。

- (必須) 名前 : URL
  値 : LDAP ディレクトリ サーバーの URL
  説明 : LDAP ディレクトリ サーバーの URL です。
  "URL"="ldap://SomeUser-solaris.symantec.com"
- (必須) 名前 : SSLEnabled
  値 : dword:00000000 または dword:00000001
  説明 : LDAP プラグインと LDAP サーバー間の通信で、値が dword:00000000 の場合は SSL が無効、dword:00000001 の場合は SSL が有効であることを意味します。この場合、LDAP プラグインでは、サーバー認証のみがサポートされます。
  "SSLEnabled"="dword:00000001"
- (必須) 名前 : TrustedCACertFile
  値 : 信頼できる CA 証明書の連鎖を含むファイル。これはプライバシー拡張メール (Privacy Enhanced Mail) のファイルで、X509 デジタル証明書を格納し PEM の拡張部分を含むファイル形式です。
  説明 : 信頼できる CA 証明書の連鎖 (PEM 形式) です。

GSS-API 認証プラグイン

Generic Security Service Application Program Interface (GSS-API) 認証プラグインは、必要最小限の構成で最大数の異なる GSS-API メカニズムをサポートします。すべての構成は認証ブローカで行われます。クライアント側での構成は必要ありません。

GSS-API の詳細については、RFC 2743 および RFC 2744 を参照してください。

GSS-API プラグインの構成

GSS-API プラグインのセクションは VRTSatlocal.conf に追加されます。gssapi メイン セクションでは、サービス名 (ServiceName) を構成したり、製品クレデンシャル (ExportGSSName) にエクスポートされたプリンシパル名を含めるかどうかを指定できます。

ServiceName は、GSS-API サーバーが提供するサービスの名前です。これは gss_init_sec_context() で使用されるターゲット名です。

ExportGSSName フラグが 0 (ゼロ) 以外の値に設定されている場合、認証ブローカは、エクスポートされたプリンシパル名を製品クレデンシャルに含めます。vrtsAtGetExportedName() を使用して、エクスポートされたプリンシパル名を製品クレデンシャルから抽出できます。

一般的な GSS-API 構成セクションは次のとおりです。

```
[Security¥Authentication¥Authentication
Broker¥AtPlugins¥gssapi]
"PluginSharedLibFileName"="authgssapi.dll"
"IsEnabled"=dword:00000000
"ServiceName"="host"
"ExportGSSName"=dword:00000001
[Security¥Authentication¥Authentication
Broker¥AtPlugins¥gssapi¥CA]
"WebExpiryInterval"=dword:00007080
"ExpiryInterval"=dword:00015180
"UserExpiryInterval"=dword:00015180
"ServiceExpiryInterval"=dword:01e13380
[Security¥Authentication¥Authentication
Broker¥AtPlugins¥gssapi¥DomainInfos]
[Security¥Authentication¥Authentication
Broker¥AtPlugins¥gssapi¥DomainInfos¥gssapi]
```

他のプラグインと同様に、「CA」セクションも構成できます。

3

Symantec Product Authentication Service のインストール

インストールおよび構成については、『Symantec Product Authentication Service インストール ガイド』を参照してください。また、README.txt ファイルおよび製品のリリース ノートも参照してください。

4

管理コンソール

この章では、管理コンソールの概要、管理コンソールへのアクセス方法、および管理コンソールでの様々な管理作業の実行方法について説明します。

内容は次のとおりです。

管理コンソールの実行の準備

注意: インストールした Symantec Product Authentication Service のビルド固有の最新情報については README を参照してください。

管理コンソールは、個別にインストールできません。標準インストール処理の一部としてインストールされます。

バイナリの位置

Windows プラットフォームの場合

- 認証サービス: すべてのバイナリ ファイルおよびスクリプト ファイルは、<*authentication install directory*>¥bin に格納されています。

Solaris プラットフォームの場合

- 認証サービス
  - `libAtWrapper.so`、`AtWrapper.jar`、`vssatgui.jar`、`VxHelpViewer.jar` および `VxHelpViewer110n.jar` は、

<authentication install directory>/lib に格納されています。

- runvssatgui.sh は、<authentication install directory>/bin に格納されています。

前提条件

管理コンソールを実行するには、次の前提条件を満たしている必要があります。

- AIX の場合、ご使用のシステムに Java 1.3.x がインストールされており、PATH 環境変数で、そのディレクトリを定義している必要があります。
- AIX 以外のシステムの場合、ご使用のシステムに Java 1.4.2 以上がインストールされており、PATH 環境変数で、そのディレクトリを定義している必要があります。JDK/JRE は、それぞれ次のサイトからダウンロードしてください。
  - SUN、Linux、Windows の場合 : Java の Web サイト
  - HP-UX の場合 : Hewlett Packard 社の Web サイト

依存関係

管理コンソールは、3 つのモードのいずれかで実行できます。

認証 + 認可モード

完全な認証 + 認可モードで管理コンソールを実行する場合、Symantec Product Authentication Service および Symantec Product Authorization Service の両方をインストールする必要があります。コンソールでは Authorization がシステムにインストールされているかどうかが認識され、それに応じて画面および機能がアクティブまたは非アクティブで表示されます。

認証専用モード

認証専用モードでコンソールを実行する場合、Symantec Product Authentication Service のみをインストールする必要があります。

クライアント専用モード (クレデンシャル管理専用)

管理コンソールの「クレデンシャル」領域のみを表示および使用する場合、認証クライアントのみをインストールする必要があります。

コンソールのセキュリティの理解

管理コンソールは、2 つの部分で構成されます。この 2 つの部分は、次の 2 つの個別のモードです。

- 認証専用
- 認証 + 認可

認可クライアントをインストールすると、コンソールの認可部分を使用できます。

すべてのユーザーが管理コンソールで作業できる状態は適切でないため、特定のセキュリティ対策が設定されています。

認証コンソールのセキュリティ

Symantec Product Authentication Service を管理するには、認証サービスが実際にインストールされているマシンにログインし、そのマシンから管理作業を実行する必要があります。つまり、現在のリリースでは認証サービスをリモート管理できません。さらに、ブローカを管理するには、Windows の場合は管理者 (Administrator)、UNIX の場合は root ユーザーとしてログインする必要があります。

認可コンソールのセキュリティ

『Symantec Product Authorization Service 管理者ガイド』を参照してください。

管理コンソールの起動

Symantec Product Authentication Service の管理には、CLI または管理コンソールを使用できます。

コンソールを使用する方法

1. Windows の場合は管理権限、UNIX の場合は root ユーザーとして、認証サービスが実際にインストールされているマシンにログインします。
   そのマシンから管理作業を実行します。現在のリリースでは認証サービスをリモート管理できません。
2. 次の手順で管理コンソールを起動します。
   - Windows の場合
     - 必要に応じて、PATH を変更します。認証サービスの場合は *<authentication install directory>*¥bin ディレクトリ、認可サービスの場合は *<authorization install*

directory>¥bin ディレクトリ (インストールされている場合) を指すようにします。

- 管理コンソールの実行は、次のいずれかの方法によって行うことができます。
  「スタート」メニューからプログラムを選択します。
  <*authentication install directory*>¥bin ディレクトリの runvssatgui.bat を実行します。

- UNIX の場合
  - 必要に応じて、PATH を変更します。認証サービスの場合は <*authentication install directory*>/bin ディレクトリ、認可サービスの場合は <*authorization install directory*>/bin ディレクトリ (インストールされている場合) を指すようにします。
  - <authentication install directory>/bin/runvssatgui.sh を実行します。

3 コンソールの起動後、認可サービスが信頼するブローカとの信頼関係を設定します。

メモ : これは 1 回限りの作業で、管理コンソールを使用するたびに設定する必要はありません。

---

a クイック アクセス パネルから「クレデンシャル (Credentials)」を選択して、「信頼関係 (Trust Relationship)」タブを選択します。

b ツールバーの「信頼性の確立 (Establish Trust)」をクリックし、ダイアログボックスで必要な設定を行います。
- 「ブローカ (Broker)」: 認可サービスを保持するマシンの名前
- 「ポート (Port)」: 2821 (デフォルト)

c 「OK」をクリックします。
「ブローカとの信頼性を確立しました (Established trust with broker)」というメッセージが表示されます。

認証時にトラブルが発生した場合

エラー メッセージが表示された場合、次のことを確認します。

- サービスが実行されていること。
- 認証ブローカとの信頼関係が設定されていること。
- ローカルの管理者としてログインしていること。
- UNIX プラットフォームの場合、ドメイン名が入力されていること。UNIX の場合、このフィールドの入力は必須です。

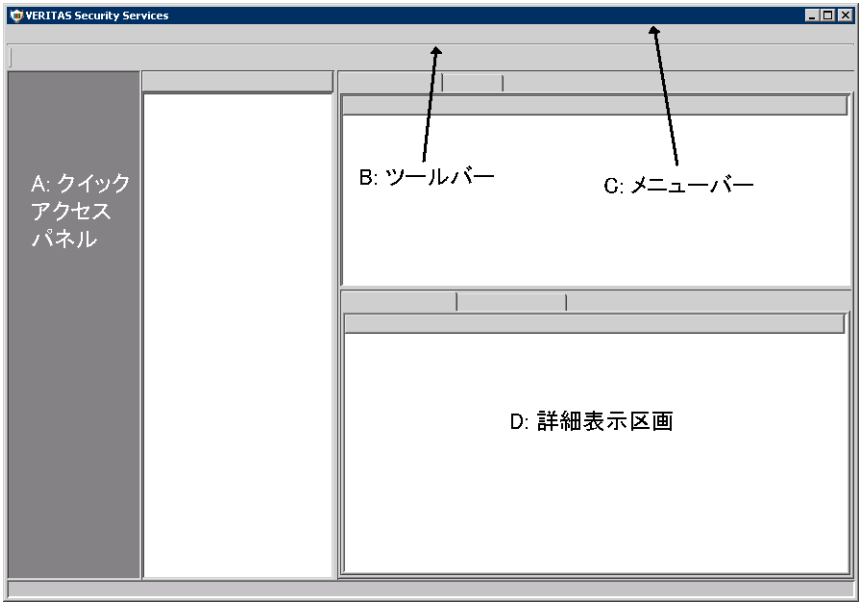
管理コンソールの外観

Symantec アプリケーション クライアントは、Symantec アプリケーション サービスがインストールされているホストから管理コンソールを取得します。したがって、管理コンソールの外観は、ホストにインストールされているコンポーネントによって異なります。

- クライアントのみがインストールされている場合、コンソールでクライアントが使用できるのは、クレデンシャルの管理に使用される部分だけです。
- 認証サービスがインストールされていて、認可サービスがインストールされていない場合、すべての認証機能は使用可能ですが、認可サービスの画面および機能は非アクティブになります。
- 認証サービスと認可サービスの両方がインストールされている場合、すべての機能が使用可能になります。
- また、使用しているリソース管理アプリケーションによっても外観が異なります。

通常、コンソールの画面は次のような画面です。右側のウィンドウの表示区画の数が異なるように、右側のタブ画面の数も異なります。

図 4-1 管理コンソール



管理コンソールの主な領域は次のとおりです。

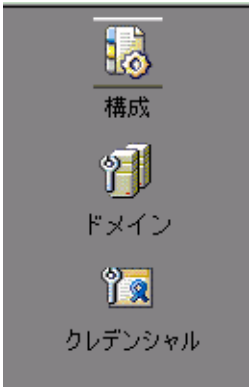
- クイック アクセス パネル (A): 異なるカテゴリの操作用ボタンが表示される領域です。クイック アクセス パネルで別のオプションを選択すると、別のタブ画面およびウィンドウが表示され操作できます。
- ツールバー (B): ツールバーのボタンをマウスでクリックすると、コンソールでよく使用される操作を簡単に実行できます。
- メニューバー (C): コンソールから実行できる様々な操作のポップアップ メニューにアクセスできます。
- 詳細表示区画 (D): クイック アクセス パネルで選択した操作に対応した情報および機能が表示されます。

クイック アクセス パネル

クイック アクセス パネルには、認証専用モード または認証 + 認可モード で作業しているかによって、異なったオプションが表示されます。

認証専用モードでは、クイック アクセス パネルは次のように表示されます。

図 4-2　　認証専用モードのクイック アクセス パネル



クイック アクセス パネルでオプションを選択すると、適切なタブ画面およびウィンドウが表示され操作できます。

ツールバー

ツールバーを使用すると、ボタンをクリックして様々な機能を実行できます。これらのボタンは、クイック アクセス パネルでの選択によって異なります。

メニューバー

メニューバーを使用すると、管理コンソールから実行できる様々な操作のポップアップ メニューにアクセスできます。無効なメニューはグレー表示されます。

詳細表示区画

詳細表示区画には、クイック アクセス パネルで選択した操作に対応した情報および機能が表示されます。詳細表示区画は、1 つ以上のタブ画面と 1 つ以上の画面で構成されます。

管理コンソールの使用

この項では、管理コンソールの使用例を示します。

実行可能な機能

Symantec Product Authentication Service をインストールした後、インストールについての特定の基本情報を確認することができます。たとえば、次のことができます。

- プライベート ドメイン リポジトリの位置の表示
- 既存のブローカの表示
- 既存のクレデンシャルの表示
- ドメイン情報の表示
  - プライベート ドメインの表示
  - 特定のプライベート ドメインについての情報の表示
  - プライベート ドメインの既存のプリンシパルの表示
  - 特定のプリンシパルについての情報の表示
  - プラグインをサポートしているドメインの一覧表示
  - プラグインの有効期間の間隔および使用可能なドメインの表示

プライベート ドメイン リポジトリの位置の表示

認証プライベート ドメイン リポジトリ (PDR) は、1 つ以上の認証プライベート ドメインのストアです。このリポジトリは認証ブローカによってロードされ、これに対してプリンシパルが照合され、検証されます。

プライベート ドメイン リポジトリの位置を表示する方法

1 クイック アクセス パネルで「構成 (Configure)」を選択します。

2 「認証ブローカ (Authentication Broker)」タブまたは「ルート ブローカ (Root Broker)」タブを選択します。

対応する CLI

vssat showpdr

既存のブローカの表示

既存のブローカを表示する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ドメイン ブローカのマッピング (Domain-Broker Mapping)」タブを選択します。

対応する CLI
vssat showbrokers

セキュリティ レベルの使用

セキュリティ管理者は、ルート証明書の配布に関して、次のいずれかのセキュリティ レベルを設定できます。

- 高セキュリティ (2): これまで信頼できなかったルートがピアから取得された場合 (同じ署名のある証明書が信頼できるストア内に存在しない場合) に、ユーザーはハッシュの検証を求められます。

メモ : ルート ハッシュとはルート ブローカのクレデンシャルの公開鍵で、バイナリ ファイルの形式でルート ブローカを一意に識別します。ルート ハッシュは信頼関係を確立するために使用されます。ルート ハッシュは UNIX の場合は `/opt/VRTSat/bin` 、Windows の場合は `<InstallDir>¥Authentication¥bin` にあります。

- 中セキュリティ (1): 最初の認証ブローカが信頼され、プロンプトは表示されません。後続の認証ブローカとの信頼関係の確立が試行されると、証明書が信頼できるストアに追加される前に、ユーザーはハッシュの検証を求められます。
- 低セキュリティ (0): 認証ブローカ証明書は常に信頼され、プロンプトは表示されません。

セキュリティ レベルの表示 (CLI のみ)

現在、管理コンソールからこの機能を実行することはできません。

セキュリティ レベルを表示するための基本的な CLI コマンドは次のとおりです。

vssat showsecuritylevel

セキュリティ レベルが低 (0)、中 (1) 、高 (2) のいずれであるかが表示されます。

セキュリティ レベルの設定

現在、管理コンソールでは、新しい信頼関係を確立した場合だけセキュリティ レベルを設定できます。

新しい信頼関係のセキュリティ レベルを設定する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「信頼関係 (Trust Relationship)」タブを選択します。

3 「認証 (Authentication)」メニューから「信頼関係 (Trust Relationship)」> 「信頼性の確立 (Establish Trust)」を選択します。

4 ダイアログボックスに必要な情報を入力し、「OK」をクリックします。

- 「ブローカ (Broker)」: ルート証明書をダウンロードするために接続するブローカを指定します。これには、ルート ブローカまたは認証ブローカのいずれかを指定できます。
  - ルート ブローカ : 自己署名されているルート証明書がダウンロードされます。ルート ブローカが別のルート証明書を信頼している (たとえば、信頼できるストアに別のルート証明書が存在する) 場合、それらもダウンロードされます。
  - 認証ブローカ: ツリー内のルート証明書 (認証ブローカ証明書に署名したルート証明書) がダウンロードされます。認証ブローカが別のルート証明書を信頼している (たとえば、信頼できるストアに別のルート証明書が存在する) 場合、それらもダウンロードされます。
- 「ポート番号 (Port Number)」: 接続するブローカのポート。
- 「セキュリティ タイプ (Security Type)」: このダイアログボックスでは、セキュリティ レベルに低 (Low)、中 (Medium) または高 (High) を選択できます。
  - 低 : ダウンロードされたルート証明書が、検証なしでローカルの信頼できるストアに追加されます。
  - 高 : ダウンロードされたルート証明書が、ハッシュの検証後にローカルの信頼できるストアに追加されます。ハッシュのリストは、root_trust_handlinginfo の形式で指定できます。ハッシュを入力しない場合、セキュリティ レベル高で信頼関係の確立を試行すると失敗します。複数のルート証明書がダウンロードされる場合、それぞれに対してハッシュの検証が必要です。

    セキュリティ レベル高で信頼関係の確立を試行し、一致するハッシュが検出されない場合、ルート証明書に対するハンドルは root_credential 出力パラメータに戻されます。アプリケーションでは、手動によるハッシュの比較または前述のようなエラー発生時の証明書情報の表示を行うオプションの提供を選択できます。
  - 中 : 最初の信頼関係の確立の試行は、セキュリティ レベル低で実行されます。それに続くすべての信頼関係の確立はセキュリティ レベル高で実行されます。
- 「信頼性のタイプ (Trust Type)」: 「信頼性のタイプ (Trust Type)」で「通常の信頼性 (Normal Trust)」を選択し、「セキュリティ タイプ (Security Type)」で「高 (High)」または「中 (Medium)」を選択する場合、管理コンソールはハッシュとともに証明書の詳細を表示します。そ

のブローカを信頼するかどうかが尋ねられます。「はい (Yes)」と答えると、そのブローカのルート証明書が追加されます。

対応する CLI
vssat setsecuritylevel

クレデンシャルの使用

製品クレデンシャルは、有効な識別情報として認識されるために必要な資格です。製品クレデンシャルには、プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された (1) プリンシパルの秘密鍵と (2) 特殊な拡張定義を含む X.509v3 証明書が必要です。製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作し、Symantec Product Authentication Service を使用するすべての Symantec アプリケーションに対してシングル サインオン機能を提供します。

クレデンシャルを使用して、次の作業を実行できます。

- クレデンシャルの格納場所の表示
- クレデンシャルを格納するディレクトリの設定
- 信頼関係の参照
- 既存のクレデンシャルの表示
- 証明書の要求
- クレデンシャルの削除
- 信頼情報の格納場所の表示
- 信頼関係の確立
- 信頼関係の削除

クレデンシャルの格納場所の表示

クレデンシャルが格納されているディレクトリを表示する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「全般 (General)」タブを選択します。

対応する CLI
vssat showcredstore

クレデンシャルを格納するディレクトリの設定

クレデンシャルを格納するディレクトリを設定する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「全般 (General)」タブを選択します。

3 「編集 (Edit)」をクリックして、選択するディレクトリを表示し選択して、「選択 (Choose)」をクリックします。

対応する CLI
vssat setcredstore

既存のクレデンシャルの表示

既存のクレデンシャルを表示する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「個別情報 (Personal)」タブを選択します。

3 クレデンシャルを表示するプリンシパルを選択し、ダブルクリックするか「証明書の表示 (View Certificate)」をクリックします。

メモ:「信頼関係 (Trust Relationship)」タブから証明書を参照することもできます。

対応する CLI
vssat showcred

証明書の要求

ローカル ストアに追加する証明書を要求する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ライフ サイクル管理 (Life Cycle Management)」タブを選択します。

3 フィールドに必要な情報を入力し、「提出 (Submit)」をクリックします。ユーザー名にスペースが含まれる場合は、その名前をクォーテーション マークで囲んでください。

対応する CLI
vssat authenticate

クレデンシャルの削除

ローカル ストアからクレデンシャルを削除する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ライフ サイクル管理 (Life Cycle Management)」タブを選択し、「クレデンシャルの抹消 (Destroy Credentials)」領域を展開します。

3 プリンシパル名、ドメイン名およびドメイン タイプを指定します。

4 クレデンシャルを発行したブローカを指定します。

5 「今すぐ削除 (Delete Now)」をクリックします。

対応する CLI
vssat deletecred

信頼関係の設定

信頼関係を設定する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「信頼関係 (Trust Relationship)」タブを選択します。

3 「認証 (Authentication)」メニューから「信頼関係 (Trust Relationship)」>「信頼性の確立 (Establish Trust)」を選択します。

4 ブローカの名前とポート番号を指定します。

5 この信頼関係で使用するセキュリティ レベルを指定します。

対応する CLI
vssat setuptrust

信頼関係の削除

信頼関係を削除する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「信頼関係 (Trust Relationship)」タブを選択します。

3 削除する信頼関係を選択します。

4 「認証 (Authentication)」メニューから「信頼関係 (Trust Relationship)」>「信頼性の削除 (Remove Trust)」を選択します。

5 「OK」をクリックして、削除を確定します。

対応する CLI
vssat removetrust

ドメイン ブローカのマッピングの使用

ドメイン ブローカのマッピングでは、認証を試行する際に、各ドメインで利用すべき認証ブローカを示す情報の集まりを提供します。

ドメイン ブローカのマップは、マシン上のすべてのユーザーまたは特定のユーザーによって共有できるように設定できます。認証サービスを使用するマシン上のすべてのユーザーに対してドメイン ブローカのマッピングを作成する必要がある場合、グローバル スコープを使用してマッピングを作成します。これは、セキュリティ対応の管理者がマシン上のすべてのユーザーに対してマップを作成する場合に便利です。グローバル マップは、ログイン ユーザー専用のローカル マップより優先させることができます。

ドメイン ブローカのマッピングを使用して、次の作業を実行できます。

- 既存のブローカのマッピングの参照
- ブローカのマッピングの追加
- ブローカのマッピングの削除

ドメイン ブローカのマッピングの表示

ドメイン ブローカのマッピングを表示する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ドメイン ブローカのマッピング (Domain-Broker Mapping)」タブを選択します。

リストに、特定形式の特定ドメインのプリンシパルが認証の際に利用するブローカが表示されます。スコープは、「ローカル (Local)」または「グローバル (Global)」のいずれかで表示されます。「ローカル (Local)」は現在のユーザーだけに関連し、「グローバル (Global)」はシステム全体に関連することを意味します。

対応する CLI
vssat showallbrokerdomains

ドメイン ブローカのマッピングの追加

ドメイン ブローカのマッピングを追加する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ドメイン ブローカのマッピング (Domain-Broker Mapping)」タブを選択します。

3 「認証 (Authentication)」メニューから「ドメイン ブローカのマッピング (Domain-Broker Mapping)」>「マッピングの追加 (Add Mapping)」を選択します。

4 ダイアログボックスで、認証の際に利用するブローカ (ドメインがマップされるブローカ) を指定します。

5 このブローカを使用するドメインの名前および形式を指定します。

6 このマッピングをローカル ユーザーだけに追加するか、グローバル レジストリに追加するかを指定します。
グローバル スコープは、セキュリティ対応の管理者が特定のマシン上のすべてのユーザーに対してマップを作成する場合に便利です。グローバル マップは、ログイン ユーザー専用のローカル マップより優先させることができます。

7 ダイアログボックスで必要な設定を行ったら、「追加 (Add)」をクリックします。

対応する CLI
vssat addbrokerdomain

ドメイン ブローカのマッピングの削除

ドメイン ブローカのマッピングを削除する方法

1 クイック アクセス パネルで「クレデンシャル (Credentials)」を選択します。

2 「ドメイン ブローカのマッピング (Domain-Broker Mapping)」タブを選択します。

3 削除するマッピングを選択します。

4 「認証 (Authentication)」メニューから「ドメイン ブローカのマッピング (Domain-Broker Mapping)」>「マッピングの削除 (Delete Mapping)」を選択します。

5 「OK」をクリックして、削除を確定します。

対応する CLI
vssat deletebrokerdomain

プライベート ドメインの使用

プライベート ドメイン (認証プライベート ドメインとも呼ばれる) は、Symantec 社製品に固有で、Symantec 社製品 (他のドメインに既存の識別情報を再利用しない) によって管理される認証プリンシパルに対する識別情報およびパスワードのハッシュを保持するための特殊な認証ドメインです。認証プライベート ドメインは、Symantec 社のポイント製品 (SANPoint Control、Volume Manager など) の識別情報を保持するために使用できます。

プライベート ドメインを使用して、次の作業を実行できます。

- プライベート ドメインの表示
- プライベート ドメインの作成または削除
- 特定のプライベート ドメインについての情報の表示
- 特定のプライベート ドメインの属性の設定
- ドメインへのプリンシパルの追加または削除
- プライベート ドメイン内のプリンシパルについての情報の更新

プライベート ドメインの表示

プライベート ドメインのリストを表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

プライベート ドメインが表示され、その各ドメインのデフォルトの有効期限ポリシーと、ユーザーとサービスの有効期限ポリシーが表示されます。

対応する CLI

vssat listpd

プライベート ドメインの作成

プライベート ドメインを作成する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 「認証 (Authentication)」メニューから「ドメイン (Domains)」>「ドメインの作成 (Create Domain)」を選択します。

4 新しいドメイン名および有効期間の間隔を入力し、「ドメインの作成 (Create domain)」をクリックします。

対応する CLI
vssat createpd

特定のプライベート ドメインについての情報の表示

特定のプライベート ドメインについての情報を表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 情報を表示するドメインを選択します。

上表示区画に、有効期限ポリシーについての情報が表示されます。下表示区画には、選択したドメインのプリンシパルが表示されます。

対応する CLI
ドメインおよび有効期限を表示する方法

vssat showpd

ドメインのプリンシパルについての情報を表示する方法

vssat listpdprincipals

プライベート ドメインの属性の設定
現在、設定可能な属性は有効期限だけです。

プライベート ドメインの属性を設定する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。
プライベート ドメインが表示され、その各ドメインのデフォルトの有効期限ポリシーと、ユーザーとサービスの有効期限ポリシーが表示されます。

3 有効期間の間隔を変更するドメインを選択します。

4 「認証 (Authentication)」メニューから「ドメイン (Domains)」>「ドメインの更新 (Update Domain)」を選択します。

5 新しい有効期間の間隔 (秒単位) を入力し、「ドメインの更新 (Update Domain)」をクリックします。

特定のプライベート ドメインの特定の属性を設定するための基本的な CLI コマンドは次のとおりです。

vssat setpdr

プライベート ドメインの削除

特定のプライベート ドメインを削除する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 削除するドメインを選択します。

4 「認証 (Authentication)」メニューから「ドメイン (Domains)」>「ドメインの削除 (Delete Domain)」を選択します。

5 「OK」をクリックして、削除を確定します。

対応する CLI
vssat deletepd

プライベート ドメインの既存のプリンシパルの表示

既存のプリンシパルのリストを表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 ドメインを選択します。

下表示区画に、選択したドメインのプリンシパルについての情報が表示されます。

対応する CLI
vssat listpdprincipals

プライベート ドメインへのプリンシパルの追加

プライベート ドメインにプリンシパルを追加する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 プリンシパルを追加するドメインを選択します。

4 「認証 (Authentication)」メニューから「プリンシパル (Principal)」>「プリンシパルの追加 (Add Principal)」を選択します。

5 新しいプリンシパルの名前およびパスワードを指定します。

6 「プリンシパル タイプ (Principal Type)」フィールドで、使用する有効期間の間隔として、ユーザーに対して確立されたもの、サービスに対して確立されたものまたはデフォルトのいずれかを指定します。

7 このプリンシパルを別のプリンシパルのプロキシとして機能させる場合、「プロキシ可 (Can Proxy)」を選択します。
これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。

8 このプリンシパルがプロキシを受け入れるようにする場合、「プロキシ承認 (Can Accept Proxy)」を選択します。
これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。

9 「プリンシパルの追加 (Add Principal)」をクリックします。

対応する CLI
vssat addprpl

特定のプリンシパルについての情報の表示

特定の既存のプリンシパルについての情報を表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 プリンシパルが存在するドメインを選択します。

下表示区画に、プリンシパルについての情報が表示されます。

対応する CLI
vssat showprpl

プライベート ドメインのプリンシパルの更新

プライベート ドメインのプリンシパルを更新する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 プリンシパルが存在するドメインからプリンシパルを選択します。

4 更新するプリンシパルを選択します。

5 「認証 (Authentication)」メニューから「プリンシパル (Principal)」>「プリンシパルの更新 (Update Principal)」を選択します。

6 必要に応じて、「プリンシパル タイプ (Principal Type)」を変更します。これには、使用する有効期間の間隔として、ユーザーに対して確立されたもの、

サービスに対して確立されたものまたはデフォルトのいずれかを指定します。

7 このプリンシパルを別のプリンシパルのプロキシとして機能させる場合、「プロキシ可 (Can Proxy)」を選択します。
これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。

8 このプリンシパルがプロキシを受け入れるようにする場合、「プロキシ承認 (Can Accept Proxy)」を選択します。
これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。

9 「保存 (Save)」をクリックします。

対応する CLI
vssat updateprpl

プリンシパルのパスワードの変更

プリンシパルのパスワードを変更する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 プリンシパルが存在するドメインを選択します。

4 パスワードを変更するプリンシパルを選択します。

5 「認証 (Authentication)」メニューから「プリンシパル (Principal)」>「パスワードの変更 (Change Password)」を選択します。

6 古いパスワードを入力します。

7 新しいパスワードを入力および再入力し、「パスワードの変更 (Change Password)」をクリックします。

対応する CLI
vssat changepasswd

プリンシパルの削除

プライベート ドメインからプリンシパルを削除する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プライベート ドメイン (Private Domains)」タブを選択します。

3 プリンシパルを削除するドメインを選択します。

4 削除するプリンシパルを選択します。

5 「認証 (Authentication)」メニューから「プリンシパル (Principal)」>「プリンシパルの削除 (Delete Principal)」を選択します。

6 「はい (Yes)」をクリックして、削除を確定します。

プリンシパルの削除後に実行する必要のある手順

プリンシパルを削除する場合、プリンシパルの削除に加えて、次の手順のいずれかを実行することをお勧めします。

- 権限を拒否するプリンシパルに含まれるすべての ACL を削除する。
- または、プリンシパルを「Disabled Principals」リストに追加する。

たとえばあるユーザーが一時的に不在となり、その期間にその識別情報を他の目的で使用されたくない場合は、そのプリンシパルを「Disabled Principals」リストに入れておく方がよいと考えるかもしれません。ユーザーが戻ってきた時にこのプリンシパルを「Disabled Principals」リストから削除すれば、すべての権限を簡単に復活させることができます。

ユーザーが会社を辞めた場合は、このプリンシパルを含むすべての ACL を削除するのも効果的です。

対応する CLI

vssat deleteprpl

プラグインの使用

認証プラグインは、認証ブローカによって、特定のドメイン内で識別情報を検証するために使用されるコンポーネントです。認証プラグインは、サポートされている認証メカニズムごとに存在します。たとえば、あるプラグインで NIS の識別情報とパスワードの組合せの検証を NIS データベースに対して行うことが可能な一方で、別のプラグインではプリンシパルの認証を行う際に Kerberos ticket を利用できます。

プラグインを使用して、次の作業を実行できます。

- プラグインをサポートしているドメインの一覧表示
- プラグインの既存の有効期間の表示
- プラグインの基本情報の表示

メモ: プラグイン関連で重要な作業の 1 つは、Symantec Product Authentication Service 用の LDAP プラグインを有効にすることです。この作業は、GUI から行うことはできません。2-27 ページの「LDAP プラグインを有効化する基本的な手順」を参照してください。この特別なプラグインの詳細については、付録 B「LDAP プラグインの詳細情報」を参照してください。

プラグインをサポートしているドメインの表示

プラグインをサポートしているドメインのリストを表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プラグイン (Plugins)」タブを選択します。

対応する CLI
vssat showdomains

プラグインの有効期間の間隔および使用可能なドメインの表示

特定のプラグインの有効期間の間隔および使用可能なドメインを表示する方法

1 クイック アクセス パネルで「ドメイン (Domains)」を選択します。

2 「プラグイン (Plugins)」タブを選択します。

3 プラグインを選択します。

デフォルトの有効期間、ユーザーの有効期間およびサービスの有効期間が上表示区画に表示され、プラグインを使用可能なドメインが下表示区画に表示されます。

対応する CLI
vssat showexpiryintervals

プリンシパルの使用

認証プリンシパルは、ユーザー、コンピュータ、コマンドライン インタフェース (CLI) などのプロセス、またはサービスの中で、一意の識別情報によって Symantec Product Authentication Service が認証を行うことができるものです。

各プリンシパルはドメインのメンバーである必要があるため、プリンシパルに関連する作業はドメインに関連する作業の一部です。したがって、詳細については、4-16 ページの「プライベート ドメインの使用」を参照してください。

プリンシパルを使用して、次の作業を実行できます。

- プライベート ドメインの既存のプリンシパルの表示

- プライベート ドメインへのプリンシパルの追加
- 特定のプリンシパルについての情報の表示
- プライベート ドメインのプリンシパルの更新
- プリンシパルのパスワードの変更
- プリンシパルの削除

コンソール オブジェクト (Symantec Product Authentication Service)

ここでは、Symantec Product Authentication Service の一連の管理コンソール オブジェクトについて説明します。

「構成」領域

構成の多くは、インストール時に決定されます。クイック アクセス パネルで「構成 (Configure)」オプションを選択すると、これらの多数のオプションを参照でき、一部を変更することもできます。

「構成 (Configure)」領域には、構成に応じて、次の一部またはすべてのタブ画面が表示されます。

- 「認証ブローカ (Authentication Broker)」
- 「ルート ブローカ (Root Broker)」
- 「認可サービス (Authorization Service)」

「認証ブローカ」タブ

この画面を使用すると、認証ブローカがインストールされているマシンの識別情報および認証プライベート ドメイン リポジトリの位置を参照できます。

認証ブローカ

認証ブローカは、ルート ブローカよりレベル (層) が 1 つ下の中間登録局および認証局として機能するコンポーネントです。認証ブローカは、クライアント (ユーザー、サービスなど) の認証を行い、製品クレデンシャルの一部となる証明書を付与することができます。ただし、認証ブローカは他のブローカを認証することはできません。他のブローカの認証は、ルート ブローカで実行する必要があります。

認証プライベート ドメイン

認証プライベート ドメインは、Symantec 社製品に固有で、Symantec 社製品 (他のドメインに既存の識別情報を再利用しない) によって管理される認証プリンシパルに対する識別情報およびパスワードのハッシュを保持するための特殊な認証ドメインです。認証プライベート ドメインは、Symantec 社のポイント製品 (SANPoint Control、Volume Manager など) の識別情報を保持するために使用できます。

認証プライベート ドメイン リポジトリ

認証プライベート ドメイン リポジトリは、1 つ以上の認証プライベート ドメインのストアです。このリポジトリは認証ブローカによってロードされ、これに対してプリンシパルが照合され、検証されます。

「ルート ブローカ」タブ

ルート ブローカは、最も信頼できる、最上位にある認証ブローカで、自己署名した証明書を持っています。ルート ブローカは、有効と判断されるブローカの名前だけを保持する 1 つのプライベート ドメインを持ちます。ルート ブローカ自身の名前は、完全修飾されたドメイン名 (FQDN) としてそのプライベート ドメインに格納されます。

ルート ブローカの構成作業はインストール時に行われます。ルート ブローカがインストールされているホストでは、「ルート ブローカ (Root Broker)」タブ画面を使用して、ルート ブローカがインストールされているマシンの識別情報およびルートのプライベート ドメイン リポジトリの位置を参照できます。

「ハッシュ (Hash)」フィールドには、ルート証明書の暗号化されたハッシュ (または公開鍵) が表示されます。このハッシュは、ルート証明書を検証するために信頼関係を設定する際に使用できます。このハッシュは秘密ではなく、ルート証明書の検証を補助するために、ハッシュを簡単にダウンロードまたは配布可能な信頼できる内部インフラストラクチャ (イントラネットやディレクトリなど) で公開可能です。

メモ : 管理コンソールからハッシュを変更することはできません。

「ドメイン」領域

認証ドメインは、認証プリンシパルに対して一連の識別情報を定義します。また、グループ メンバーシップなど、プリンシパルに関連する認可情報を提供します。たとえば、NIS+、NTML、Active Directory ドメイン内の名前などです。

認証ドメインには、公開されるものもあります。特別な形式の認証ドメインとして、Symantec 社製品に独自の認証プライベート ドメインがあります。

クイック アクセス パネルから「ドメイン (Domains)」オプションを選択すると、次のタブ画面を使用できるようになります。

- 「プライベート ドメイン (Private Domain)」
- 「プラグイン (Plugins)」

「プライベート ドメイン」タブ

この画面を使用すると、次の管理作業を実行できます。

- プライベート ドメインに属するプリンシパルの詳細の参照
- プライベート ドメインの作成または削除
- プライベート ドメインのプリンシパルの作成または削除
- パスワードの再設定

上表示区画でプライベート ドメインを選択すると、下表示区画にプリンシパルの詳細が表示されます。

ドメインを作成、削除または更新するには、「認証 (Authentication)」メニューから「ドメイン (Domains)」を選択し、必要なオプションを設定します。

ドメインのプリンシパルの追加、削除、更新またはパスワードの変更を行うには、「認証 (Authentication)」メニューから「プリンシパル (Principals)」を選択し、必要なオプションを設定します。

プライベート ドメインの特徴

認証プライベート ドメインは、Symantec 社製品に固有で、Symantec 社製品 (他のドメインに既存の識別情報を再利用しない) によって管理される認証プリンシパルに対する識別情報およびパスワードのハッシュを保持するための特殊なドメインです。

ルート ブローカは、有効と判断されるブローカの名前だけを保持する 1 つのプライベート ドメインを持ちます。ルート ブローカ自身の名前は、完全修飾されたドメイン名 (FQDN) としてそのプライベート ドメインに格納されます。

他の認証ブローカは、プライベート ドメインを持たないか、1 つ以上持っていて、そのメンバーの形式は、ユーザー、サービス、コマンドライン インタ

フェースと様々です。ただし、これらの形式はプライベート ドメインでは区別されません。

認証プライベート ドメインは、Symantec 社のポイント製品 (SANPoint Control、Volume Manager など) の識別情報を保持するために使用できます。

「ドメインの作成」ダイアログボックス

このダイアログボックスを使用すると、ブローカに認証プライベート ドメインを追加できます。ドメイン名を指定し、有効期間 (秒単位) を入力します。その後、「ドメインの作成 (Create Domain)」をクリックします。

認証プライベート ドメインは、Symantec 社製品に固有で、Symantec 社製品 (他のドメインに既存の識別情報を再利用しない) によって管理される認証プリンシパルに対する識別情報およびパスワードのハッシュを保持するための特殊なドメインです。

ルート ブローカは、有効と判断されるブローカの名前 (ルート ブローカ自身の名前を含む) だけを保持する 1 つのプライベート ドメインを持ちます。そのため、ルート ブローカにドメインを追加できません。

他の認証ブローカは、プライベート ドメインを持たないか、1 つ以上持っていて、そのメンバーの形式は、ユーザー、サービス、コマンドライン インタフェースと様々です。ただし、これらの形式はプライベート ドメインでは区別されません。

認証プライベート ドメインは、Symantec 社のポイント製品 (SANPoint Control、Volume Manager など) の識別情報を保持するために使用できます。

「ドメインの削除」ダイアログボックス

このダイアログボックスで「はい (Yes)」をクリックすると、選択されている項目の削除を確定できます。

「ドメインの更新」ダイアログボックス

このダイアログボックスを使用すると、ドメインの有効期間の間隔を変更できます。

有効期間の間隔は秒数で指定します。0 (ゼロ) は、有効期限ポリシーの次のレベルが使用されることを意味します。たとえば、ドメインの有効期限ポリシーが使用されます。ドメインの有効期限ポリシーも 0 (ゼロ) の場合は、プラグイン全体の有効期限ポリシーが使用されます。プラグイン全体の有効期限ポリシーも 0 (ゼロ) の場合は、ソフトウェアによってデフォルトが指定されます。

「プリンシパルの追加」ダイアログボックス

このダイアログボックスを使用すると、選択した認証プライベート ドメインにプリンシパルを追加できます。

プリンシパルを追加する方法

1. プリンシパルを追加するドメインが選択されていることを確認します。選択されていない場合は、「キャンセル (Cancel)」をクリックし、正しいドメインを選択します。
2. 新しいプリンシパルの名前およびパスワードを指定します。
3. 「プリンシパル タイプ (Principal Type)」フィールドで、使用する有効期間の間隔として、ユーザーに対して確立されたもの、サービスに対して確立されたものまたはデフォルトのいずれかを指定します。
4. このプリンシパルを別のプリンシパルのプロキシとして機能させる場合、「プロキシ可 (Can Proxy)」を選択します。
   これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。
5. このプリンシパルがプロキシを受け入れるようにする場合、「プロキシ承認 (Can Accept Proxy)」を選択します。
   これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。
6. 「プリンシパルの追加 (Add Principal)」をクリックします。

「プリンシパルの削除」ダイアログボックス

このダイアログボックスで「はい (Yes)」をクリックすると、選択されている項目の削除を確定できます。

「パスワードの変更」ダイアログボックス

このダイアログボックスを使用すると、選択されているプリンシパルのパスワードを変更できます。

パスワードを再設定する方法

1. 古いパスワードを入力します。
2. 新しいパスワードを入力します。
3. 新しいパスワードを再入力して確定します。
4. 「パスワードの変更 (Change Password)」をクリックします。

「プリンシパルの更新」ダイアログボックス

このダイアログボックスを使用すると、プリンシパルの情報を変更できます。

有効期限ポリシーは、ユーザー、サービスまたはデフォルト値に対して設定できます。設定の対象は、ドロップダウン メニューから選択します。

有効期間の間隔は秒数で指定します。0 (ゼロ) は、有効期限ポリシーの次のレベルが使用されることを意味します。たとえば、ドメインの有効期限ポリシーが使用されます。ドメインの有効期限ポリシーも 0 (ゼロ) の場合は、プラグイン全体の有効期限ポリシーが使用されます。プラグイン全体の有効期限ポリシーも 0 (ゼロ) の場合は、ソフトウェアによってデフォルトが指定されます。

「プロキシ可 (Can Proxy)」を選択すると、このプリンシパルは別のプリンシパルのプロキシとして機能できるようになります。これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。

「プロキシ承認 (Can Accept Proxy)」を選択した場合、このプリンシパルはプロキシを受け入れることができるようになります。これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。

「プラグイン」タブ

認証メカニズムは、ドメインで定義された名前空間内のユーザーに対して認証を行う方法です。認証メカニズムは、認証アルゴリズムのすべての細目 (API、プロトコル、トークン形式、トークン コンテンツの構文、データベース オブジェクト形式など) をカプセル化します。関連する構成要素は、メカニズムごとに異なります。

サポートされている各認証メカニズムには、プラグインがあります。プラグインとは、認証ブローカによって、特定のドメイン内で識別情報を検証するために使用されるコンポーネントです。たとえば、あるプラグインで NIS の識別情報とパスワードの組合せの検証を NIS データベースに対して行うことが可能な一方で、別のプラグインではプリンシパルの認証を行う際に Kerberos ticket を利用できます。

「プラグイン (Plugins)」タブ画面を使用すると、既存のプラグインの詳細を参照、または有効期限ポリシーを指定できます。

認証サービスでは、ご使用の個々の OS に対してサポートされているすべてのプラグインがインストールされます。今回のリリースの Symantec Product Authentication Service では、プラグインの追加および削除はできません。

有効期間の間隔

プラグインでは、有効期限ポリシーはプリンシパルごとではなくプラグインごとに設定します。有効期限ポリシーは、ブローカ (ルート ブローカまたは認証ブローカ) に対して、ブローカが生成したクレデンシャルに設定する必要がある有効期間の長さを指示します。

ポリシーは、ユーザー、サービスまたはデフォルト値に対して設定できます。ドロップダウン メニューから有効期間の間隔を選択するか、「ユーザー定義 (User Defined)」を選択して有効期間の間隔 (時間単位、日単位または月単位) を設定します。

認証されたプリンシパルがサービス (または CLI) の場合、サービス プリンシパルの有効期間の間隔が適用されます。認証されたプリンシパルがユーザーの場合、ユーザー プリンシパルの有効期間の間隔が適用されます。プリンシパルがサービスかユーザーかを判断できない場合は、デフォルトの有効期間の間隔が使用されます。

「有効期間の間隔」ダイアログボックス

このダイアログボックスを使用すると、選択したプラグインの有効期間の間隔を変更できます。

プラグインごとに設定される有効期限ポリシーは、ブローカに対して、ブローカが生成したクレデンシャルに設定する必要がある有効期間の長さを指示します。

ユーザー、サービスまたはデフォルト値のいずれをポリシーに設定するかを指定し、有効期間 (秒単位) を指定します。その後、「有効期限の変更 (Change Expiry)」をクリックします。

「クレデンシャル」領域

クイック アクセス パネルから「クレデンシャル (Credentials)」オプションを選択すると、クレデンシャル マネージャを管理できるようになります。

クレデンシャル マネージャの定義

クレデンシャル マネージャは、認証の際に取得したクレデンシャルを管理するコンポーネントです。取得されたクレデンシャルは、ローカルのクレデンシャル ストアにキャッシュされます。

ヒント：アプリケーション サービスまたはクライアントが認証ブローカに一度認証されると、その後の動作がブローカの状態に左右されることはありません。ブローカが稼動していない場合でも動作することができます。

「クレデンシャル」領域で使用可能なタブ

「クレデンシャル」領域では、次のタブ画面が使用できます。

- 「全般 (General)」
- 「信頼関係 (Trust Relationship)」
- 「ライフ サイクル管理 (Life Cycle Management)」
- 「ドメイン ブローカのマッピング (Domain-Broker Mapping)」
- 「個別情報 (Personal)」

メモ:「識別名」、「ドメイン名」、「ドメイン タイプ」および「パスワード」からなるユーザー情報が指定された場合、内部的には API サブルーチンがクレデンシャルを取得するため、クレデンシャル マネージャがこの問題を処理します。この API を使用すると、クレデンシャル マネージャがドメイン情報に基づいて、利用するブローカを検出します。

「クレデンシャル」:「全般」タブ

製品クレデンシャル (管理コンソールでは単にクレデンシャルと呼ばれる) は、有効な識別情報として認識されるために必要な資格です。製品クレデンシャルには、次の 2 つが必要です。

- プリンシパルの秘密鍵
- プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された特殊な拡張定義を含む X.509v3 証明書

製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作し、Symantec Product Authentication Service を使用するすべての Symantec アプリケーションに対してシングル サインオン機能を提供します。

「全般 (General)」タブを使用すると、ルートのクレデンシャルの格納場所を参照できます。

「クレデンシャル」:「信頼関係」タブ

認証局は、所有者の識別情報を保証する証明書の発行、管理および取消しを行う信頼できるサード パーティです。プリンシパルが正当な利用者であることを示す証明書は、認証局の各階層で署名されます。

- ルート ブローカのルート認証局は、階層の最上位に位置するエンティティで、そのため最も信頼できる認証局です。ルート自身を証明する証明書は自己署名されており、ルート証明書と呼ばれます。

- 信頼階層の次のレベルには、認証ブローカが存在します。認証ブローカは、セキュリティ プリンシパルを認証し、認証ブローカによって署名された証明書を生成します。つまり、認証ブローカは中間の認証局として機能し、事実上、ルート ブローカと認証ブローカは相互に信頼しているといえます。

「信頼関係 (Trust Relationship)」タブ画面を使用すると、確立されている信頼関係の情報を参照できます。

- 「発行先ユーザー (Issued To User)」領域には、信頼できるエンティティが `user[domaintype:domainname]` の形式で表示されます。たとえば、次のとおりです。

  ```
  broker[vx:root@something.something.com]
  ```

- 「発行元ブローカ (Issued By Broker)」領域には、発行したエンティティの名前が、信頼できるエンティティと同じ形式で表示されます。
- 「有効期限 (Expiration Date)」領域には、証明書の有効期限が表示されます。

「証明書の表示」ダイアログボックス

このダイアログボックスを使用すると、選択した証明書の詳細を参照できます。

製品クレデンシャル (管理コンソールでは単にクレデンシャルと呼ばれる) は、有効な識別情報として認識されるために必要な資格です。製品クレデンシャルには、次の 2 つが必要です。

- プリンシパルの秘密鍵
- プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された特殊な拡張定義を含む X.509v3 証明書

製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作し、Symantec Product Authentication Service を使用するすべての Symantec アプリケーションに対してシングル サインオン機能を提供します。

「信頼性の確立」ダイアログボックス

認証局は、所有者の識別情報を保証する証明書の発行、管理および取消しを行う信頼できるサード パーティです。プリンシパルが正当な利用者であることを示す証明書は、認証局の各階層で署名されます。

ルート ブローカのルート認証局は、階層の最上位に位置するエンティティで、そのため最も信頼できる認証局です。ルート自身を証明する証明書は自己署名されており、ルート証明書と呼ばれます。信頼階層の次のレベルには、認証ブローカが存在します。認証ブローカは、セキュリティ プリンシパルを認証し、認証ブローカによって署名された証明書を生成します。つまり、認証ブローカは中間の認証局として機能し、事実上、ルート ブローカと認証ブローカは相互に信頼しているといえます。

「ブローカ (Broker)」: ルート証明書をダウンロードするために接続するブローカを指定します。これには、ルート ブローカまたは認証ブローカのいずれかを指定できます。

- ルート ブローカ : 自己署名されているルート証明書がダウンロードされます。ルート ブローカが別のルート証明書を信頼している (たとえば、信頼できるストアに別のルート証明書が存在する) 場合、それらもダウンロードされます。
- 認証ブローカ: ツリー内のルート証明書 (認証ブローカ証明書に署名したルート証明書) がダウンロードされます。認証ブローカが別のルート証明書を信頼している (たとえば、信頼できるストアに別のルート証明書が存在する) 場合、それらもダウンロードされます。

「ポート番号 (Port Number)」: 接続するブローカのポート。

「セキュリティ タイプ (Security Type)」: このダイアログボックスでは、セキュリティ レベルに低 (Low)、中 (Medium) または高 (High) を選択できます。

- 低 : ダウンロードされたルート証明書が、検証なしでローカルの信頼できるストアに追加されます。
- 中 : 最初の信頼関係の確立の試行は、セキュリティ レベル低で実行されます。それに続くすべての信頼関係の確立はセキュリティ レベル高で実行されます。
- 高 : ダウンロードされたルート証明書が、ハッシュの検証後にローカルの信頼できるストアに追加されます。ハッシュのリストは、root_trust_handlinginfo の形式で指定できます。ハッシュを入力しない場合、セキュリティ レベル高で信頼関係の確立を試行すると失敗します。複数のルート証明書がダウンロードされる場合、それぞれに対してハッシュの検証が必要です。

  セキュリティ レベル高で信頼関係の確立を試行し、一致するハッシュが検出されない場合、ルート証明書に対するハンドルは root_credential 出力パラメータに戻されます。アプリケーションでは、手動によるハッシュの比較または前述のようなエラー発生時の証明書情報の表示を行うオプションの提供を選択できます。

「信頼性のタイプ (Trust Type)」:「信頼性のタイプ (Trust Type)」で「通常の信頼性 (Normal Trust)」を選択し、「セキュリティ タイプ (Security Type)」で「高 (High)」または「中 (Medium)」を選択する場合、管理コンソールはハッシュとともに証明書の詳細を表示します。そのブローカを信頼するかどうかが尋ねられます。「はい (Yes)」と答えると、そのブローカのルート証明書が追加されます。

「信頼性の削除」ダイアログボックス

このダイアログボックスで「はい (Yes)」をクリックすると、選択されている項目の削除を確定できます。

「クレデンシャル」:「ライフ サイクル管理」タブ

製品クレデンシャル (管理コンソールでは単にクレデンシャルと呼ばれる) は、有効な識別情報として認識されるために必要な資格です。製品クレデンシャルには、次の 2 つが必要です。

- プリンシパルの秘密鍵
- プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された特殊な拡張定義を含む X.509v3 証明書

製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作し、Symantec Product Authentication Service を使用するすべての Symantec アプリケーションに対してシングル サインオン機能を提供します。

製品クレデンシャルのライフ サイクルには、次の 3 つの段階があります。

- 使用開始 : クレデンシャルがストアに追加されます。
- 使用中 : クレデンシャルが使用されます。
- 使用終了 : クレデンシャルの有効期限が切れるか、抹消されています。

このタブ画面で、「手動によるクレデンシャルの要求 (Manual Request For Credential)」または「クレデンシャルの抹消 (Destroy Credentials)」を展開すると、新しいクレデンシャルを要求、または既存のクレデンシャルを抹消できます。

クレデンシャルの要求

「手動によるクレデンシャルの要求 (Manual Request For Credential)」領域を展開します。必要な情報を入力し、「提出 (Submit)」をクリックします。

- 「名前 (Name)」: クレデンシャルが要求されているユーザーの名前。ユーザーを指定しない場合は、現在ログインしているユーザーの名前になります。ユーザー名にスペースが含まれる場合は、その名前をクォーテーションマークで囲んでください。
- 「パスワード (Password)」: クレデンシャルが要求されているプリンシパルのパスワード。指定しない場合は、現在ログインしているユーザーのパスワードが使用されます。
- 「ドメイン名 (Domain Name)」: クレデンシャルが要求されているプリンシパルのドメイン名 (オプション)。
- 「ドメイン タイプ (Domain Type)」: クレデンシャルが要求されているプリンシパルのドメイン タイプ。
- 証明書を発行する必要があるブローカを選択する場合は、「ブローカ (Broker)」をクリックし、ダイアログボックスで必要な設定を行います。

クレデンシャルの抹消

「クレデンシャルの抹消 (Destroy Credentials)」領域を展開します。必要な情報を入力し、「今すぐ削除 (Delete Now)」をクリックします。

- 「名前 (Name)」: クレデンシャルが抹消されるユーザーの名前。ユーザーを指定しない場合は、現在ログインしているユーザーの名前になります。
- 「ドメイン名 (Domain Name)」: クレデンシャルが抹消されるプリンシパルのドメイン名 (オプション)。
- 「ドメイン タイプ (Domain Type)」: クレデンシャルが抹消されるプリンシパルのドメイン タイプ。
- 「発行元ブローカ (Issued By Broker)」: 抹消する証明書を発行したブローカ。

期限切れのクレデンシャルを抹消するには、「期限切れクレデンシャルの抹消 (Destroy Expired Credentials)」領域をクリックし、「今すぐ削除 (Delete Now)」をクリックします。

「ブローカの選択」ダイアログボックス

このダイアログボックスを使用すると、クレデンシャルを要求するブローカの名前およびポート番号を指定できます。

「クレデンシャル」:「ドメイン ブローカのマッピング」タブ

セキュリティ管理者は、クライアントが認証を受けるために問い合わせる認証ブローカをドメインごとに選択できます。次に例を示します。

- nis+ クライアントである場合は、認証ブローカ A を使用
- unixpwd クライアントである場合は、認証ブローカ B を使用

ドメイン ブローカのマッピングは、認証を試行する際に、各ドメインで利用すべき認証ブローカを示す情報の集まりです。

ドメイン ブローカのマッピングの情報は、グローバル構成またはローカル構成のいずれかに格納されます。認証サービスを使用するマシン上のすべてのユーザーに対してドメイン ブローカのマッピングを作成する必要がある場合、グローバル スコープを使用してマッピングを作成します。これは、セキュリティ対応の管理者がマシン上のすべてのユーザーに対してマップを作成する場合に便利です。グローバル マップは、ログイン ユーザー専用のローカル マップより優先させることができます。

認証ブローカがドメインに接続する必要がある場合は、最初にローカル エントリが検索され、次にグローバル エントリが検索されます。

「マッピングの追加」ダイアログボックス

このダイアログボックスを使用すると、別のマッピング (認証を試行する際に利用すべき認証ブローカを示す情報の集まり) を作成できます。情報は、グローバル構成またはローカル構成のいずれかに格納されます。

認証ブローカがドメインに接続する必要がある場合は、最初にローカル エントリが検索され、次にグローバル エントリが検索されます。

「マッピングの削除」ダイアログボックス

このダイアログボックスで「はい (Yes)」をクリックすると、選択されている項目の削除を確定できます。

「クレデンシャル」:「個別情報」タブ

このタブ画面を使用すると、クレデンシャルを参照することができます。

- 「発行先ユーザー (Issued To User)」領域には、信頼できるエンティティが `user[domaintype:domainname]` の形式で表示されます。たとえば、次のとおりです。

  ```
  broker[vx:root@something.something.com]
  ```

- 「発行元ブローカ (Issued By Broker)」領域には、発行したエンティティの名前が、信頼できるエンティティと同じ形式で表示されます。
- 「有効期限 (Expiration Date)」領域には、証明書の有効期限が表示されます。

5

コマンドライン インタフェース

Symantec Product Authentication Service は、様々な管理作業を実行するためのコマンドライン インタフェース (CLI) を提供します。

内容は次のとおりです。

CLI の目的

コマンドライン インタフェースを使用すると、グラフィカル ユーザー インタフェース (GUI) を使用せずに、コマンドを入力して作業を実行できます。機能の多くはどちらのインタフェースからでも実行できますが、どちらか一方のインタフェースに固有のものもあります。

CLI の管理機能

CLI の管理機能には、次の 2 つの種類があります。

- ブローカの管理 : vxatd (詳細については、5-3 ページの「vxatd の使用」を参照。)
- 認証サービスの管理 (詳細については、5-7 ページの「vssat の使用」を参照。)

CLI へのアクセス

認証サービスの CLI (コマンドライン インタフェース) にアクセスする方法

1. 認証サービスをインストールします。
2. (デフォルトの位置にインストールした場合、) 次のディレクトリに移動します。

   Windows の場合 : `C:¥Program Files¥VERITAS¥Security¥Authentication¥bin`

   UNIX の場合 : `/opt/VRTSat/bin`

コマンドの使用方法

コマンドライン インタフェース (CLI) で使用される表記規則を次に示します。例として、`vssat` コマンドを使用します。

略語の説明

すべてのコマンドで、略語 AT は Authentication を、略語 AZ は Authorization を示します。

引数を持たないコマンド

引数が必要でない場合があります。これは、通常、グローバルな情報を示し、フィルタリングするための修飾語句を必要としないオプションの場合です。

```
vssat commandoption
```

任意選択または必須の引数を持つコマンド

任意選択の引数の場合、引数は大括弧 ([ ]) で囲みます。次に例を示します。

```
vssat commandoption [--optionalargument <data>]
```

必須の引数の場合、次の構文を使用します。

```
vssat commandoption --mandatoryargument <data>
```

相互排他的な引数を持つコマンド

2 つの引数が相互排他的な場合、引数はバー (|) で区切ります。次に例を示します。

```
vssat commandoption --mutuallyexclusiveargument
          <choice1|choice2|choice3|>
```

相互排他的な引数がそれぞれ異なるデータを必要とする場合、次の構文を使用します。

```
vssaz commandoption --mandatoryargument
          {Choice1,<Data1>|Choice2,<Data2a>,<Data2b>|Cho
          ice3,<Data3a>,<Data3b>|Choice4,<Data4>}
```

vxatd の使用

様々な引数を指定して vxatd コマンドを使用すると、次のいずれかのモードでブローカを管理できます。

- Root モード
- Root + AB (認証ブローカ) モード
- AB (認証ブローカ) モード

ブローカを構成するには、次の説明に従って vxatd コマンドを実行します。

ブローカを起動するための構文

vxatd のオプションはトークンとして入力され、各オプションに関連する情報を指定できます。vxatd を初めて実行する場合は、次の構文を使用します。

Root モードでの起動

Root モードで起動するには、次の構文を使用します。

```
vxatd -r [-d]
```

AB モードでの起動

AB モードで起動するには、次の構文を使用します。

```
vxatd -a -n <broker identity> -p <password> -x <domain
type> -y <domain name> -q <root broker name> -z <root
broker port> -h <hash file name>
```

Root + AB モードでの起動

Root + AB モードで起動するには、次の構文を使用します。

```
vxatd -a -r
```

最初の起動以降は、コマンドによってレジストリから適切な構成が読み込まれ、既存の鍵ペアと証明書が選択されます。そのため、最初の起動以降は、必須の引数はありません。

共通のオプション

`-r`

ブローカを Root モードで起動します。これがシステムに配置される最初のブローカになります。

ルート鍵マテリアルが生成されます。自己署名した証明書が生成されます。ルート プライベート ドメイン リポジトリが初期化されます。ハッシュ ファイルが生成されます。ブローカが起動されます (-a オプションと -r オプションを組み合わせて指定すると、ブローカが Root + AB モードで起動されます)。

`-a`

認証ブローカをルートで認証して起動します。認証ブローカ鍵マテリアルが生成されます。

認証要求がルートに送信されます。認証が成功すると、認証ブローカのクレデンシャルがストアにインストールされます。認証ブローカのプライベート ドメイン リポジトリが初期化されます。ブローカは、指定されたポート上での待機を開始します。

前提条件 : 認証ブローカの認証プリンシパルの識別情報が、ルート ブローカのプライベート ドメインに追加されている必要があります。また、ルートへのネットワーク接続が可能である必要があります。

`-a -r`

ブローカを Root + AB モードで起動します。

ルート鍵マテリアルが生成されます。自己署名した証明書が生成されます。ルート プライベート ドメイン リポジトリが初期化されます。ハッシュ ファイルが生成されます。認証ブローカ鍵マテリアルが生成され

ます。ルートによって署名された認証ブローカのクレデンシャルが生成されます。認証ブローカのプライベート ドメイン リポジトリが初期化されます。ブローカは、指定されたポート上での待機を開始します。

`-d`

ブローカをデバッグ モードで起動します。

AB Only モードでの認証ブローカの起動における追加の引数

次の引数は、ルート ブローカではなく認証ブローカを初めて起動する際に必須です。

`-h <hash file name>`

ハッシュ ファイル名。このオプションを指定すると、認証ブローカの認証プロセスが強制的にセキュリティ レベル高で実行されます。ファイルのハッシュが、ダウンロードされた証明書のハッシュと一致する場合にだけ、ルート証明書がローカル ストアに追加されます。AB Only モードで構成する場合、ルート ハッシュ ファイルの引数は必須です。

前提条件 : ハッシュ ファイルをルートから認証ブローカにコピーする必要があります。

AB Only モードでインストールされた認証ブローカは、セキュリティ レベル高だけで起動できます。ブローカをインストールする際に信頼関係を確立するフェーズで、ダウンロードされたルート証明書がファイル内のハッシュと比較されます。一致しない場合、ブローカ サービスは停止します。

ルート ハッシュ ファイルがルート ブローカ ホスト上で生成されます。`vxatd` を `-h` 引数を指定して使用する前に、ルートから認証ブローカに手動でこのファイルをコピーする必要があります。

`-n <broker identity>`

ルート プライベート ドメインで構成されているブローカの識別情報。

`-o`

ブローカの、鍵およびクレデンシャルの生成モード。鍵およびクレデンシャルは、適切なディレクトリ構造で生成および格納されます。ブローカの起動状態 (AB、Root、Root + AB) が格納されます。ブローカは、このフラグを指定しないで起動された場合にだけ、要求の待機および受入れを開始します。ストア内の鍵は、ユーザー コンテキストで保護されます。これにより、ファイル システムのセキュリティを越えた、ハッカーに対するもう 1 つのレベルのセキュリティ (プログラム形式の作業) が提供されます。現在は、この保護はマシンに依存しません。

`-p <password>`

ルート プライベート ドメインで構成されているブローカのパスワード。

`-q <root broker name>`

ルート ブローカ名、ホスト名または IP。

-x <*domain type*>
認証ブローカの識別情報のドメイン タイプ。これは、vx (プライベート ドメイン) です。
-y <*domain name*>
認証ブローカの識別情報のドメイン名。これは、認証ブローカの識別情報が構成されているルート プライベート ドメイン名です。
-z <*root broker port*>
ルート ブローカ ポート。

Windows 固有の引数

-u
サービス マネージャからプログラムを削除します。
-k
サービスを停止します。
-t
既存のサービスの起動方法を設定します。

- 新しいクレデンシャルを要求して、指定されたドメインでブローカを作成します。
- ブローカ モードおよびレジストリ内の識別情報をリセットします。

例

例 1
たとえば、マシン A 上で vxatd を起動している場合に子ノード上で vxatd を起動する構文は、vxatd -r -a です。次の操作を実行して vxatd をマシン B 上で起動して、マシン B がマシン A の信頼できる子ノードになるようにします。
マシン A 上で Root + AB を所有すると想定します。

次の手順を実行して、マシン B 上で認証ブローカを起動します。

1 ルート (マシン A) のプライベート ドメイン内に、マシン B 上の認証ブローカ用の認証プリンシパルを追加します。

2 vxatd を、次のように実行します。
vxatd -a -n <*broker identity*> -p <*password*> -x <*domain type*> -y <*domain name*> -q <*root broker name*> -z <*root broker port*> -h <*root hash file name if working in high security level*>

メモ : -h を指定しない場合、セキュリティ モード低でインストールされるため認証は行われません。

例 2

Root + AB をドメイン root@somename.mycompany.com にマイグレートするには (プライベート ドメインが vx の場合)、次の構文を使用します。

```
vxatd -j -n brokeridentity -p password -x vx -y
root@somename.mycompany.com -h hashfile -qdurga -z2821
```

この結果、認証ブローカが root@somename.mycompany.com ドメインに作成されます。

vssat の使用

コマンドライン インタフェース (CLI) で使用する表記規則は、次のとおりです。

任意選択の引数は大括弧 ([ ]) で囲みます。引数に、一連の値の中からいずれか 1 つだけを指定する必要がある場合、データの選択肢はパイプ (|) で区切ります。コマンドの引数が相互排他的な場合、引数は中括弧 ({ }) で囲みます。

```
vssat SampleOption --Arg <data> --ArgWithChoiceOfData
<DataChoice1|DataChoice2|DataChoice3>
{ArgChoice1,<data>|ArgChoice2,<data1>,<data2>| ArgChoice3,
<data1>,<data2>} [--OptionalArg <data>]
```

addbrokerdomain

名前

addbrokerdomain

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat addbrokerdomain --broker <host:port> --domain
<type:name> [--global]
```

説明

このコマンドを実行すると、ブローカへのドメインのマッピングを追加できます。このマッピングにより、特定のドメインへの認証を試行する際に利用すべきブローカが示されます。追加先のブローカが起動していて、ping が正常に実行できる必要があります。認証プリンシパルを削除した場合、次のいずれか (または両方) の手順を実行して不正なアクセスを回避します。

- 識別情報を「Disabled Principals」リストに追加する。
- この識別情報に関連付けられている ACL を削除し、この識別情報が属するグループからこの識別情報のメンバーシップを削除する。

引数

このコマンドには、次の引数を使用できます。

`--broker <host:port>`
: ブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

`--domain <type:name>`
: ブローカの名前を構成する必要があるドメインのドメイン情報。

`--global`
: エントリをグローバル レジストリに追加する必要があることを示します。指定しない場合、エントリはローカル レジストリに追加されます。ローカル レジストリの設定は、現在ログオンしている OS プリンシパルにだけ影響します。これに対して、グローバル レジストリの設定は、ホストのすべての OS プリンシパルに適用されます。

例

このコマンドは、次のように使用します。

```
vssat addbrokerdomain --broker MyHost:2821 --domain
nt:NewBrokerDomain
```

addprpl

名前

addprpl

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat addprpl --pdrtype <root|ab|cluster> --domain <name>
--prplname <prpl name> [--password <password>] [--
credexpiry <expiry period (sec)>] [--prpltype
<default|user|service>] [--can_proxy] [--can_accept_proxy]
[--is_broker_admin] [--is_domain_admin] [--broker
<host:port> --domain_admin_prplname <domain admin
identity> [--domain_admin_domain <type:name>]]
```

説明

このコマンドを実行すると、ドメイン内に認証プリンシパルを作成できます。プリンシパルの作成中に、プリンシパル名、パスワード、形式などを入力する必要があります。

引数

このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: プリンシパルを作成するドメインの名前。

`--is_broker_admin`
: 作成するプリンシパルに対してブローカ管理者権限を付与します。

`--is_domain_admin`
: 作成するプリンシパルに対してドメイン管理者権限を付与します。

`--prplname <prpl name>`
: 作成するプリンシパルの名前。

`--password <password>`
: 新しいプリンシパルに対して使用するパスワード。

`--credexpiry <expiry period (sec)>`
: 有効期間の間隔 (秒数)。0 (ゼロ) は、有効期限ポリシーの次のレベルが使用されることを意味します。たとえば、ドメインの有効期限ポリシーが使用されます。ドメインの有効期限ポリシーも 0 (ゼロ) の場合は、プラグイン全体の有効期限ポリシーが使用されます。プラグイン全体の有効期限ポリシーも 0 (ゼロ) の場合は、ソフトウェアによってデフォルトが指定されます。

--prpltype <*default*|*user*|*service*>
作成するプリンシパルの形式。ユーザーまたはサービスを指定します。
--can_proxy
この引数を指定すると、このプリンシパルは別のプリンシパルのプロキシとして機能します。これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。
--can_accept_proxy
この引数を指定すると、エンティティに対してプロキシを受け入れる権限を付与します。これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの製品 Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。

次のパラメータは、リモート ブローカ上でプリンシパルを作成する場合にのみ必要です。リモート ブローカは、PBX がサポートされた状態で実行されている必要があります。呼出し元は、リモート ドメインのブローカ管理者の識別情報またはドメイン管理者の識別情報のいずれかを使用してリモート ブローカへの認証を行い、次のパラメータを使用してその情報を渡す必要があります。

--broker <host:port>
リモート ブローカ ホスト名およびポート番号。
--domain_admin_prplname <domain admin identity>
リモート ブローカ上のターゲット ドメインのブローカ管理者またはドメイン管理者であるプリンシパルの名前。
--domain_admin_domain <type:name>
リモート ドメイン管理者の識別情報のドメイン名およびドメイン タイプ。このパラメータを指定しない場合、管理者のプリンシパルは、新しいプリンシパルを作成するドメインと同じドメインに存在すると見なされます。

例 1

```
vssat addprpl --pdrtype ab --domain broker@MyHost --
prplname TomSawyer --password LetTomIn --expinterval 24000
--prpltype user
```

例 2

この操作をリモート ブローカ上で実行する場合、ユーザーは addprpl を呼び出す前に setuptrust および authenticate を実行する必要があります。

```
vssat setuptrust --broker root_broker.my_domain.com:2821 -
-securitylevel high --hashfile /tmp/root_hash

vssat authenticate --domain
vx:dom1@remote_broker.my_domain.com --broker
remote_broker.my_domain.com:1556 --prplname admin --
password secret
```

```
vssat addprpl --pdrtype ab --domain
dom1@remote_broker.my_domain.com --password my_pass --
prpltype service --is_broker_admin --is_domain_admin --
broker remote_broker.my_domain.com:1556 --
domain_admin_prplname admin --domain_admin_domain
vx:dom1@remote_broker.my_domain.com
```

authenticate

名前

authenticate

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat authenticate  --domain <type:name> [--prplname <prpl
name> [--password <password>]] [--broker <host:port>]
```

説明

このコマンドを実行すると、認証プリンシパルに対するクレデンシャルを認証ブローカから取得できます。ブローカ情報によって指定された認証ブローカによって、認証プリンシパル名、ドメイン、ドメイン タイプおよびパスワードを使用して識別情報が検証され、クレデンシャルが発行されます。

引数

このコマンドには、次の引数を使用できます。

--domain <*type:name*>
: プリンシパルを保持しているドメインの名前および形式。プライベート ドメイン名は、完全修飾された名前である必要はありません。指定したブローカ名に「@< 完全修飾されたブローカ名 >」が含まれない場合も受け入れられます。

--prplname <*prpl name*>
: 認証するプリンシパルの名前。この引数の指定は、nt ドメイン タイプを使用して SSPI を使用する場合は、任意です。同様に、localhost ドメイン タイプを使用する場合も任意です。その他のドメイン タイプの場合は、任意ではなく、必須です。

--password <*password*>
: 認証するプリンシパルのパスワード。この引数の指定は、nt ドメイン タイプを使用して SSPI を使用する場合は、任意です。同様に、localhost ドメイン タイプを使用する場合も任意です。その他のドメイン タイプの場合は、任意ではなく、必須です。

--broker <*host:port*>
: ブローカのホストおよびポート。ドメイン ブローカのマッピングがすでに存在する場合、ブローカ情報の指定は必須ではありません。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

例 1

```
vssat authenticate --domain vx:broker@MyHost --prplname
TomSawyer--password LetTomIn --broker MyHost:2821
```

例 2

```
vssat authenticate --domain vx:broker --prplname TomSawyer
--password LetTomIn --broker MyHost:2821
```

changepasswd

名前
changepasswd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat changepasswd --pdrtype <root|ab|cluster> --domain
<name> --prplname <prpl name> [--currentpasswd
<oldpasswd>] [--newpasswd <newpasswd>] [--
repeatednewpasswd <repnewpasswd>]
```

説明
このコマンドを実行すると、プリンシパルのパスワードを変更できます。パスワードは、コマンドラインで任意に指定できます。コマンドラインで指定しない場合、非 echo モードでプロンプトが表示されます。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
プライマリ ドメインの名前。

`--prplname <prpl name>`
パスワードを変更するプリンシパルの名前。

`--currentpasswd <oldpasswd>`
変更する古いパスワード。

`--newpasswd <newpasswd>`
設定する新しいパスワード。

`--repeatednewpasswd <repnewpasswd>`
確認のために再入力する新しいパスワード。

例
このコマンドは、次のように使用します。

```
vssat changepasswd --pdrtype ab --domain broker@MyHost --
prplname TomSawyer --currentpasswd LetTomIn --newpasswd
PleaseLetTomIn --repeatednewpasswd PleaseLetTomIn
```

createpd

名前

createpd

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat createpd --pdrtype <ab|cluster> --domain <name> [--
credexpiry <expiry period (sec)>] [--domain_admin_password
<domain admin password>] [--broker <host:port> --
broker_admin_prplname <broker admin identity> --
broker_admin_domain <type:name>]
```

説明

このコマンドを実行すると、このドメインのプリンシパルに対して発行された一意の名前およびその他の属性 (クレデンシャルの有効期限など) を使用して、リポジトリ内にプライベート ドメインを作成できます。

引数

このコマンドには、次の引数を使用できます。

--pdrtype <*ab*|*cluster*>
: プライベート ドメイン リポジトリの形式。認証ブローカまたはクラスタを指定します。ルート プライベート ドメイン リポジトリ内ではドメインを作成および削除することができないため、ルート ブローカはオプションに含まれません。ルート プライベート ドメイン リポジトリには、すべての認証ブローカの識別情報が格納されているドメインが 1 つだけ存在します。

--domain <*name*>
: 作成するドメインの名前。

--credexpiry <*expiry period (sec)*>
: 有効期限 (秒単位)。

--domain_admin_password
: 作成するドメインのドメイン管理者のパスワード。

次のパラメータは、リモート ブローカ上でプライベート ドメインを作成する場合にのみ必要です。リモート ブローカは、PBX がサポートされた状態で実行されている必要があります。呼出し元は、ブローカ管理者の識別情報を使用してリモート ブローカへの認証を行い、次のパラメータを使用してその情報を渡す必要があります。

--broker <*host:port*>
: リモート ブローカ ホスト名およびポート番号。

--broker_admin_prplname <*broker admin identity*>
: リモート ブローカ上でブローカ管理者であるプリンシパルの名前。

--broker_admin_domain <type:name>
リモート ブローカ管理者の識別情報のドメイン名およびドメイン タイプ。

例 1

```
vssat createpd --pdrtype ab --domain broker@MyHost --
credexpiry 24000
```

例 2

この操作をリモート ブローカ上で実行する場合、ユーザーは createpd を呼び出す前に setuptrust を実行する必要があります。

```
vssat authenticate --domain
vx:broker@remote_broker.my_domain.com --broker
remote_broker:1556 --prplname admin --password secret

vssat createpd --pdrtype ab --domain new_domain --
domain_admin_password secret --broker
remote_broker.my_domain.com:1556 --broker_admin_prplname
admin --broker_admin_domain
vx:broker@remote_broker.my_domain.com
```

deletebrokerdomain

名前
deletebrokerdomain

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat deletebrokerdomain --broker <host:port> --domain <
type:name> [--global]
```

説明
このコマンドを実行すると、ブローカへのドメインのマッピングを削除できます。このマッピングにより、特定のドメインへの認証を試行する際に利用すべきブローカが示されます。このエントリをローカル レジストリまたはグローバル レジストリのどちらから削除するかを指定するオプションがあります。

引数
このコマンドには、次の引数を使用できます。

`--broker <host:port>`
: ブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

`--domain <type:name>`
: 削除するドメインの名前。

`--global`
: エントリをグローバル レジストリから削除するように指定します。ローカル レジストリの設定は、現在ログオンしている OS プリンシパルにだけ影響します。これに対して、グローバル レジストリの設定は、ホストのすべての OS プリンシパルに適用されます。

例
MyHost:2821 への nt: NewBrokerDomain のマッピングをローカル レジストリから削除するには、次のように指定します。

```
vssat deletebrokerdomain --broker MyHost:2821 --domain
nt:NewBrokerDomain
```

グローバル構成から削除するには、次のように指定します。

```
vssat deletebrokerdomain --broker MyHost:2821 --domain
nt:NewBrokerDomain  --global
```

deletecred

名前
deletecred

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat deletecred --domain <type:name> [--prplname <prpl
name> [--broker <name:port>]]
```

説明
このコマンドを実行すると、名前やドメインなどのユーザー情報を指定して、ストアからクレデンシャルを削除できます。指定したユーザー情報に該当するクレデンシャルが削除されます。

引数
このコマンドには、次の引数を使用できます。

--domain <*type:name*>
: クレデンシャルを削除するプリンシパルを保持しているドメインの名前。

--prplname <*prpl name*>
: クレデンシャルを削除するプリンシパルの名前。

--broker <*name:port*>
: ブローカのホストおよびポート。ここでポートを指定しても、このコマンドの処理では無視されます。ブローカを指定すると、特定のブローカのクレデンシャルだけが削除されます。

  2 つの異なる認証ブローカの同じ認証プリンシパルに対して、2 つの異なるクレデンシャルが存在する場合があります。

例
このコマンドは、次のように使用します。

```
vssat deletecred --domain nt:NewDomainName --prplname
TomSawyer --broker MyHost:2821
```

deleteexpiredcreds

名前
deleteexpiredcreds

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat deleteexpiredcreds
```

説明
このコマンドを実行すると、ストアから期限切れのクレデンシャルを削除できます。

引数
なし

deletepd

名前
deletepd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat deletepd --pdrtype <ab|cluster> --domain <name>
```

説明
このコマンドを実行すると、認証プライベート ドメイン リポジトリからプライベート ドメインを削除できます。ドメインを削除すると、ドメイン自身とともにドメイン内のプリンシパルが削除されます。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <ab|cluster>`
: プライベート ドメイン リポジトリの形式。認証ブローカまたはクラスタを指定します。ルート プライベート ドメイン リポジトリ内ではドメインを作成および削除することができないため、ルート ブローカはオプションに含まれません。ルート プライベート ドメイン リポジトリには、すべての認証ブローカの識別情報が格納されているドメインが 1 つだけ存在します。

`--domain <name>`
: 削除するドメインの名前。

例
このコマンドは、次のように使用します。

```
vssat deletepd --pdrtype ab --domain nt:NewBrokerDomain
```

deleteprpl

名前

deleteprpl

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat deleteprpl --pdrtype <root|ab|cluster> --domain
<name> --prplname <prpl name>[--silent]
```

説明

このコマンドを実行すると、プライベート ドメインからプリンシパルを削除できます。プリンシパルおよびドメインが存在しない場合、このコマンドは失敗します。

引数

このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: プリンシパルが存在するドメインの名前。

`--prplname <prpl name>`
: 削除するプリンシパルの名前。

`--silent`
: 確認メッセージを表示しないようにします。

例

このコマンドは、次のように使用します。

```
vssat deleteprpl --pdrtype ab --domain broker@MyHost --
prplname TomSawyer
```

listpd

名前
listpd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat listpd --pdrtype <root|ab|cluster> [--broker
<host:port> --broker_admin_prplname <broker admin
identity> --broker_admin_domain <type:name>]
```

説明
このコマンドを実行すると、ローカル ブローカまたはリモート ブローカのプライベート ドメイン リポジトリ内のドメインを表示できます。リモート ブローカのドメインを表示するには、リモート ブローカのブローカ管理者の識別情報を使用して、リモート ブローカで認証する必要があります。

引数
このコマンドには、次の引数を使用できます。

--pdrtype <root|ab|cluster>
プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

次のパラメータは、リモート ブローカ上のプライベート ドメインを表示する場合にのみ必要ですリモート ブローカは、PBX がサポートされた状態で実行されている必要があります。呼出し元は、ブローカ管理者の識別情報を使用してリモート ブローカへの認証を行い、次のパラメータを使用してその情報を渡す必要があります。

--broker <host:port>
リモート ブローカ ホスト名およびポート番号。

--broker_admin_prplname <broker admin identity>
リモート ブローカ上でブローカ管理者であるプリンシパルの名前。

--broker_admin_domain <type:name>
リモート ブローカ管理者の識別情報のドメイン名およびドメイン タイプ。

例 1
```
vssat listpd --pdrtype ab
```

例 2
この操作をリモート ブローカ上で実行する場合、ユーザーは `listpd` を呼び出す前に `setuptrust` および `authenticate` を実行する必要があります。

```
vssat setuptrust --broker remote_broker.my_domain.com:1556
--securitylevelhigh
```

```
vssat authenticate --domain
vx:broker@remote_broker.my_domain.com --prplname
remote_broker_admin --password secret --broker
remote_broker.my_domain.com:1556

vssat listpd --pdrtype ab --broker
remote_broker.my_domain.com:1556 --broker_admin_prplname
remote_broker_admin --broker_admin_domain
vx:broker@remote_broker.my_domain.com
```

listpdprincipals

名前
listpdprincipals

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat listpdprincipals --pdrtype <root|ab|cluster> --
domain <name>
```

説明
このコマンドを実行すると、プライベート ドメイン内のすべてのプリンシパルを表示できます。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: 表示するプリンシパルのプライベート ドメインの名前。

例
このコマンドは、次のように使用します。

```
vssat listpdprincipals --pdrtype ab --domain broker@MyHost
```

removetrust

名前
removetrust

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat removetrust --broker <brokerinfo like host>
```

説明
このコマンドを実行すると、指定したブローカから発行されたルート証明書を削除できます。

引数
--broker
削除するルート証明書を発行したブローカの名前。

例
このコマンドは、次のように使用します。

```
vssat removetrust --broker MyHost
```

renewcredential

名前
renewcredential

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat renewcredential --domain <type:name> --prplname
<prpl name> --broker <host:port>
```

説明
このコマンドを実行すると、ドメインおよびブローカを指定して、特定のプリンシパルのクレデンシャルを更新できます。

引数
このコマンドには、次の引数を使用できます。

`--domain <type:name>`
: 更新するクレデンシャルを保持しているドメインの名前。

`--prplname <prpl name>`
: クレデンシャルを更新するプリンシパルの名前。

`--broker <host:port>`
: ブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

例
このコマンドは、次のように使用します。

```
vssat renewcredential --domain nt:NewBrokerDomain --
prplname JohnDoe --broker MyHost:2821
```

resetpasswd

名前
resetpasswd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat resetpasswd --pdrtype <root|ab|cluster> --domain
<name> --prplname <prpl name> [--newpasswd <newpasswd>] [-
-repeatednewpasswd <repnewpasswd>]
```

説明
認証プリンシパルがパスワードを忘れてしまった場合に、管理者がこのコマンドを使用してパスワードをリセットします。このコマンドでは、古いパスワードを入力する必要はありません。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: プライマリ ドメインの名前。

`--prplname <prpl name>`
: パスワードを変更するプリンシパルの名前。

`--newpasswd <newpasswd>`
: 設定する新しいパスワード。

`--repeatednewpasswd <repnewpasswd>`
: 確認のために再入力する新しいパスワード。

例
このコマンドは、次のように使用します。

```
vssat resetpasswd --pdrtype ab --domain broker@MyHost --
prplname TomSawyer --newpasswd PleaseLetTomIn --
repeatednewpasswd PleaseLetTomIn
```

setcredstore

名前
setcredstore

形式
このコマンドを実行する前に、認証ブローカを停止します。次の構文に従って入力してください (改行は不要)。

```
vssat setcredstore --storetype <file|memory|registry> --
storefile <file if file type> [--enableobfuscation]
```

説明
このコマンドを実行すると、クレデンシャル ストアの詳細情報を設定できます。詳細情報には、ストアの形式 (メモリー、ファイル、Windows のレジストリなど) が含まれます。ファイルの場合、ファイルの位置を指定および表示できます。

引数
このコマンドには、次の引数を使用できます。

`--storetype <file|memory|registry>`
詳細情報を指定するクレデンシャル ストアの形式についての情報。メモリー、ファイルまたはレジストリを指定します。

`--storefile <file if file type>`
ファイルが存在するパス。ストアの形式にファイルを指定した場合に指定します。

`--enableobfuscation`
難読化を有効にするように指定します。

例
このコマンドは、次のように使用します。

```
vssat setcredstore --storetype file --storefile
"C:¥Program Files¥VERITAS¥Security¥Authentication¥System
Profile¥Certstore"
```

注意事項
今回のリリースでは、指定可能なストアの形式はファイルだけです。

setexpiryintervals

名前

setexpiryintervals

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setexpiryintervals --pluginname <plugin name> --
prpltype <default,user,service,webcredential> --credexpiry
<expiry period>
```

説明

このコマンドを実行すると、クレデンシャルの有効期間の間隔を 3 つのレベル (一般、ユーザー プリンシパルおよびサービス (または CLI) プリンシパルの有効期限レベル) のいずれかに設定できます。これらの間隔は、プラグイン レベルで設定する必要があります。1 つ上のレベルに変更する場合 (たとえば、プリンシパルからドメイン、ドメインからプラグインに変更する場合)、変更前のレベルの有効期限を 0 (ゼロ) に設定する必要があります。たとえば、プリンシパルの有効期限が 1000 であると想定します。プリンシパルの有効期限を削除して、Authentication によってドメインの有効期限に基づいた証明書が発行されるようにするには、管理者は、プリンシパルの有効期限を 0 (ゼロ) に設定する必要があります。ドメインからプラグインに変更する場合も同様です。

引数

このコマンドには、次の引数を使用できます。

`--plugin <plugin name>`
: クレデンシャルの有効期間の間隔を設定するプラグインの名前。プラグインの名前をインストール時から変更していない場合、値は vx、nt、nis、nisplus または unixpwd になります。

`--prplptype <default,user,service,product web credential>`
: 設定する有効期間の形式。OS ドメインまたはパブリック ドメインの場合、Symantec Product Authentication Service ではユーザー アカウントとサービス アカウントを区別できないため、デフォルトの有効期限ポリシーだけが使用されます。したがって、ネイティブ ドメインに対してユーザーまたはサービスの有効期限ポリシーを設定しても、実際のクレデンシャルの有効期限には影響しない可能性があります。

`--credexpiry <expiry period (sec)>`
: 有効期限 (秒単位)。

例

このコマンドは、次のように使用します。

```
vssat setexpiryintervals --pluginname vx --prpltype user -
-credexpiry 36000
```

setispbxexchflag

名前
setispbxexchflag

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setispbxexchflag [--enable|--disable]
```

説明
このコマンドを実行すると、--enable オプションまたは --disable オプションに基づいて、PBX Exchange Installed 属性を有効または無効 (1 または 0) のいずれかの状態に設定できます。PBX Exchange Installed 属性の設定に基づいて、ブローカによって PBX に関連するサービスが起動されるかどうかが決定されます。この属性が設定されている場合は PBX に関連するサービスは起動され、設定されていない場合は起動されません。PBX に関連するサービスには、PBX に対する認証のサポートおよびリモート管理が含まれます。

引数
このコマンドには、次の引数を使用できます。

--enable
: PBX に関連するサービスを起動します。

--disable
: PBX に関連するサービスを起動しません。

例
このコマンドは、次のように使用します。

```
vssat setispbxexchflag --enable
```

setpd

名前
setpd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setpd --pdrtype <root|ab|cluster> --domain <name> --
credexpiry <expiry period (sec)>
```

説明
このコマンドを実行すると、プライベート ドメインの属性を設定できます。現在、この方法で設定できる属性は有効期限だけです。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: 属性を設定するドメインの名前。

`--credexpiry <expiry period (sec)>`
: 有効期限 (秒単位)。

例
このコマンドは、次のように使用します。

```
vssat setpd --pdrtype ab --domain Broker@MyHost --
credexpiry 4200
```

setpdr

名前

setpdr

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setpdr --pdrtype <root|ab|cluster> --pdrfile <fqfn
of pdr file>
```

説明

このコマンドを実行すると、プライベート ドメイン リポジトリのデフォルトの位置を変更できます。pdrfile を変更した場合、新しい pdrfile への現在の構成の保存はすぐには行われません。再起動後に、新しい pdrfile がロードされます。

引数

このコマンドには、次の引数を使用できます。

--pdrtype <*root*|*ab*|*cluster*>
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

--pdrfile
: プライベート ドメイン リポジトリとして機能するファイルの名前。

例

このコマンドは、次のように使用します。

```
vssat setpdr --pdrtype root --pdrfile C:¥Program
Files¥VERITAS¥Security¥Authentication¥bin¥RBAuthPDR
```

setsecuritylevel

名前
setsecuritylevel

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setsecuritylevel --level <low|medium|high>
```

説明
このコマンドを実行すると、セキュリティ レベルを設定できます。

引数
このコマンドには、次の引数を使用できます。

`--level <low|medium|high>`
設定するセキュリティ レベル。

例
このコマンドは、次のように使用します。

```
vssat setsecuritylevel --level low
```

注意事項
セキュリティ管理者は、ルート証明書の配布に関して、次のいずれかのセキュリティ レベルを設定できます。

- 高セキュリティ (2): これまで信頼性のなかったルートがピアから取得された場合 (同じ署名のある証明書が信頼できるストア内に存在しない場合) に、ユーザーはハッシュの検証を求められます。
- 中セキュリティ (1): 最初の認証ブローカが信頼され、プロンプトは表示されません。後続の認証ブローカとの信頼関係の確立が試行されると、証明書が信頼できるストアに追加される前に、ユーザーはハッシュの検証を求められます。
- 低セキュリティ (0): 認証ブローカ証明書は常に信頼され、プロンプトは表示されません。

setuptrust

名前

setuptrust

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat setuptrust --broker <host:port> --securitylevel
<low|medium|high> [--hashfile <filename> | --hash <root
hash in hex>]
```

説明

このコマンドを実行すると、信頼関係を設定しようとしているブローカへの問合せ、ケーブルを介した証明書または詳細情報の取得、詳細情報が信頼できる場合に信頼できるリポジトリへの追加を行うことができます。

引数

このコマンドには、次の引数を使用できます。

`--broker <host:port>`
: 信頼関係を設定しようとしているブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

`--hash <root hash in hex>`
: 16 進数形式のルート ハッシュ。セキュリティ レベル高で信頼関係が設定されます。指定したルート ハッシュが検証されなかった場合、信頼関係の設定は失敗します。

`--hashfile <filename>`
: ルート ハッシュを含むバイナリ ファイル。セキュリティ レベル高で信頼関係が設定されます。指定したルート ハッシュが検証されなかった場合、信頼関係の設定は失敗します。

`--securitylevel <low|medium|high>`
: 設定するセキュリティ レベル。(2-17 ページの「ルート証明書の配布」を参照。)

例 1

```
vssat setuptrust --broker MyHost:2821 --securitylevel high
```

例 2

```
vssat setuptrust --broker root_broker.my_domain.com:2821 -
-securitylevel high --hashfile /tmp/root_hash
```

例 3

```
vssat setuptrust --broker root_broker.my_domain.com:2821 -
-securitylevel high --hash
668a754f8201f10955db6326cb076e4086c10477
```

注意事項

セキュリティ管理者は、ルート証明書の配布に関して、次のいずれかのセキュリティ レベルを設定できます。

- 高セキュリティ (2): これまで信頼できなかったルートがピアから取得された場合 (同じ署名のある証明書が信頼できるストア内に存在しない場合) に、ユーザーはハッシュの検証を求められます。
- 中セキュリティ (1): 最初の認証ブローカが信頼され、プロンプトは表示されません。後続の認証ブローカとの信頼関係の確立が試行されると、証明書が信頼できるストアに追加される前に、ユーザーはハッシュの検証を求められます。
- 低セキュリティ (0): 認証ブローカ証明書は常に信頼され、プロンプトは表示されません。

showallbrokerdomains

名前
showallbrokerdomains

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showallbrokerdomains [--global]
```

説明
このコマンドを実行すると、ブローカへのドメインのすべてのマッピングを表示できます。コマンドの実行結果として、ブローカ名、ブローカ ポート、ドメイン名およびドメイン タイプが表示されます。これは、指定した形式の指定したドメインへの認証を試行する際に、指定したブローカ名を指定したポート番号で利用することを示します。--global オプションでは、このマッピングの対象がすべてのプリンシパルか、または現在 OS がログオンしているプリンシパルだけかを指定します。

引数
このコマンドには、次の引数を使用できます。

```
--global
```

グローバル構成レジストリからのすべてのドメインおよびブローカに対して照会を行うように指定します。

例
このコマンドは、次のように使用します。

```
vssat  showallbrokerdomains --global
```

showalltrustedcreds

名前
showalltrustedcreds

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showalltrustedcreds
```

説明
このコマンドを実行すると、信頼できるすべてのクレデンシャルのリスト (ルート証明書) を表示できます。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat showalltrustedcreds
```

showbackuplist

名前

showbackuplist

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showbackuplist [--filename <file name>]
```

説明

このコマンドを実行すると、バックアップおよびリカバリの対象となる、バックアップが必要なファイルおよびディレクトリのリストを取得できます。各ディレクトリまたはファイルは、別々の行に表示されます。--filename 引数を指定すると、リストはそのファイルに出力されます。引数を指定しない場合、標準出力に表示されます。これは、次のように行われます。B| と K| という 2 つの形式のレコードがあるとします。B| 形式のレコードは、バックアップ対象のファイルを示します。このレコードの次の行が R| タグで始まる場合は、レコードの続きです。R| タグの後には、ファイルのリストア時に使用する名前が続きます。R| タグで始まる行がない場合、ファイルのリストア時に使用する名前は、バックアップ ファイル名と同じです。

K| 形式のレコードは 1 行からなり、K| フラグの後にレジストリ キーが続きます。

出力形式は次のとおりです。

B|FileOrDirToBeBackedup
R|RestoreAboveFileOrDirToFileOrDir
K|RegistryKey

すべての B| の後には、R| が続きます。R| がない場合、B| と R| は同じです。

引数

このコマンドには、次の引数を使用できます。

`--filename`
: ファイルおよびディレクトリのリストが書き込まれるファイル名。

例

バックアップが必要なディレクトリおよびファイルのリストを画面に表示するには、次のコマンドを実行します。

```
vssat showbackuplist
```

`list.txt` という名前のファイルに同じリストを取得するには、次のコマンドを実行します。

```
vssat showbackuplist --filename list.txt
```

showbrokerhash

名前
showbrokerhash

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat  showbrokerhash
```

説明
このコマンドを実行すると、ルート ブローカ ハッシュを表示できます。ルート ブローカ ハッシュは、ユーザーがこの情報を使用して信頼関係を確立できるようにルート ブローカ管理者によって公開されます。公開は、企業内で承認されているセキュリティ関連の情報公開ツールを使用して行われます。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat  showbrokerhash
```

showbrokermode

名前
showbrokermode

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showbrokermode
```

説明
このコマンドは、認証ブローカがインストールされているマシンでのみ有効です。管理者 (Administrator) または root ユーザーのみが実行できます。このコマンドを実行すると、現在ブローカが実行されているモードが表示されます。

- 0: ブローカはまだ構成されていません。
- 1: 認証ブローカ専用で実行されています。
- 2: ルート ブローカ専用で実行されています。
- 3: 認証ブローカ兼ルート ブローカで実行されています。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat showbrokermode
```

showbrokers

名前
showbrokers

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showbrokers --domain <type:name>
```

説明
このコマンドを実行すると、特定のドメインのブローカを表示できます。

引数
このコマンドには、次の引数を使用できます。

--domain <*type:name*>
: ブローカを表示するドメイン。

例
このコマンドは、次のように使用します。

```
vssat showbrokers --domain nt:NetBrokerDomain
```

showcred

名前

showcred

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showcred [ --domain <type:name> [--prplname <prpl
name> [-- broker <name:port>]]]
```

説明

このコマンドを実行すると、ローカル リポジトリで使用可能なクレデンシャルを、認証プリンシパルの情報 (名前、ドメイン名およびドメイン タイプなど) を指定して表示できます。オプションを指定しないで実行すると、コマンドを実行したユーザーに対する、証明書のクレデンシャル ストア内のすべてのクレデンシャルが戻されます。ユーザーは、Credential Manager ディレクトリに対するアクセス権を所有し、かつ問題なくアクセスできるため、パスワードは必要ありません。ブローカ情報を指定しない場合、認証プリンシパルに属するすべてのクレデンシャルが表示されます。

異なる認証ブローカの同じ認証プリンシパルに対して、複数のクレデンシャルが存在する場合があります。

引数

このコマンドには、次の引数を使用できます。

--domain <*type:name*>
: クレデンシャルを表示するプリンシパルを保持しているドメインの名前。

--prplname <*prpl name*>
: クレデンシャルを表示するプリンシパルの名前。

--broker <*host:port*>
: ブローカのホストおよびポート。ポートは、指定する必要がありますが、このコマンドでは無視されます。

例

このコマンドは、次のように使用します。

```
vssat showcred --domain vx:broker@MyHost --prplname admin
```

showcredinfo

名前
showcredinfo

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showcredinfo --tag <identity tag> [--en]
```

説明
このコマンドを実行すると、ターゲット マシン上で、リモートから提供された識別情報のプリンシパルおよびドメイン情報を表示できます。

引数
このコマンドには、次の引数を使用できます。

--tag <identity tag>
: 修飾されていない識別情報タグ。多数のマシン上に一意の識別情報が提供されている場合の完全なプリンシパル名は、tag@fully_qualified_host_name です。

--en
: 識別情報が英語で表示されます。

例
このコマンドは、次のように使用します。

```
vssat showcredinfo --tag NBU_AGENT
```

表示内容

```
Principal Name : NBU_AGENT@my_host.my_domain.com
Domain Type    : vx
Domain Name  : broker@my_broker.my_domain.com
Broker Name    : my_broker.my_domain.com
Broker Port      : 1556
```

showcredstore

名前
showcredstore

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showcredstore
```

説明
このコマンドを実行すると、クレデンシャル ストアの詳細情報を表示できます。詳細情報には、ストアの形式 (メモリー、ファイル、Windows のレジストリなど) が含まれます。ファイルの場合、ファイルの位置を指定および表示できます。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat showcredstore
```

showdomains

名前
showdomains

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showdomains --pluginname <plugin name>
```

説明
このコマンドを実行すると、指定したプラグインをサポートしているドメイン名を照会できます。

引数
このコマンドには、次の引数を使用できます。

--pluginname <plugin name>
サポートされているドメインを表示するプラグインの名前。

例
このコマンドは、次のように使用します。

```
vssat showdomains --pluginname vx
```

showexpiryintervals

名前
showexpiryintervals

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showexpiryintervals --pluginname <plugin name>
```

説明
このコマンドを実行すると、設定されているクレデンシャルの有効期間を表示できます。CLI では、4 つのレベルのクレデンシャルの有効期間の間隔 (一般、ユーザー、Web およびサービス プリンシパルの有効期間の間隔) を設定できます。これらの間隔は、プラグイン レベルで設定する必要があります。プライベート ドメインの場合、一般の有効期間の間隔がサポートされています。

引数
このコマンドには、次の引数を使用できます。

`--pluginname <plugin name>`
: クレデンシャルの有効期限レベルを表示するプラグインの名前。

例
このコマンドは、次のように使用します。

```
vssat showexpiryintervals --pluginname vx
```

showglobalplugininfo

名前

showglobalplugininfo

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showglobalplugininfo
```

説明

このコマンドを実行すると、すべてのプラグインの、クレデンシャルの有効期限ポリシーを表示できます。クレデンシャルの有効期限ポリシーは、(1) 個別のプリンシパルの有効期限ポリシー、(2) ドメインの有効期限ポリシー、(3) プラグインの有効期限ポリシー、(4) グローバル (すべてのプラグインの) 有効期限ポリシーの順序で適用されます。

引数

なし

例

このコマンドは、次のように使用します。

```
vssat showglobalplugininfo
```

showispbxexchflag

名前
showispbxexchflag

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showispbxexchflag
```

説明
このコマンドを実行すると、ブローカに PBX Exchange Installed 属性が設定されているかどうかを表示できます。PBX Exchange Installed 属性の設定に基づいて、ブローカによって PBX に関連するサービスが起動されるかどうかが決定されます。この属性が設定されている場合は PBX に関連するサービスは起動され、設定されていない場合は起動されません。PBX に関連するサービスには、PBX に対する認証のサポートおよびリモート管理が含まれます。このコマンドの出力は、フラグが設定されていない場合は 0、フラグが設定されている場合は 1 です。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat showispbxexchflag
```

showpd

名前
showpd

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showpd --pdrtype <root|ab|cluster> --domain <name>
```

説明
このコマンドを実行すると、プライベート ドメインの属性を表示できます。現在、表示できる属性は有効期間の間隔だけです。

引数
このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <name>`
: 属性を表示するドメインの名前。

例
このコマンドは、次のように使用します。

```
vssat showpd --pdrtype ab --domain broker@MyHost
```

showpdr

名前
showpdr

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showpdr --pdrtype <root|ab|cluster>
```

説明
このコマンドを実行すると、プライベート ドメイン リポジトリの位置を表示できます。

引数
`--pdrtype <root|ab|cluster>`
プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

showplugininfo

名前
showplugininfo

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showplugininfo --pluginname <name of the plugin>
```

説明
このコマンドを使用すると、1 つのプラグインについてのすべての詳細情報を表示できます。詳細情報には、有効期限ポリシーなどが含まれます。

引数
このコマンドには、次の引数を使用できます。

`--pluginname <name of the plugin>`

詳細を表示するプラグインの名前 (vx、nis、nisplug、unixpwd、nt など)。

例
このコマンドは、次のように使用します。

```
vssat showplugininfo --pluginname vx
```

showprpl

名前

showprpl

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showprpl --pdrtype <root|ab|cluster> --domain <name>
--prplname <prpl name>
```

説明

ドメイン内のプリンシパルの属性 (プリンシパルの形式、有効期限ポリシーなど) を表示します。

引数

このコマンドには、次の引数を使用できます。

--pdrtype <*root*|*ab*|*cluster*>
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

--domain <*name*>
: プリンシパルが存在するドメインの名前。

--prplname <*prpl name*>
: 属性を表示するプリンシパルの名前。

例

このコマンドは、次のように使用します。

```
vssat showprpl --pdrtype ab --domain broker@MyHost --
prplname TomSawyer
```

showsecuritylevel

名前
showsecuritylevel

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showsecuritylevel
```

説明
このコマンドを実行すると、セキュリティ レベルを表示できます。

引数
なし

例
このコマンドは、次のように使用します。

```
vssat showsecuritylevel
```

showsystemtrustdir

名前

showsystemtrustdir

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showsystemtrustdir
```

説明

このコマンドを実行すると、システム全体に信頼情報が使用されているかどうかを確認して、対応するディレクトリを表示できます。コマンドの実行結果として、デフォルトの System Trust Directory のリストが、コロンで区切られた文字列で表示されます。これは、OpenSSL がサポートしているプラットフォーム固有のディレクトリです。このコマンドでは、OpenSSL によって選択された項目と SSL_CERT_DIR 環境変数に格納されているディレクトリ値が表示されます。ディレクトリ内のすべてのルート証明書は信頼できるルートです。

vssat showsystsemtrustdir によって存在しないディレクトリが戻されるように見える場合があります。この動作は、SSL によって設定されるデフォルトの信頼できるディレクトリが次の場合に発生します。

```
/usr/local/ssl/certs:/var/VRTSat/.VRTSat/profile/
systruststore
```

このディレクトリは、X509_get_default_cert_dir によって戻されます。このディレクトリが存在する必要はありません。このディレクトリが存在し、自己署名した証明書を持つ場合、証明書は信頼されます。このディレクトリは、存在する場合は使用され、存在しない場合は使用されません。

例

このコマンドは、次のように使用します。

```
vssat showsystemtrustdir
```

showversion

名前
showversion

形式
このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat showversion
```

説明
このコマンドを実行すると、Symantec Product Authentication Service コマンドライン インタフェースのバージョンを表示できます。

例
このコマンドは、次のように使用します。

```
vssat showversion
```

updateprpl

名前

updateprpl

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat updateprpl --pdrtype <root|ab|cluster> --domain
<name> --prplname <prpl name>  --prpltype
<default|user|service> --credexpiry <expiry period (sec)>
[--can_proxy] [--can_accept_proxy]
```

説明

このコマンドを実行すると、プリンシパルの属性を更新できます。これらの属性は、作成時に設定されたものです。

引数

このコマンドには、次の引数を使用できます。

`--pdrtype <root|ab|cluster>`
: プライベート ドメイン リポジトリの形式。ルート ブローカ、認証ブローカまたはクラスタを指定します。

`--domain <domain name>`
: プリンシパルが存在するドメインの名前。

`--prplname <prplname>`
: 属性を更新するプリンシパルの名前。

`--prpltype <default|user|service>`
: 最初の設定と異なる場合、このプリンシパルが更新されます。

`--credexpiry <expiry period (sec)>`
: 有効期限 (秒単位)。プリンシパルの有効期限を設定解除してドメインのデフォルトの有効期限ポリシーに戻す場合は、0 (ゼロ) に設定します。異なる場合、プリンシパルが更新されます。

`--can_proxy`
: この引数を指定すると、このプリンシパルは別のプリンシパルのプロキシとして機能します。これは、Web ブラウザを使用しているエンド ユーザーが、Web サーバーをプロキシとしてバックエンド サービスにアクセスする場合の Web クレデンシャルとして使用できます。異なる場合、プリンシパルが更新されます。

`--can_accept_proxy`
: この引数を指定すると、エンティティに対してプロキシを受け入れる権限を付与します。これは、特に Web サーバーのバック エンド サービスで有効です。Web サーバーでは、エンド ユーザーの製品 Web クレデンシャルを配布する前に、受信中のピアが製品 Web クレデンシャルを承

認したかどうか、あるいは、プロキシを受け付けることができるかをチェックします。

例

このコマンドは、次のように使用します。

```
vssat updateprpl --pdrtype ab --domain broker@MyHost --
prplname TomSawyer --prpltype user --credexpiry 0
```

validategroup

名前

validategroup

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat validategroup --groupname <name> --domain
<type:name> --broker <host:port>
```

説明

このコマンドを実行すると、ドメイン名およびブローカを指定して、特定のグループの妥当性を確認できます。

引数

このコマンドには、次の引数を使用できます。

--groupname <*name*>

検証するグループの名前。

--domain <*type:name*>

検証するグループを保持しているドメインの名前。

--broker <*host:port*>

ブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

例

このコマンドは、次のように使用します。

```
vssat validategroup --groupname MyGroup --domain
nt:NewBrokerDomain --broker MyHost:2821
```

validateprpl

名前

validateprpl

形式

このコマンドを使用する場合は、次の構文に従って入力してください (改行は不要)。

```
vssat validateprpl --domain <type:name> --prplname <prpl
name> --broker <host:port>
```

説明

このコマンドを実行すると、ドメイン名およびブローカを指定して、特定のプリンシパルの妥当性を確認できます。

引数

このコマンドには、次の引数を使用できます。

`--domain <type:name>`
: 検証するプリンシパルを保持しているドメインの名前。

`--prplname <prpl name>`
: 検証するプリンシパルの名前。

`--broker <host:port>`
: ブローカのホストおよびポート。Authentication 用の登録ポートは、2821 です。ブローカが他のポート番号を使用して構成されている場合、セキュリティ管理者に問い合わせてください。

例

このコマンドは、次のように使用します。

vssat validateprpl --domain nt:NewBrokerDomain --prplname JohnDoe --broker MyHost:2821

6

その他の管理作業

Symantec Product Authentication Service のその他の管理機能は、管理コンソールでは表示されません。ここでは、その他の管理機能の概要を説明します。また、その機能の詳細を説明した参照先がある場合はそれも示します。

内容は次のとおりです。

- 認証クライアントのオプション構成
- ルート証明書のセキュリティの管理
- Symantec アプリケーション クライアントおよび Symantec アプリケーション サービスの管理
- 個々の Symantec アプリケーション クライアントの管理

認証クライアントのオプション構成

管理者は、必要に応じて、送信ポートの範囲を指定するか、またはライブラリが割り当てられるインタフェースを指定することによって、認証クライアントを構成できます。

認証クライアントへの送信ポートの範囲の指定

認証クライアントでは送信ポートの範囲を構成できます。ポートの範囲は、Windows の場合はレジストリ、UNIX の場合は `/etc/vx/vss/VRTSat.conf` で指定できます。

Windows での送信ポートの範囲の指定

Windows では、HKEY_LOCAL_MACHINE¥Software¥VERITAS¥Security¥Authentication¥Client に、PortRangeMin および PortRangeMax の 2 つのキーを指定できます。

- PortRangeMin は、ポートの開始番号を指定します。
- PortRangeMax が指定されない場合は、デフォルトで、PortRangeMax は PortRangeMin に 1000 を加算した値になります。

UNIX での送信ポートの範囲の指定

UNIX では、このセクションは `Security¥Authentication¥Client` です。キーの名前および意味は、Windows と同じです。

認証クライアントのインタフェースの指定

複数のネットワーク インタフェースを持つマシンの場合、VRTSat クライアント ライブラリが、特定のインタフェースに割り当てられるように構成できます。このインタフェースは、次のレジストリで指定できます。

Windows のクライアント インタフェースの指定

Windows では、次のようにクライアント インタフェースを指定します。

HKEY_LOCAL_MACHINE¥Software¥VERITAS¥Secuity¥Authentication¥Client の
UseInterface = "IP アドレス "

UNIX のクライアント インタフェースの指定

UNIX では、次のようにクライアント インタフェースを指定します。

/etc/vx/vss/VRTSat.conf ファイル内の
Security¥Authentication¥Client セクションの

UseInterface = "IP アドレス "

ここで、IP アドレスには、インタフェースのアドレスを指定します。

ルート証明書のセキュリティの管理

SSL 通信リンクの設定を試行する任意の 2 つのエンティティは、エンティティの証明書の到達先のルート証明書を信頼する必要があります。ルート証明書が正常に配布されていない場合、SSL 通信リンクは確立できません。

Symantec Product Authentication Service は、この問題を解決するために次の 3 つのセキュリティ レベルを識別します。

- 高 : セキュリティ レベル高では、ルート証明書は帯域内に配布されますが、接続を確立する前に、ユーザーに受入れの確認が求められます。
- 中 : セキュリティ レベル中では、ルート証明書は初回だけ受け入れられます。次に新しいルート証明書を見つけたときは、ユーザーに受入れの確認が求められます。
- 低 : セキュリティ レベル低では、新しいルート証明書は常に自動的に受け入れられます。

メモ : ルート ブローカおよび認証ブローカでは、セキュリティは「高 (High)」に設定されます。クライアントでは、セキュリティ レベルはクレデンシャル マネージャ (「全般 (General)」タブ) から設定できます。

Symantec アプリケーション クライアントおよび Symantec アプリケーション サービスの管理

リソース管理アプリケーションとは、Symantec Product Authentication Service によってリソースが保護されている Symantec 社製品のことです。

- Symantec アプリケーション クライアントは、Symantec アプリケーション サービスと呼ばれる別プログラムが提供するサービスまたは機能にアクセスするプログラムです。
- Symantec アプリケーション サービスは、Symantec アプリケーション クライアントから要請されてサービスを提供するプログラムです。クライアントが通信する必要のあるサービスは、ホストにインストールされています。

管理作業には、個々の Symantec 社のリソース管理アプリケーションに固有のものもあります。たとえば、NetBackup 管理者は、バックアップ スケジュールの設定などを行うことができます。このような管理作業については、リソース管理アプリケーション固有のマニュアルを参照してください。

通常、クライアントが使用する必要のある認証ブローカの設定を除いて、Symantec アプリケーション クライアントの管理について Authentication セキュリティ管理者が考慮する必要はありません。

個々の Symantec アプリケーション クライアントの管理

メモ: Symantec アプリケーション クライアントは、Symantec アプリケーション サービスがインストールされているホストから管理コンソールを取得します。管理コンソールでクライアントが使用できるのは、クレデンシャルの管理に使用される部分だけです。

Authentication を使用するための新しいアプリケーションの準備

新しい Symantec 社のリソース管理アプリケーションをインストールする場合、アプリケーションで Symantec Product Authentication Service を使用可能にする前に、認証ブローカのプライベート ドメインに、新しいリモート管理アプリケーションのサービスを追加する必要があります。

A

デバッグおよびログ

内容は次のとおりです。

目的

Symantec Product Authentication Service では、実行時に詳細なデバッグ情報を生成できます。この情報は、バグの追跡のために、開発チームから要求される場合があります。

サービスのデバッグの有効化

コマンド `vxatd -d` を使用すると、Symantec Product Authentication Service のデバッグおよびログの機能を有効にできます。

クライアント側のデバッグの有効化

クライアント側のデバッグおよびログの機能を有効にする手順は、次のとおりです。

UNIX の場合

Bourne または Korn シェルで、次のコマンドを実行します。

```
$ AtClientDebugLog=4:<log file>
$ export AtClientDebugLog
```

C シェルで、次のコマンドを実行します。

```
$ setenv AtClientDebugLog 4:<log file>
```

Windows の場合

```
set AtClientDebugLog=4:<log file>
```

さらに 2 つの環境変数によって、共有ライブラリ ローダー モジュールからデバッグの出力が生成されます。有効にする手順は、次のとおりです。

UNIX の場合

Bourne または Korn シェルで、次のコマンドを実行します。

```
$ VRTSat_API_DEBUG_LEVEL=4
$ VRTSat_API_DEBUG_FILE=<log file>
$ export VRTSat_API_DEBUG_LEVEL
$ export VRTSat_API_DEBUG_FILE
```

C シェルで、次のコマンドを実行します。

```
$ setenv VRTSat_API_DEBUG_LEVEL=4
$ setenv VRTSat_API_DEBUG_FILE=<log file>
```

Windows の場合

```
set VRTSat_API_DEBUG_LEVEL=4
set VRTSat_API_DEBUG_FILE=<log file>
```

ログ レベルの選択

ログ レベルを指定する場合、`vxatd -d` オプションで任意のパラメータを指定します。ログ レベルは次のとおりです。

- 0: ログなし
- 1: エラー ログ
- 2: 警告ログ
- 3: デバッグ メッセージ ログ
- 4: 情報メッセージ ログ

次に例を示します。

`vxatd -d4` (ログ レベルを「情報メッセージ ログ」に設定)

`vxatd -d1` (ログ レベルを「エラーのログ」に設定)

非対話モードでは、localconfig ファイルの「DebugLevel」値から DebugLevel が取得されます。DebugLevel のデフォルト値は 1 (エラー) です。

コマンドラインで指定するログ レベルは、localconfig ファイルで指定されているログ レベルより優先されます。これによって、管理者は、`vxatd` を一定期間デバッグ モードで実行した後、エラー ログ モードで実行できます。

AtClientDebugLog 変数は、サーバーのログ機能には影響しません。

ログ ファイルの場所

非対話モード (デーモンまたは NT サービス) では、メッセージは vxatd.log に記録されます。ログ ファイル名は変更可能です。ログ ファイル名は、localconfig ファイルの「DebugLogFileName」エントリから取得されます。デフォルト値は、次のとおりです。

- Windows の場合 : 現在のディレクトリ内の vxatd.log
- UNIX の場合 : /var/VRTSat/vxatd.log

B

LDAP プラグインの詳細情報

ユーザー データおよびネットワーク データを LDAP (Lightweight Directory Access Protocol) ディレクトリを使用して管理している場合、認証ブローカに LDAP 認証プラグインを使用してユーザー認証を実行することができます。

この付録では、LDAP データの保存とプラグインの動作について説明します。

使用可能な構成情報の詳細については、『Symantec Product Authentication Service リリース ノート』を参照してください。

LDAP の有効化の詳細については、2-27 ページの「LDAP プラグインを有効化する基本的な手順」を参照してください。

スキーマ

NIS データを LDAP ディレクトリに移行する場合、RFC 2307 で指定されているスキーマの仕様に準拠していることが想定されます。ただし、RFC 2307 はガイドラインであり、絶対的な要件ではありません。Microsoft Active Directory などの一部のドメイン認証の実装は、RFC 2307 に準拠していません。

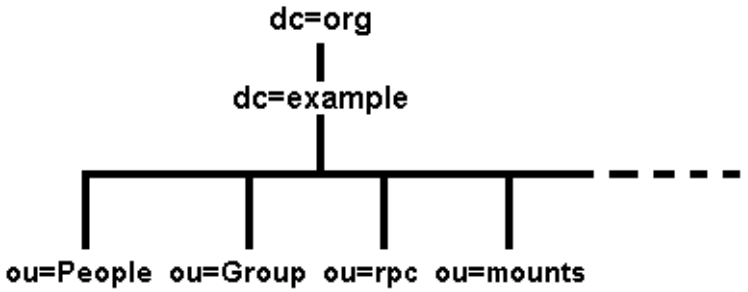
LDAP 認証プラグインは、デフォルトでは RFC 2307 をサポートするように設計されていますが、属性、ベース識別名 (DN) およびオブジェクト クラスが構成可能であるため、その他の導入例にも柔軟に対応できます。

LDAP ディレクトへの NIS データの格納

RFC 2307 では、NIS データを LDAP ディレクトリに格納するためのスキーマが指定されています。このスキーマでは、一般的なすべてのデータベースに対して、passwd、group、hosts、shadow、services、netgroup、protocol、ethers などの属性およびオブジェクト クラスが提供されます。ただし、ツリーの編成方法は指定されていません。

一般的なツリー構造は、次のとおりです。

一般的なツリー構造



ここでは、domain-component の命名規則を使用し、ドメイン名は `example.org` となります。情報の種類ごとに、別々のサブツリーが提供されます。passwd ファイルからのデータは、`ou=passwd` ではなく `ou=People` に格納されます。これは、各ユーザーが 1 つのプライマリ アカウントを所有し、電話番号やメール アドレスなどのその他の情報が同じエントリに追加されることを想定しているためです。

ユーザー パスワード データ

次に、一般的なアカウントのエントリの例を示します。

```
dn: uid=jdoe,ou=People,dc=example,dc=org
uid: jdoe
cn: John Doe
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowLastChange: 11296
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/csh
uidNumber: 500
gidNumber: 500
homeDirectory: /home/jdoe
gecos: John Doe
userPassword: {crypt}$Aab1$uQSw.ohy$XuiRSC...
```

ユーザーのパスワードは、LDAP ディレクトリに格納する前に暗号化する必要があります。パスワードを暗号化する方法の詳細については、UNIX シェルの crypt コマンドの man ページ (man crypt など) を参照してください。

グループ データ

RFC 2307 では、posixGroup オブジェクトの memberUid 属性を使用してグループ メンバーシップを定義します。memberUid は複数値属性であるため、グループ マップを非常に効率的に検索することができます。次に、このディレクトリ内のグループ エントリの例を示します。

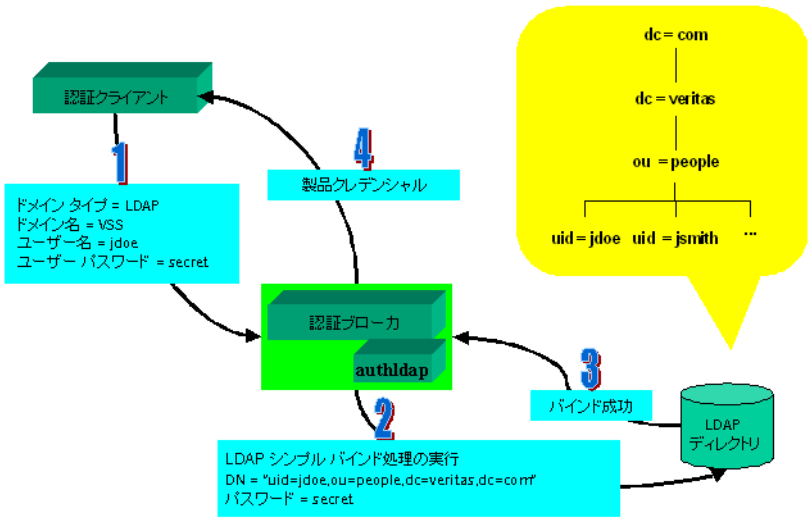
```
dn: cn=ldapbods,ou=Group,dc=example,dc=org
objectClass: posixGroup
objectClass: top
cn: ldapbods
userPassword: {crypt}x
gidNumber: 389
memberUid: tim
memberUid: steve
memberUid: colin
memberUid: damy
memberUid: Andrew
```

authldap の動作

LDAP 認証プラグイン モジュール (authldap) は、認証ブローカに付属している共有ライブラリです。

「LDAP 認証」の図に、認証処理を示します。ここでは、veritas.com ドメインに属する企業内のユーザー John Doe を例としてとりあげます。John Doe は、パスワードとして「secret」を選択し、ドメイン名「VSS」が LDAP ディレクトリ ツリー「ou=people,dc=veritas,dc=com」にマップするように構成されています。ドメイン名が LDAP ツリーにマッピングされているため、ドメイン名およびユーザー名を使用して、ユーザーに対する LDAP DN を正確に作成することができます。

図 B-1 LDAP 認証



LDAP 認証の図の解説

LDAP 認証の図は、次のように解釈します。

1 認証クライアントが、認証ブローカ (AB) を使用してユーザー認証を実行します。この例では、次のとおりです。

- ドメイン タイプ : LDAP
- ドメイン名 : VSS
- ユーザー名 : jdoe
- ユーザー パスワード : secret

2 認証ブローカによって、次の処理が行われます。

   a 指定されたユーザー名およびドメイン名に基づいて、John Doe に対応する LDAP DN が作成されます。

   b 必要に応じて、LDAP ディレクトリへの SSL セッションが確立されます。

   c LDAP ディレクトリを使用して LDAP のバインド処理が実行されます。

3 LDAP のバインド処理が成功すると、ユーザーは LDAP ディレクトリに対して認証されます。Authentication によって、LDAP ディレクトリからグループ情報が取得されます。

4 Authentication によって、John Doe に対する製品クレデンシャルが発行されます。

用語集

AT

CLI コマンドおよび特定のグラフィックで Authentication を示す略語。

CLI

コマンドライン インタフェース。

Secure Sockets Layer プロトコル (Secure Sockets Layer Protocol: SSL)

Netscape 社が開発した公開鍵プロトコル。クライアントとサーバーが Web を介してセキュリティ保護された通信を行うために使用されます。Symantec Product Authentication Service の場合、Secure Sockets Layer テクノロジは、クライアント、認証ブローカおよびサービスの間でセキュリティ保護された通信を提供します。この用語に対しては、通常、略語の SSL が使用されます。

SSPI

Windows のセキュリティ サポート プロバイダー インターフェース (SSPI)。Microsoft プラットフォーム上で動作するアプリケーション間の認証および通信に関する一連のセキュリティ サービスを提供します。

Symantec Product Authentication Service

識別情報を検証し、認証されたエンティティ (ピアとも呼ばれる) 間のセキュリティ保護された通信の設定を行うコンポーネント。管理者が Symantec Product Authentication Service によって保護するように設定したすべての Symantec 社製品にシングル サインオン サービスを提供します。

アカウント名 (Account Name)

「認証プリンシパル」のこと。

アクセス トークン (Access Token)

プリンシパルのログイン時に認証プリンシパルに対して生成されるデータ構造。認証プリンシパルのセキュリティ識別子、プリンシパルが属するグループの識別子、およびログインしたローカル コンピュータに対してプリンシパルが持つ権限のリストが含まれます。アクセス トークンは、認証プリンシパルに対するセキュリティ コンテキストを定義します。

アプリケーション クライアント (Application Client)

アプリケーション サービスと呼ばれる別プログラムが提供するサービスまたは機能にアクセスするプログラム。アプリケーション クライアントには、VERITAS Volume Manager GUI などがあります。アプリケーション クライアントは、Authentication を使用して、そのクライアントのユーザーの ID を検証します。

アプリケーション サービス (Application Service)

アプリケーション クライアントから要請されてサービスを提供するプログラム。

アプリケーション ホスト (Application Host)

アプリケーションが実行されているマシン。

暗号文 (Cyphertext)
暗号化処理によって暗号化された出力。

オブジェクト (Object)
視覚的に具象化できるものであるかどうかを問わず、プロセスまたはプログラムによって取り扱うことのできるエンティティ。

管理コンソール (Administration Console)
Authentication の管理に使用するグラフィカル インタフェース。たとえば、管理者は、別のコンポーネントの位置、信頼関係、プラグイン、プライベート Symantec ドメインを表示する目的で使用します。

公開鍵暗号化 (Public Key Encryption)
セキュリティ方式の 1 つ。1 つの鍵を使用してデータを暗号化し、復号化にはその鍵と数学的な関係を持つ別の鍵が必要です。これら 2 つの鍵には、誰でも使用できる公開鍵と、特定の公開鍵に関連付けられており、かつ秘匿しておく必要がある秘密鍵があります。暗号化にはどちらの鍵も使用できますが、復号化には対となるもう一方の鍵を使用する必要があります。両方の鍵がない場合、処理は失敗します。公開鍵暗号化は、非対称暗号化とも呼ばれます。

公開鍵基盤 (Public Key Infrastructure: PKI)
公開鍵証明書の発行、管理および取消しを行うために構築された枠組み。

サブジェクト (Subject)
認証プリンシパルに代わって (たとえば、認証プリンシパルの権限を使用して) 実行されるスレッド。これらの権限は、その認証プリンシパルを含むセキュリティ プリンシパルに対して、管理者から明示的に付与されます。

証明書 (Certificate)
電子パスポートまたは ID カードの一種。所有者の識別情報を保証して、プリンシパルの名前をユーザーの公開鍵に関連付けます。製品クレデンシャルには、証明書とクライアントの秘密鍵が必要となります。

製品 Web クレデンシャル (Product Web Credential)
ライブラリ内に対応する秘密鍵が存在しないことを Symantec Product Authentication Service ライブラリに示す特殊なクレデンシャル。このクレデンシャルは、プロキシ権限を持つ Web コンソールのクレデンシャルとともに使用する必要があります。

製品クレデンシャル (Product Credential)
有効な識別情報として認識されるために必要な資格。製品クレデンシャルには、プリンシパルの名前をその公開鍵にバインドするために、認証ブローカまたはルート ブローカによって作成および署名された (1) プリンシパルの秘密鍵と (2) 特殊な拡張定義を含む X.509v3 証明書が必要です。製品クレデンシャルは、Symantec 社のシングル サインオン セッション内で動作し、Symantec Product Authentication Service を使用するすべての Symantec アプリケーションに対してシングル サインオン機能を提供します。

セキュリティ コンテキスト (Security Context)
認証プリンシパルの識別情報、認証プリンシパルが属するグループ、およびログインしたローカル コンピュータに対してプリンシパルが持つ権限のセット。セキュリティ コンテキストは、アクセス トークンによって設定されます。

セキュリティ プリンシパル名 (Security Principal Name)
ドメイン内の人間ユーザー、グループまたはコンピュータを識別するために使用する一意の名前。

セキュリティ ポリシー (Security Policy)
製品がユーザーの環境でどのように使用されるべきか、どのように誤用される可能性があるか、アクセス規則のどの範囲を製品によって有効にするかを考慮して、十分に検討して決定した一連の事項。

セキュリティ識別子 (Security Identifier)
企業内のアカウントを持つセキュリティ保護されたプリンシパルを識別する一意の値。

通信ライブラリ (Communications Library)
Symantec Authentication の一部。アプリケーション クライアントとアプリケーション サービス間で、あらかじめ認証処理で取得した製品クレデンシャルを使用してセキュリティ保護された通信を提供します。

デジタル証明書 (Digital Certificate)
「証明書 (Certificate)」を参照。

デジタル署名 (Digital Signature)
メッセージの受信者がメッセージの内容と作成者を検証できるように、メッセージに追加されるデータ ブロック。多数のデジタル署名アルゴリズムが使用されています。

認証局 (Certification Authority)
所有者の識別情報を保証する証明書の発行、管理および取消しを行う信頼できるサードパーティ。Symantec Product Authentication Service では、認証局は認証ブローカの一部です。

認証グループ (Authentication Group)
認証プリンシパルの名前付きのコレクション。ネイティブ オペレーティング システムで設定され、便宜上 1 つのエンティティとして処理されます。認証グループのすべてのメンバーが同じドメインに存在することになります。製品クレデンシャルには、認証ドメイン内でプリンシパルが属するすべてのグループのリストが含まれます。OS グループとも呼ばれます。

認証プライベート ドメイン (Authentication Private Domain)
Symantec 社製品に固有で、Symantec 社製品 (他のドメインに既存の識別情報を再利用しない) によって管理される認証プリンシパルに対する識別情報およびパスワードのハッシュを保持するための特殊な認証ドメイン。認証プライベート ドメインは、ポイント製品 (SANPoint Control、Volume Manager など) の識別情報を保持するために使用できます。

認証プライベート ドメイン リポジトリ (Authentication Private Domain Repository: PDR)
1 つ以上の認証プライベート ドメインのストア。このリポジトリは認証ブローカによってロードされ、これに対してプリンシパルが照合され、検証されます。

認証プラグイン (Authentication Plugin)
認証ブローカによって、特定のドメイン内で識別情報を検証するために使用されるコンポーネント。認証プラグインは、サポートされている認証メカニズムごとに存在します。たとえば、あるプラグインで NIS の識別情報とパスワードの組合せの検証を NIS データベースに対して行うことが可能な一方で、別のプラグインではプリンシパルの認証を行う際に Kerberos ticket を利用できます。

認証プリンシパル (Authentication Principal)
ユーザー、コンピュータ、コマンドライン インタフェース (CLI) などのプロセス、またはサービスの中で、一意の識別情報によって Symantec Product Authentication Service が認証を行うことができるもの。認証プリンシパルは、セキュリティ プリンシパル (すべてが検証できるわけではなく、その処理の責任を必ずしも負うわけではない) とは異なります。

認証ブローカ (Authentication Broker)
ルート ブローカよりレベル (層) が 1 つ下の中間登録局および認証局として機能するコンポーネント。認証ブローカは、クライアント (ユーザー、サービスなど) の認証を行い、製品クレデンシャルの一部となる証明書を付与することができます。ただし、認証ブローカは他のブローカを認証することはできません。他のブローカの認証は、ルート ブローカで実行する必要があります。

認証ブローカ ツリー (Authentication Broker Tree)
3 つのレベル (層) で構成される証明書の階層。すべての識別されるエンティティがこれに含まれ、その証明書は単一のルート証明書につながっています。

認証 メカニズム (Authentication Mechanism)
ドメインで定義された特定の名前空間内のプリンシパルに対して認証を行う方法。たとえば、Kerberos ドメインでは、Kerberos ticket およびパスワードが使用されます。UNIX プラットフォームの場合、Kerberos ドメインは GSS-API を介して使用されます。認証メカニズムは、認証アルゴリズムのすべての細目 (API、プロトコル、トークン形式、トークン コンテンツの構文、データベース オブジェクト形式など) をカプセル化します。関連する構成要素は、メカニズムごとに異なります。

認証ライブラリ (Authentication Library)
Symantec Product Authentication Service の一部。認証の要求を行う際に必要なプログラムの呼出しを実装しており、アプリケーション クライアントにリンクします。

平文 (Plaintext)
暗号化処理されていない入力データ。

プライベート ドメイン (Private Domain)
「認証プライベート ドメイン (Authentication Private Domain)」を参照。

保護されたアプリケーション (Protected Application)
Symantec Product Authentication Service または Symantec Product Authorization Service を使用して保護されるように構成されているリソース管理アプリケーションを意味する簡易名称。

マッピング (Mapping): ドメイン ブローカ
認証を試行する際に、各ドメインで利用すべき認証ブローカを示す情報の集まり。

メッセージ ダイジェスト関数 (Message Digest Function)
入力 (メッセージなど) からダイジェストを生成するアルゴリズム。ダイジェストは統計的には一意であるため、別の入力内容に同じ署名が付けられる可能性はほとんどありません。また、入力に対して少しでも変更を行うと出力が大きく変更されるため、簡単に見破ることができます。

ユーザー (User)
人間の認証プリンシパル。その名前は、Symantec Product Authentication Service によって認識され、オペレーティング システムのアクセス アカウントの名前でもあります。「人間ユーザー」という場合は、この形式のプリンシパルを指します。

リソース管理アプリケーション (Resource Management Application)
Symantec Product Authentication Service によってリソースが保護されている Symantec 社製品のこと。

ルート ハッシュ (Root Hash)
ルート ブローカのクレデンシャルの公開鍵。バイナリ ファイルの形式でルート ブローカを一意に識別します。ルート ハッシュは信頼関係を確立するために使用されます。ルート ハッシュは UNIX の場合は `/opt/VRTSat/bin`、Windows の場合は `<InstallDir>¥Authentication¥bin` にあります。

ルート ブローカ (Root Broker)
自己署名した証明書を持つ最上位にある認証ブローカ。ルート ブローカは、有効と判断されるブローカの名前だけを保持する 1 つのプライベート ドメインを持ちます。ルート ブローカ自身の名前は、完全修飾されたドメイン名 (FQDN) としてそのプライベート ドメインに格納されます。

ルート証明書 (Root Certificate)
デジタル検証に自己署名したもので、認証局の証明書であることを示す固有の情報を含みます。

ルート認証局 (Root Certification Authority)
認証局の最上位の階層に位置するエンティティ。デジタル証明書に署名してプリンシパルの妥当性を保証することができるため、最も信頼できる認証局です。

索引

W

あ

お

か

く

は

ひ

ふ

ほ

ま

め

ゆ

よ

ら

り

る

ろ