Symantec Product Authentication Service™ インストール ガイド

Linux、Microsoft Windows および UNIX

4.3

symantec.

Symantec Product Authentication Service インストール ガイド

Documentation version 2.3

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。サードパーティのソフトウェアの使用に必要なライセンスおよび著作権に関する情報については、本製品リリースノートのサードパーティに関する章を参照してください。

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 システム要件

第 2 章 標準インストール手順

第 4 章 高可用性インストール

第 5 章 管理コンソールの実行

付録 A UNIX の OS ツールを使用したインストール

x

はじめに

このマニュアルは、Symantec Product Authentication Service をインストールおよび構成するユーザーを対象としています。また、製品をインストールする環境を総合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

このマニュアルには、Symantec Product Authentication Service の目的、使用方法、基本的な技術、概念などの概要、またはアーキテクチャに関するより高度な説明は、記載されていません。概要については、『Symantec Product Authentication Service 管理者ガイド』および『Symantec Product Authorization Service 管理者ガイド』を参照してください。

表 1-1　　このマニュアルの内容

タイトル	説明
第 1 章「システム要件」	Symantec Product Authentication Service をインストールおよび実行する際のシステム要件および推奨事項について説明します。
第 2 章「標準インストール手順」	Symantec Product Authentication Service のインストール方法およびアンインストール方法について説明します。
第 3 章「Language Pack およびパッチの使用」	Symantec 製品の Language Pack のインストール方法およびアンインストール方法について説明します。
第 4 章「高可用性インストール」	高可用性を実現するための Symantec Product Authentication Service のインストールおよび構成方法について説明します。

表 1-1 このマニュアルの内容 (続き)

タイトル	説明
第 5 章「管理コンソールの実行」	インストールおよび構成した後で、管理コンソールを実行する方法について説明します。コンソールを使用して実行できる作業については、『VERITAS Security Services 管理者ガイド』を参照してください。
付録 A「UNIX の OS ツールを使用したインストール」	ユーザーが UNIX システムに固有の OS ツールを使用する場合を想定して、OS ツールを使用したインストール方法について説明します。
付録 B「Storage Foundation and High Availability Solutions インストーラを使用した Symantec Product Authentication Service のインストール」	Storage Foundation and High Availability Solutions 製品のインストーラへのアクセス方法および使用方法について説明します。
付録 C「Web コンソールを使用するための構成」	Web コンソールを使用するときに製品 Web クレデンシャルが必要となる理由について説明します。また、Veritas Enterprise Administrator と Web コンソールを併用するための構成例についても示します。

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

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 1-2 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。キーボード 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

Symantec Product Authentication Service のマニュアル

次のマニュアルは、オンライン ヘルプとともに、Symantec Product Authentication Service のマニュアル セットに含まれています。

表 1-3 Symantec Product Authentication Service のマニュアル セットに含まれるマニュアル

マニュアル名称	ファイル名
『Symantec Product Authentication Service インストール ガイド』	AT_InstallGuide.pdf
『Symantec Product Authentication Service 管理者ガイド』	AT_AdminGuide.pdf

1

システム要件

この章では、Symantec Product Authentication Service をインストールおよび実行する際のシステム要件および推奨事項について説明します。

Symantec Product Authentication Service は、識別情報を検証し、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します。認証サービスのシステム要件は、認証サービスを実行する Symantec アプリケーションの要件と同じです。場合によってはさらに要件が増えることもあります。

ハードウェア要件

Symantec Product Authentication Service インストーラでは、ディスク領域の確認が行われ、十分な領域が割り当てられていない場合はエラー メッセージが生成されます。

ソフトウェア要件

Symantec 社のリソース管理アプリケーションには、それぞれ独自のハードウェア要件があります。詳細については、Symantec Product Authentication Service を実行するリソース管理アプリケーションのマニュアルを参照してください。

サポートされているプラットフォーム : 認証サービス

次の表に Symantec Product Authentication Service のサポートを示します。

プラットフォーム	Symantec Product Authentication Service のサポート
AIX 4.3.3.10, 5.1, 5.2, 5.3 (32 ビット版)	サーバーおよびクライアント
AIX 5.1, 5.2, 5.3 (PPC 64 ビット版)	クライアントのみ
FreeBSD 4.9 (x86)	クライアントのみ
HPUX 11.00, 11.11, 11.23	サーバーおよびクライアント
HPUX 11.23 PI (32 ビット版)	サーバーおよびクライアント
HPUX 11.23 PI (64 ビット版)	サーバーおよびクライアント
IRIX 6.5.15-22 (MIPS-32)	クライアントのみ
Linux Redhat AS 2.1 (x86 版)	サーバーおよびクライアント
Linux AS/ES 3.0 (x86 版)	サーバーおよびクライアント
Linux Redhat AS/ES 3.0 (IA64 版)	サーバーおよびクライアント (64 ビット)
Linux Redhat EL 4.0 (x86 版)	サーバーおよびクライアント
Linux Redhat EL 4.0 (IA64 版)	サーバーおよびクライアント (64 ビット)
Linux Redhat EL 4.0 (x86 64 ビット版)	サーバーおよびクライアント (32 ビット互換モード)、クライアント (64 ビット)
Linux SuSe SLES 8.0, 9.0 (x86 版)	サーバーおよびクライアント
Linux SuSe SLES 8.0, 9.0 (IA64 版)	サーバーおよびクライアント (64 ビット)

プラットフォーム	Symantec Product Authentication Service のサポート
Linux SuSe SLES 9.0 (x86 64 ビット版)	サーバーおよびクライアント (32 ビット互換モード)、クライアント (64 ビット)
Linux MontaVista 11.0 (x86 版)	クライアントのみ
Linux WS 21, 30 (x86 版)	クライアントのみ
Mac OS 10.3 (PPC)	クライアントのみ
Solaris 2.6	Symantec Product Authentication Service 4.2 以上ではサポート対象外
Solaris 7、8、9 および 10	サーバーおよびクライアント
Solaris 7、8、9 および 10 (64 ビット版)	サーバーおよびクライアント
Tru64 5.1、5.2	サーバーおよびクライアント
Windows 2000、2003 (x86 版)	サーバーおよびクライアント
Windows XP SP1 および SP2 (x86 版)	サーバーおよびクライアント
Windows Storage Server 2003 (x86 版)	サーバーおよびクライアント
Windows 2000 SAK、SAK Business Server (x86 版)	クライアントのみ
Windows 2003 (x86 64 ビット版)	クライアントのみ (64 ビットおよび 32 ビット互換モード)
Windows 2003 (IA64 版)	サーバーおよびクライアント (64 ビットおよび 32 ビット互換モード)

必要なパッチおよび Service Pack

次に、HP-UX 11.x のパッチのリストを示します。このマニュアルに記載されているパッチは、変更されている場合があります。基本パッチが使用できない場合は、そのパッチを含む累積パッチを適用する必要があります。

HP-UX 11.00 に必要なパッチ

次の表に、HP-UX 11.00 のパッチを示します。

表 1-4 HP-UX 11.00 のパッチ

パッチ ID	パッチの説明
PHSS_26559	s700_800 11.00 ld(1) およびリンカー ツールの累積パッチ
PHSS_24303	11.0 ld(1) およびリンカー ツールの累積パッチ
PHSS_24627	11.0 HP aC++ -AA ランタイム ライブラリ (aCC A.03.33)
PHSS_26945	11.0 HP aC++ -AA ランタイム ライブラリ (aCC A.03.37)
PHCO_18227	11.0 libc の累積パッチ
PHCO_29633	11.0 libc の累積パッチ
PHCO_26960	pthread ライブラリの累積パッチ

HP-UX 11.11 に必要なパッチ

次の表に、HP-UX 11.11 のパッチを示します。

表 1-5 HP-UX 11.11 のパッチ

パッチ ID	パッチの説明
PHSS_26560	1.0 ld(1) およびリンカー ツールの累積パッチ
PHSS_24304	1.0 ld(1) およびリンカー ツールの累積パッチ
PHSS_26946	1.0 ld(1) HP aC++ ランタイム ライブラリ A.03.37
PHSS_32226	s700_800 11.11 libcl パッチ

Solaris に必要なパッチ

Sun Solaris 2.9 SPARC では、Sun パッチ 112907-03 および 112908-17 をインストールする必要があります。

Service Pack

次に、Windows プラットフォームでの Symantec Product Authentication Service の正常なインストールに必要な Service Pack を示します。

- Service Pack 3 (NT 4.0)
- Service Pack 2 (Windows 2000)

その他の要件

Linux RedHat EL 4.0 32 ビット版のマシンに必要な glibc バージョンは 2.3.4-2.9 以降です。

Symantec Product Authentication Service をインストールする前に、Sun Enterprise Authentication Mechanism (SEAM) が非標準の Sun Solaris OS では、すでにインストールされていることを確認してください。SEAM は、GSS-API 認証に必要です。

依存関係

Symantec Product Authentication Service のインストールの準備を行う際、コンポーネントの相互の依存関係を理解しておくと役立ちます。

- 依存性が最も低いコンポーネントは、認証クライアントです。認証クライアントは、マシン上に単独で存在することができます。同じマシンに Symantec Product Authentication Service または Symantec Product Authorization Service の一部が存在する必要はありません。ただし、Symantec Product Authentication Service はいずれかのマシンに存在している必要があります。
- Symantec Product Authentication Service は、同じマシンに認証クライアントが存在する必要があります。

コンソールを実行するための構成要件

管理コンソールは、2 つのモード (認証専用モードおよび認証 + 認可モード) で実行できます。

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
- Tru64 および HP-UX の場合は、セマフォの待ち行列サイズを 256 以上に設定する必要があります。また、プロセス数も、256 以上に設定する必要があります。場合によっては、これらのシステム リソースを利用できないために、認可サービスの起動に失敗することもあります。
- HP でクラスタ環境を構成している場合は、メモリーのサイズが 1 GB 以上である必要があります。
- グラフィカル ユーザー インタフェースを実行する場合、Symantec Product Authentication Service には JDK 1.4.0 以上が必要です。
- ホスト名の名前解決機能が備わっている必要があります。
- Perl 5.6 以上がシステムに存在する必要があります。

メモ : Perl は、パス名に空白が含まれていないディレクトリにインストールされている必要があります。

2

標準インストール手順

この章では、Symantec Product Authentication Service のインストールについて説明します。内容は次のとおりです。

- インストール、構成およびアンインストールする方法の概要
- Symantec Product Authentication Service の設定に必要な作業の概要
- Windows プラットフォームでのインストール、構成およびアンインストール手順
- UNIX プラットフォームでのインストール、構成およびアンインストール手順
- サービスの起動および停止手順

クラスタ環境でのインストールについては、第 4 章「高可用性インストール」を参照してください。

Language Pack のインストールについては、第 3 章「Language Pack およびパッチの使用」を参照してください。

インストールおよび構成方法

Symantec Product Authentication Service は、Windows プラットフォームまたは UNIX プラットフォームにインストールできます。(第 1 章「システム要件」を参照)

メモ : アップグレードを実行する場合は、アップグレードの最後でインストーラからマシンを再起動するように指示されます。これに従ってマシンを再起動する必要があります。これは、Symantec Product Authentication Service に依存しているすべての製品を新しいバージョンで起動させるためです。

Windows でのインストール方法

Windows プラットフォームでは、次の方法でインストールできます。

- 従来のウィザードを使用する。各ウィザード画面で必要な設定を行ってから「Next」をクリックして次のウィザードに進み、「Finish」をクリックしてインストールを完了します。ウィザードは MSI ファイルから起動できますが、対話的なインストールの説明の項では `VxSSVRTSatSetup.exec` を使用しています。
- 2 つのサイレント モードのうちのどちらかを使用する。
  - `VxSSVRTSatSetup.exe` を使用したサイレント インストール。1 度は手動によるインストールが必要ですが、その後は何度でもサイレント インストールを実行できます。
  - MSI ファイル、「`VERITAS Authentication Service.msi`」を使用したサイレント インストール。

UNIX でのインストール方法

UNIX の場合、Symantec Product Authentication Service は、Infrastructure Core Services の一部としてインストールされます。UNIX プラットフォームにインストールする場合、次の 2 通りの方法があります。

- すべての UNIX プラットフォームに有効な、対話形式の方法を使用する。この方法については、この章で説明します。
- プラットフォームに固有の、対話形式の OS ツールを使用する。OS ツールを使用したインストール方法の詳細については、A-1 ページの「UNIX の OS ツールを使用した認証サービスのインストール」を参照してください。
- ICS インストーラを使用して 1 度でも手動でインストールしたことがある場合、生成された応答ファイルを使用してサイレント モードでインストールする。

応答ファイルは、installicsプログラムで対話形式のインストールを行うたびに生成されます。生成された応答ファイルのフル パス名は、インストールの最後に画面上に表示されます。パスは次のような形式です。
/opt/VRTS/install/logs/installics207163245.response
次のようなコマンドを使用して、後でこのファイルをサイレント インストールに使用できます。
installics -responsefile <response file>
installicsを使用したインストールに関する詳細は、『VERITAS Infrastructure Core Services インストール ガイド』を参照してください。

認証サービスの設定に必要な基本作業

少なくとも 1 つのルート ブローカ、1 つの認証ブローカ、および 1 つの認証クライアントをインストールする必要があります。次に示す順序で、インストールしてください。

1 ルート ブローカをインストールします。
ルート ブローカは、認証ブローカと同じマシンにインストールすることも、別のマシンにインストールすることもできます。

- Root + AB: ルート ブローカと認証ブローカを同じマシンにインストールします。(このマシンには、クライアントが存在してもしなくてもかまいません。) これは、1 つのポートで待機する単一プロセスです。

メモ: Root + AB は、最も単純なインストールおよび構成のモードです。ただし、モードを変更する場合にはアンインストールが必要となるため、別のモードの説明を読んでから、このモードを使用するかどうかを決定してください。

- Root Only: 認証ブローカなしでマシンにルート ブローカをインストールします。(このマシンには、クライアントが存在してもしなくてもかまいません。) 他の認証ブローカとは別の、完全にセキュリティ保護されたマシンにルート ブローカをインストールするとセキュリティを強化できると考えられる場合に、このモードを選択します。また、複数の OS ドメインが存在する場合にも、Root Only モードを選択します。たとえば、ホストにルート ブローカ、2 台目のマシンに Windows 用の認証ブローカ、3 台目のマシンに NIS 用の認証ブローカ、4 台目のマシンに NIS+ 用の認証ブローカなどのようにインストールできます。

メモ: このモードを選択する場合は、1 つ以上の認証ブローカを他の場所にインストールする必要があります。Symantec Product Authentication Service は、ルート ブローカと認証ブローカの両方が存在しないと機能しません。

---

2 認証ブローカをインストールします (Root + AB を選択しなかった場合、必須)。
AB Only モードは、ルート ブローカなしでマシンに認証ブローカをインストールします。(このマシンには、クライアントが存在してもしなくてもかまいません。) すでにルートが単独で別の場所にインストールされており、認証ブローカをインストールする必要がある場合にこのオプションを選択します。または、複数の認証ブローカが必要な場合にもこのオプションを選択します。
どちらの場合も、AB Only モードでのインストールは処理が複雑で、いくつかの準備手順が必要となります。準備手順を終了しない限り、AB Only モードでのインストールは試行しないでください。

3 クライアントをインストールします。
このインストール処理では、サービスと同時にまたは単独でクライアントをインストールできます。

Root または Root + AB のインストール

最初に、認証ブローカなしで (Root Only モード)、または認証ブローカと一緒に (Root + AB モード)、ルート ブローカをマシンにインストールします。この項では、Windows および UNIX プラットフォームでのインストール方法について説明します。

Windows での Root または Root + AB のインストール

Windows プラットフォームでは、Root または Root + AB を対話形式またはサイレント モードでインストールできます。

メモ : Symantec Product Authentication Service 4.3 のネイティブ パッケージを直接使用するユーザー自身がインストール時にブローカのデフォルト管理パスワードの変更をすることをお勧めします。2-20 ページの「インストール後のパスワードの変更」を参照してください。また、`vssat createpd` の CLI を使用して作成されたドメインの管理パスワードを変更してください。つまり、`--domain_admin_password` パラメータを使用して、新しく作成されたドメインのドメイン管理パスワードを指定することをお勧めします。パスワードを指定しない場合、ドメイン管理識別情報は、デフォルトのパスワードで作成されます。

メモ : 既存のドメインについては、`vssat resetpasswd` コマンドを使用して管理パスワードを変更できます。

ウィザードを使用した Root または Root + AB のインストール

VxSSVRTSatSetup.exe を使用した認証サービスのインストールでは、従来のウィザードが使用されます。

Windows で従来のウィザードを使用してインストールする方法

メモ: クラスタ環境へのインストールの詳細については、第 4 章「高可用性インストール」を参照してください。

---

1 インストールするマシンに、管理者 (Administrator) としてログオンします。

2 マシンで NTFS ファイル システムが使用されていることを確認します。FAT ではファイル システムのセキュリティが提供されないため、Symantec Product Authentication Service のセキュリティは保証できません。

3 CD から VxSSVRTSatSetup.exe を実行します。

4 InstallShield の最初のウィザード画面が表示されたら、「Next」をクリックします。

5 「Setup Type」画面が表示されたら、「Complete」を選択して、「Next」をクリックします。

メモ: デフォルト (「Typical」) では、クライアントのみがインストールされることに注意してください。サービスもインストールするには、「Complete」を選択する必要があります。

---

6 「Authentication Broker Service Options」画面で必要な設定を行います。

   a 「Root Broker Only」または「Root + Authentication Broker」(最も単純な構成) を選択します。
   (「Root Broker Only」を選択する場合は、2-9 ページの「認証ブローカのインストールおよび構成」を参照して、後で行う認証ブローカの設定に必要な作業を確認してください。)

   b クラスタを有効にする場合は、「Service is Clustered」チェックボックスをチェックし、クラスタ名を入力します。クラスタ名は大文字と小文字が区別されます。

   c サービスを手動と自動のどちらで起動するか、およびインストール後すぐに起動するかどうかを指定します。

   d 必要な選択を行ったら、「Next」をクリックします。

7 「Summary」画面が表示されたら、「Next」をクリックします。

8 ファイルのコピーが完了すると、「InstallShield Wizard Complete」画面が表示されます。

9 「Finish」をクリックします。

メモ: Root Only モードでインストールした場合は、認証ブローカを他の場所にインストールする必要があります。Symantec Product Authentication Service は、認証ブローカが存在しないと機能しません。

Root または Root + AB のサイレント インストール

Windows では、`VxSSVRTSatSetup.exe` または MSI を使用して、Root または Root + AB をサイレント モードでインストールできます。

VxSSVRTSatSetup.exe を使用したサイレント インストールの実行

`VxSSVRTSatSetup.exe` を使用してサイレント モードでインストールするには、1 度は手動でインストール手順を実行する必要があります。その後は何度でもサイレント インストールを実行できます。

1 度 /r オプションを使用してインストールを実行します。

```
VxSSVRTSatSetup.exe /r /f1"c:¥at.rsp"
```

このコマンドによって GUI が起動され、一連のダイアログが表示されます。ダイアログに応答した後で、インストーラはその情報を応答ファイルに保存します。このファイルは次のコマンドを使用してサイレント モードでインストールする場合に何度でも使用できます。

```
VxSSVRTSatSetup.exe /s /f1"c:¥at.rsp"
```

メモ: Root Only モードでインストールする場合は、認証ブローカを他の場所にインストールする必要があります。Symantec Product Authentication Service は、認証ブローカが存在しないと機能しません。(「Root Broker Only」を選択する場合は、2-9 ページの「認証ブローカのインストールおよび構成」を参照して、後で行う認証ブローカの設定に必要な作業を確認してください。)

MSI を使用したサイレント インストールの実行

次のコマンドでは、MSI ファイル (`VERITAS Authentication Services.msi`) が現在のディレクトリにあることを前提とします。

メモ: BROKERMODE、INSTALLLEVEL、PASSWORD1/PASSWORD2 は MSI を使用してブローカをインストールする場合の必須パラメータです。

- Root Only モードでクライアント、サーバーをインストールする場合

```
msiexec /qn /i "VERITAS Authentication Service.msi"
INSTALLLEVEL=2 BROKERMODE=r PASSWORD1 = pass1
```

- Root + AB モードでクライアント、サーバーをインストールする場合
  ```
  msiexec /qn /i "VERITAS Authentication Service.msi"
  INSTALLLEVEL=2
  BROKERMODE=rab PASSWORD1=pass1 PASSWORD2=pass2
  ```

デフォルトの場所または任意の場所のどちらにインストールした場合でも、次の引数を追加できます。

- クラスタ名の指定
  ```
  CLUSTERNAME=abcd
  ```
- SCM の起動タイプの指定
  ```
  SCMSTARTTYPE=auto
  ```
  そのほかに使用可能な値は「manual」で、これはデフォルトです。
- 設定後にサービスを起動させるための指定
  ```
  STARTSERVICE=YES
  ```
  そのほかに使用可能な値は「manual」で、これはデフォルトです。
- アップグレードさせないための指定
  DOUPGRADE=NO
  そのほかに使用可能な値は「YES」で、これはデフォルトです。
- PBX と接続させないための指定
  INSTALLPBX=NO
  そのほかに使用可能な値は「YES」で、これはデフォルトです。

UNIX での Root または Root + AB のインストール

UNIX プラットフォーム上では、対話形式またはサイレント モードでインストールできます。

メモ: Symantec Product Authentication Service 4.3 のネイティブ パッケージを直接使用するユーザー自身がインストール時にブローカのデフォルト管理パスワードの変更をすることをお勧めします。2-20 ページの「インストール後のパスワードの変更」を参照してください。また、`vssat createpd` の CLI を使用して作成されたドメインの管理パスワードを変更してください。つまり、`--domain_admin_password` パラメータを使用して、新しく作成されたドメインのドメイン管理パスワードを指定することをお勧めします。パスワードを指定しない場合、ドメイン管理識別情報は、デフォルトのパスワードで作成されます。

メモ: 既存のドメインについては、`vssat resetpasswd` コマンドを使用して管理パスワードを変更できます。

対話形式を使用した UNIX での Root または Root + AB のインストール

Symantec Product Authentication Service でサポートされる様々な UNIX プラットフォームに対して、同じ手順で対話形式のインストールを実行できます。プラットフォームに固有の OS ツールを使用する場合は、A-1 ページの「UNIX の OS ツールを使用した認証サービスのインストール」を参照してください。

様々な UNIX プラットフォームにインストールする方法

1 root ユーザーとしてホストにログインします。

メモ: Tru64 の OS の制限事項により、インストール処理では、指定したホストにすでにインストールされている旧バージョンの Symantec Product Authentication Service を検出できません。旧バージョンは、最新のバージョンをインストールする前に手動で削除する必要があります。

---

2 コンソールなどのクライアントが実行されていないことを確認します。

3 `installics` プログラムが格納されている CD のディレクトリに移動し、`installics` を実行します。

4 「(I) Install a Product」を選択します。

5 「Symantec Product Authentication Service」を選択します。

6 プロンプトに答えます。

7 「Do you Want to Install the Authentication Broker Server [y, n, q]」と表示されたら、「y」を選択して、クライアントとサーバーの両方をインストールします。

メモ: 「Cannot Copy」というメッセージが表示されても、これは無視できます。これは無意味なメッセージで、インストールには影響しません。

---

8 プロンプトが表示されたら、この時点で構成するかどうかを指定します。「n」を選択した場合は、後で `installics` を再度実行して、「(C) Configure an Installed Product」を選択して構成できます。「y」を選択した場合は、表示される残りのプロンプトに答えます。2-22 ページの「UNIX でのインストール処理後の構成」を参照してください。

9 モードを選択するように求められたら、ルート ブローカ、認証ブローカのみ、または認証 + ルートブローカを選択します。(「Root Broker Only」を選択する場合は、2-9 ページの「認証ブローカのインストールおよび構成」を参照して、後で行う認証ブローカの設定に必要な作業を確認してください。)

10 クラスタ構成を行うかどうかを指定して、表示される残りのプロンプトに答えます。
クラスタの一部であるシステム、クラスタの論理名、プロセス パス、IP アドレスなどの情報の入力が求められます。クラスタ構成での動作に関する情報については、Symantec Cluster Server のマニュアルを参照してください。

11 インストールを行った後に、MANPATH を追加する必要があります。sh または ksh を使用している場合は、次のコマンドを使用します。
```
MANPATH=/opt/VRTS/man:$MANPATH
export MANPATH
```
csh または tcsh を使用している場合は、次のコマンドを使用します。
```
setenv MANPATH /opt/VRTS/man:$MANPATH
```

メモ : Root Only モードでインストールした場合は、認証ブローカを他の場所にインストールする必要があります。Symantec Product Authentication Service は、認証ブローカが存在しないと機能しません。

サイレント モードを使用した UNIX での Root または Root + AB のインストール

応答ファイルは、installics プログラムで対話形式のインストールを行うたびに生成されます。生成された応答ファイルのフル パス名は、インストールの最後に画面上に表示されます。パスは次のような形式です。

```
/opt/VRTS/install/logs/installics207163245.response
```

次のようなコマンドを使用して、後でこのファイルをサイレント インストールに使用できます。

```
installics -responsefile <response file>
```

installics を使用したインストールに関する詳細は、『VERITAS Infrastructure Core Services インストール ガイド』を参照してください。

認証ブローカのインストールおよび構成

認証ブローカをルート ブローカとは別のマシンにインストールする場合は、次の作業を実行します。

1 認証ブローカの識別情報を準備します。(2-10 ページの「認証ブローカの識別情報の準備」を参照。)

2 ルート ハッシュ ファイルを、ルート マシンから認証ブローカ マシンにコピーします。(2-11 ページの「ルート ハッシュ ファイルの検索およびコピー」を参照。)

3 再度インストール プログラムを実行して、認証ブローカをマシンにインストールします。(2-11 ページの「Windows での認証ブローカのインストー

ル」または 2-13 ページの「UNIX での認証ブローカのインストール」を参照。)

認証ブローカの識別情報の準備

ルート ブローカのプライベート ドメイン リポジトリに認証ブローカの識別情報が存在しないと、認証ブローカは正常に機能しません。

認証ブローカの識別情報を準備する方法

1 Root または Root + AB がインストールされているマシンに、root ユーザーまたは管理者 (Administrator) としてログインします。

2 認証ブローカがインストールされている場所の `/bin` ディレクトリに移動し、次のコマンドを実行します。

```
vssat listpd --pdrtype root
```

通常は、次の出力が表示されます。

```
Domain(s) Found 1
****************************
Domain Name root@hostname.fullyqualifieddomain
Expiry Interval 0
****************************
```

メモ: ドメイン名は、書き留めておいてください。この後のコマンドで、この値が必要になります。

---

3 次のように `addprpl` コマンドを実行して、認証ブローカの識別情報を作成します。

```
vssat addprpl --domain root@hostname.fullyqualifieddomain
--pdrtype root --prplname <ABonHostName> --password
<SomeSecurePassword>
```

ここで、`--domain` の引数には、手順 2 で返されたドメイン名を使用します。

<ABOnHostName> は、認証ブローカの識別情報を表します。この名前には、認証ブローカを実行しているマシンのホスト名を指定できます。

<SomeSecurePassword> は、新しく作成した認証のパスワードを表します。セキュリティ保護された、予測不可能なパスワードを使用する必要があります。

識別情報を作成すると、ルートは、AB Only モードで認証ブローカを認証するように構成されます。

ルート ハッシュ ファイルの検索およびコピー

ルート ハッシュ ファイルのコピーが存在しないと、認証ブローカは正常に機能しません。

認証ブローカにルート ハッシュ ファイルを提供する方法

1. 認証ブローカの識別情報を作成したルートがインストールされているマシンにログオンします。
2. ルート ハッシュ ファイルの位置を確認します。ルート ハッシュ ファイルは、認証サービスを Root または Root+AB モードで実行すると作成されます。
   ルート ハッシュ ファイルは root_hash という名前が付けられ、認証サービスがインストールされているディレクトリの /bin ディレクトリに格納されます。
   - UNIX の場合のデフォルト : /opt/VRTSat/bin/root_hash
   - Windows の場合のデフォルト : C:¥Program Files¥VERITAS¥Security¥Authentication¥bin¥root_hash
3. ルート マシンから、新しい認証ブローカをインストールするマシンの特定のディレクトリに root_hash をコピーします。

メモ : ASCII としてではなく、バイナリとしてコピーします。

Windows での認証ブローカのインストール

Windows プラットフォームでは、認証ブローカを対話形式またはサイレント モードでインストールできます。

ウィザードを使用した認証ブローカのインストール

VxSSVRTSatSetup.exe を使用した認証サービスのインストールでは、従来のウィザードが使用されます。

Windows で従来のウィザードを使用してインストールする方法

メモ : クラスタの設定方法については、第 4 章「高可用性インストール」を参照してください。

1. 認証ブローカをインストールするマシンに、管理者 (Administrator) としてログオンします。

2 マシンで NTFS ファイル システムが使用されていることを確認します。FAT ではファイル システムのセキュリティが提供されないため、Symantec Product Authentication Service のセキュリティは保証できません。

3 CD から `VxSSVRTSatSetup.exe` を実行します。

4 InstallShield の最初のウィザード画面が表示されたら、「Next」をクリックします。

5 「Setup Type」画面が表示されたら、「Complete」を選択して、「Next」をクリックします。

6 「Authentication Broker Service Options」画面で必要な設定を行います。

   a 「Authentication Broker Only」モードを選択します。

   b クラスタを有効にする場合は、「Service is Clustered」チェックボックスをチェックし、クラスタ名を入力します。クラスタ名は大文字と小文字が区別されます。

   c サービスを手動と自動のどちらで起動するか、およびインストール後すぐに起動するかどうかを指定します。

   d 「Next」をクリックします。

7 「Authentication Broker Identity」画面で必要な設定を行います。

   - 「Root Broker」領域を次のように設定します。
     - 「Host Name」には、認証ブローカがルート ブローカにアクセスできるホスト名または IP アドレスを入力します。
     - 「Port」には、デフォルトで 2821 が表示されます。この値は変更することができます。
     - 「Hash File」では、「Browse」をクリックし、ルート ブローカからコピーした `root_hash` ファイルを選択します。
   - 「Broker Identity」領域を次のように設定します。
     - 「Name」には、ルート ブローカのプライベート ドメイン リポジトリ内に構成されている認証ブローカの識別情報を入力します。
     - 「Password」には、ルート ブローカのプライベート ドメイン リポジトリ内に構成されている認証ブローカのパスワードを入力します。
     - 「Domain Name」には、ルートおよびこの認証ブローカが存在するドメインを入力します。
   - すべてのフィールドの設定が完了したら、「Next」をクリックします。

8 「InstallShield Wizard Complete」画面が表示されたら、「Finish」をクリックします。

認証ブローカのサイレント インストール

Windows では、VxSSVRTSatSetup.exe または MSI を使用して、認証ブローカをサイレント モードでインストールできます。

VxSSVRTSatSetup.exe を使用したサイレント インストールの実行

VxSSVRTSatSetup.exe を使用してサイレント モードでインストールするには、1 度は手動でインストール手順を実行する必要があります。その後は何度でもサイレント インストールを実行できます。

1 度 /r オプションを使用してインストールを実行します。

```
VxSSVRTSatSetup.exe /r /f1"c:¥at.rsp"
```

このコマンドによって GUI が起動され、一連のダイアログが表示されます。ダイアログに応答した後で、インストーラはその情報を応答ファイルに保存します。このファイルは次のコマンドを使用してサイレント モードでインストールする場合に何度でも使用できます。

```
VxSSVRTSatSetup.exe /s /f1"c:¥at.rsp"
```

MSI を使用したサイレント インストールの実行

次のコマンドでは、MSI ファイル (VERITAS Authentication Services.msi) が現在のディレクトリにあることを前提とします。

メモ : BROKERMODE は MSI を使用してブローカをインストールする場合の必須パラメータです。

```
msiexec /qn /i "VERITAS Authentication Service.msi"
INSTALLLEVEL=2  BROKERMODE=ab IDENTITY=<broker account in
the root domain>  PASSWORD=<broker account password in
root domain>  DOMAIN=root@<fully qualified root machine
name> ROOTHOST=<fully qualified root machine name>
ROOTPORT=<root broker port number> ROOTHASH=<root hash
file>
```

ブローカ モードが AB ではない場合、前述のコマンドで BROKERMODE 以降のプロパティは無視されます。

応答ファイルを使用して構成を行うには、vssconfig.exe コマンドを次のように実行して、作成された vssconfig.xml ファイルを指定します。

```
<InstallDir>¥Authentication¥bin¥vssconfig.exe
..¥vssconfig.xml
```

UNIX での認証ブローカのインストール

UNIX プラットフォーム上では、対話形式またはサイレント モードでインストールできます。

対話形式を使用した UNIX での認証ブローカのインストール

Symantec Product Authentication Service でサポートされる様々な UNIX プラットフォームに対して、同じ手順で対話形式のインストールを実行できます。プラットフォームに固有の OS ツールを使用する場合は、A-1 ページの「UNIX の OS ツールを使用した認証サービスのインストール」を参照してください。

様々な UNIX プラットフォームにインストールする方法

1 root ユーザーとしてホストにログインします。

メモ: Tru64 の OS の制限事項により、インストール処理では、指定したホストにすでにインストールされている旧バージョンの Symantec Product Authentication Service を検出できません。旧バージョンは、最新のバージョンをインストールする前に手動で削除する必要があります。

---

2 コンソールなどのクライアントが実行されていないことを確認します。

3 `installics` プログラムが格納されている CD のディレクトリに移動し、`installics` を実行します。

4 「(I) Install a Product」を選択します。

5 「Symantec Product Authentication Service」を選択します。

6 プロンプトに答えます。

7 「Do you Want to Install the Authentication Broker Server [y, n, q]」と表示されたら、「y」を選択して、クライアントとサーバーの両方をインストールします。(「n」を選択してクライアントのみをインストールする場合、この時点では Root をインストールすることはできません。)

メモ: 「Cannot Copy」というメッセージが表示されても、これは無視できます。これは無意味なメッセージで、インストールには影響しません。

---

8 プロンプトが表示されたら、この時点で構成するかどうかを指定します。「n」を選択した場合は、後で `installics` を再度実行して、「(C) Configure an Installed Product」を選択して構成できます。「y」を選択した場合は、表示される残りのプロンプトに答えます。2-22 ページの「UNIX でのインストール処理後の構成」を参照してください。

9 モードを選択するように求められたら、認証ブローカのみを選択します。

10 次の情報を入力してプロンプトに答えます。

- 認証ブローカを構成するマシン名
- ルート ブローカを実行するホストの名前
- ブローカ ポート (2821)

- 認証ブローカの識別情報
- パスワード
- ドメイン名 (root@mydomain.mycompany.com など)
- ルート ハッシュ ファイルのフル パス名 (2-11 ページの「ルート ハッシュ ファイルの検索およびコピー」を参照。)

11 クラスタ構成を行うかどうかを指定して、表示される残りのプロンプトに答えます。

- Symantec Cluster Server の場合、クラスタの一部であるシステム、クラスタの論理名、プロセス パス、IP アドレスなどの情報の入力が求められます。クラスタ構成での動作に関する情報については、Symantec Cluster Server のマニュアルを参照してください。
- TruCluster の場合、クラスタ名の入力が求められる場合があります。
- Sun Cluster の場合、次の情報の入力が求められます。
  - 共有ストレージとしてマウントするデバイス。
  - 共有ストレージとしてマウントされたデバイスに対応するブロック デバイス。共有ストレージ上に UFS ファイル システムが存在していることを想定しています。

サイレント モードを使用した UNIX での認証ブローカのインストール

応答ファイルは、installics プログラムで対話形式のインストールを行うたびに生成されます。生成された応答ファイルのフル パス名は、インストールの最後に画面上に表示されます。パスは次のような形式です。

```
/opt/VRTS/install/logs/installics207163245.response
```

次のようなコマンドを使用して、後でこのファイルをサイレント インストールに使用できます。

```
installics -responsefile <response file>
```

installics を使用したインストールに関する詳細は、『VERITAS Infrastructure Core Services インストール ガイド』を参照してください。

インストール ログの参照

Windows インストーラは、MSI ログを %temp%¥vrtsatinstall.log に作成します。

認証サービスのインストール後の構成ログは、
<*InstallDir*>¥postinstll.log に格納されます。

認証サービスの起動および停止

インストールが完了すると、Symantec Product Authentication Service が起動します。アンインストールを開始すると、Symantec Product Authentication Service が停止します。これ以外のときに認証サービスを起動または停止する場合は、次の方法を使用します。

Windows でのサービスの起動および停止

Symantec Product Authentication Service は、インストールが完了すると自動的に起動し、アンインストールを開始すると自動的に停止します。ただし、これ以外のときにも認証サービスの起動または停止が必要となる場合があります。

メモ: ブローカは起動する前に特定のモード (Root、Root + AB、AB Only) に指定しておく必要があります。指定されていない場合、ブローカは起動されません。

サービスの起動

Windows で Symantec Product Authentication Service を起動するには、次のいずれかの方法を実行します。

- Windows の「サービス」表示区画での開始オプションの使用
- コマンド コンソールでの `net start vrtsat` コマンドの実行

サービスの停止

Windows で Symantec Product Authentication Service を停止するには、次のいずれかの方法を実行します。

- Windows の「サービス」表示区画での停止オプションの使用
- コマンド コンソールでの `net stop vrtsat` コマンドの実行

UNIX でのサービスの起動および停止

Symantec Product Authentication Service は、インストールが完了すると自動的に起動し、アンインストールを開始すると自動的に停止します。ただし、これ以外のときにも認証サービスの起動または停止が必要となる場合があります。

サービスの起動

UNIX で Symantec Product Authentication Service を起動するには、次のように `vxatd` コマンドを実行します。

```
/opt/VRTSat/bin/vxatd
```

メモ: ブローカは起動する前に特定のモード (Root、Root + AB、AB Only) に指定しておく必要があります。指定されていない場合、ブローカは起動されません。

サービスの停止

UNIX で Symantec Product Authentication Service を停止するには、`vxatd` サービスのプロセス ID に対して `kill` コマンドを発行します (kill 203 など)。

クライアントのみのインストール

多くの場合、認証クライアントは、ルート ブローカまたは認証ブローカ (あるいはその両方) と同時にインストールします。この項では、クライアントを単独でインストールする方法について説明します。

Windows でのクライアントのみのインストール

Windows プラットフォームでは、Windows の `VxSSVRTSatSetup.exe` (InstallShield) を使用して、対話形式またはサイレント モードでクライアントをインストールできます。

ウィザードを使用した認証クライアントのインストール

マシンに認証クライアントを単独でインストールすることが必要な場合もあります。

Windows プラットフォームで従来のウィザードを使用してインストールする方法

1. クライアントをインストールするマシンに、管理者 (Administrator) としてログオンします。
2. マシンで NTFS ファイル システムが使用されていることを確認します。FAT ではファイル システムのセキュリティが提供されないため、Symantec Product Authentication Service のセキュリティは保証できません。
3. CD から `VxSSVRTSatSetup.exe` を実行します。
4. InstallShield の最初のウィザード画面が表示されたら、「Next」をクリックします。
5. 「Setup Type」画面が表示されたら、「Typical」を選択してクライアントのみをインストールし、「Next」をクリックします。
6. 「Summary」画面が表示されたら、「Next」をクリックします。

7 ファイルのコピーが完了すると、「InstallShield Wizard Complete」画面が表示されます。

8 「Finish」をクリックします。

認証クライアントのサイレント インストール

Windows では、VxSSVRTSatSetup.exe または MSI を使用して、認証クライアントをサイレント モードでインストールできます。

VxSSVRTSatSetup.exe を使用したサイレント インストールの実行

VxSSVRTSatSetup.exe を使用してサイレント モードでインストールするには、1 度は手動でインストール手順を実行する必要があります。その後は何度でもサイレント インストールを実行できます。

1 度 /r オプションを使用してインストールを実行します。

```
VRTSatSetup.exe /r /f1"c:¥at.rsp"
```

このコマンドによって GUI が起動され、一連のダイアログが表示されます。ダイアログに応答した後で、インストーラはその情報を応答ファイルに保存します。このファイルは次のコマンドを使用してサイレント モードでインストールする場合に何度でも使用できます。

```
VxSSVRTSatSetup.exe /s /f1"c:¥at.rsp"
```

MSI を使用したサイレント インストールの実行

次のコマンドでは、MSI ファイル (VERITAS Authentication Services.msi) が現在のディレクトリにあることを前提とします。

- クライアントのみをデフォルトの位置にインストールする場合

```
msiexec /qn /i "VERITAS Authentication Service.msi"
```

- クライアントのみを任意の場所にインストールする場合

```
msiexec /qn /i "VERITAS Authentication Service.msi"
INSTALLDIR=d:¥the¥customdir
```

UNIX でのクライアントのみのインストール

マシンに認証クライアントを単独でインストールすることが必要な場合もあります。

対話形式を使用した UNIX でのクライアントのみのインストール

Symantec Product Authentication Service でサポートされる様々な UNIX プラットフォームに対して、同じ手順で対話形式のインストールを実行できます。プラットフォームに固有の OS ツールを使用する場合は、A-1 ページの「UNIX の OS ツールを使用した認証サービスのインストール」を参照してください。

UNIX プラットフォームでクライアントをインストールする方法

1 root ユーザーとしてホストにログインします。

メモ: Tru64 の OS の制限事項により、インストール処理では、指定したホストにすでにインストールされている旧バージョンの Symantec Product Authentication Service を検出できません。旧バージョンは、最新のバージョンをインストールする前に手動で削除する必要があります。

---

2 コンソールなどのクライアントが実行されていないことを確認します。

3 `installics` プログラムが格納されている CD のディレクトリに移動し、`installics` を実行します。

4 「(I) Install a Product」を選択します。

5 「Symantec Product Authentication Service」を選択します。

6 プロンプトに答えます。

7 Sun および HP-UX の場合のみ:「Do you Want to Install the Authentication Broker Server [y, n, q]」と表示されたら、「n」を選択して、クライアントのみをインストールします。(インストールを中止する場合は、「q」を選択します。)

メモ:「Cannot Copy」というメッセージが表示されても、これは無視できます。これは無意味なメッセージで、インストールには影響しません。

サイレント モードを使用した UNIX でのクライアントのみのインストール

応答ファイルは、`installics` プログラムで対話形式のインストールを行うたびに生成されます。生成された応答ファイルのフル パス名は、インストールの最後に画面上に表示されます。パスは次のような形式です。

```
/opt/VRTS/install/logs/installics207163245.response
```

次のようなコマンドを使用して、後でこのファイルをサイレント インストールに使用できます。

```
installics -responsefile <response file>
```

`installics` を使用したインストールに関する詳細は、『VERITAS Infrastructure Core Services インストール ガイド』を参照してください。

インストール後のパスワードの変更

Symantec Product Authentication Service 4.3 のネイティブ パッケージを直接使用するユーザー自身がインストール時にブローカのデフォルト管理パスワードの変更をする必要があります。

認証ブローカのデフォルトの管理者パスワードの変更

この手順は、Symantec Product Authentication Service が $INSTALLDIR にインストールされていることを想定しています。

認証ブローカのデフォルトの管理者パスワードを変更する方法

1 認証ブローカのドメイン名を取得します。

```
$INSTALLDIR/bin/vssat listpd --pdrtype ab | grep "Domain
Name" | awk '{print $3}'
```

2 認証ブローカの管理者パスワードを変更します。

```
$INSTALLDIR/bin/vssat resetpasswd --pdrtype ab --domain
<domainname> --prplname admin --newpasswd <new admin
password> --repeatednewpasswd <new admin password>
```

- *<domain name>* には、手順 1 で取得した認証ブローカのドメイン名を指定します。
- *<new admin password>* には、新しい管理者パスワードを指定します。

ルート ブローカのデフォルトの管理者パスワードの変更

この手順は、Symantec Product Authentication Service が $INSTALLDIR にインストールされていることを想定しています。

ルート ブローカのデフォルトの管理者パスワードを変更する方法

1 ルート ブローカのドメイン名を取得します。

```
$INSTALLDIR/bin/vssat listpd --pdrtype root | grep "Domain
Name" | awk '{print $3}'
```

2 ルート ブローカの管理者パスワードを変更します。

```
$INSTALLDIR/bin/vssat resetpasswd --pdrtype root --domain
<domain name> --prplname admin --newpasswd <new admin
password> --repeatednewpasswd <new admin password>
```

- *<domain name>* には、手順 1 で取得したルート ブローカのドメイン名を指定します。
- *<new admin password>* には、新しい管理者パスワードを指定します。

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¥Security¥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。

UNIX でのインストール処理後の構成

構成は、インストール処理の一部として、または単独で行うことができます。

インストール処理後に構成する方法

1. 構成するマシンに、root ユーザーとしてログインします。
2. CD から `installics` を実行し、「(C) Configure an Installed Product」を選択します。
3. モードを選択するように求められたら、ルート ブローカ、認証ブローカのみ、または認証 + ルートブローカを選択します。(クライアントのみのインストールを選択した場合、このプロンプトは表示されません。)
4. 手順の詳細については、2-7 ページの「UNIX での Root または Root + AB のインストール」または 2-13 ページの「UNIX での認証ブローカのインストール」を参照してください。

「クライアントのみ」から「クライアントおよびサーバー」へのアップグレード

認証クライアントがすでにインストールされている場合、セットアップの再実行でアップグレードを行うためのプロンプトが表示されないときは次の回避策を使用します。

```
msiexec /qn /i "VERITAS Authentication Service.msi"
ADDLOCAL="Server" BROKERMODE=<r|ab|arb>
```

メモ : BROKERMODE は MSI を使用してブローカをインストールする場合の必須パラメータです。

このコマンドラインでは、すべてのサーバー固有のプロパティを使用できます。たとえば、次のような引数を追加できます。

- クラスタ名の指定
  `CLUSTERNAME=abcd`
- SCM の起動タイプの指定
  `SCMSTARTTYPE=auto`
  そのほかに使用可能な値は「manual」で、これはデフォルトです。

- 設定後にサービスを起動させるための指定
  STARTSERVICE=YES
  そのほかに使用可能な値は「manual」で、これはデフォルトです。

認証サービスのアンインストール

この項では、Windows および UNIX プラットフォームでのアンインストール方法について説明します。

Windows での認証サービスのアンインストール

Windows プラットフォームでは、Windows の VxSSVRTSatSetup.exe (InstallShield) を使用して、対話形式またはサイレント モードでクライアントをアンインストールできます。

ウィザードを使用した認証サービスのアンインストール

Windows のウィザードを使用してアンインストールする方法

1. アンインストールするマシンに、管理者 (Administrator) としてログオンします。
2. 「コントロール」メニューの「アプリケーションの追加と削除」パネルを使用して、認証サービスのパッケージを削除します。
3. Symantec Product Authentication Service 全体をアンインストールする場合は、「削除」を選択します。

メモ : Symantec Product Authentication Service 全体ではなく個別の機能をアンインストールする場合は、1-5 ページの「依存関係」を参照して、依存関係にある機能をアンインストールしないように確認してください。確認したら、「削除」ではなく「変更」を選択します。

NetBackup クライアント ユーザーの場合は、2-25 ページの「NBU クライアント ユーザーが Symantec Product Authentication Service を削除する方法」を参照してください。

認証サービスのサイレント アンインストール

Windows では、VxSSVRTSatSetup.exe または MSI を使用して、Symantec Product Authentication Service をサイレント モードでアンインストールできます。

VxSSVRTSatSetup.exe を使用したサイレント アンインストールの実行

VxSSVRTSatSetup.exe を使用してサイレント モードでアンインストールするには、1 度は手動でアンインストール手順を実行する必要があります。その後は何度でもサイレント アンインストールを実行できます。

1 度 /r オプションを使用してインストーラを実行し、アンインストールを行います。

```
VxSSVRTSatSetup.exe /r /f1"c:¥at.rsp"
```

このコマンドによって GUI が起動され、一連のダイアログが表示されます。ダイアログに応答した後で、インストーラはその情報を応答ファイルに保存します。このファイルは次のコマンドを使用してサイレント モードでアンインストールする場合に何度でも使用できます。

```
VxSSVRTSatSetup.exe /s /f1"c:¥at.rsp"
```

MSI を使用したサイレント アンインストールの実行

次のコマンドでは、MSI ファイル (VERITAS Authentication Services.msi) が現在のディレクトリにあることを前提とします。

- クライアントおよびサーバーがインストールされている状態からサーバーを削除する場合

  ```
  msiexec /qn /x "VERITAS Authentication Service.msi"
  REMOVE="Server"
  ```

- MSI ファイルを指定して、Symantec Product Authentication Service を完全にアンインストールする場合

  ```
  msiexec /qn /x "VERITAS Authentication Service.msi"
  ```

- MSI ファイルを指定しないで Symantec Product Authentication Service を完全にアンインストールする場合

  ```
  msiexec /qn /x "{A824C2E4-8D3B-4D7A-8BBF-ACAB75E925CA}"
  ```

NetBackup クライアント ユーザーの場合は、2-25 ページの「NBU クライアント ユーザーが Symantec Product Authentication Service を削除する方法」を参照してください。

UNIX での認証サービスのアンインストール

Symantec Product Authentication Service でサポートされる様々な UNIX プラットフォームに対して、同じ手順でアンインストールを実行できます。

UNIX プラットフォームで認証サービスをアンインストールする方法

1. 現在 root ユーザーであることを確認します。
2. 管理コンソールなどの認証クライアントが実行されていないことを確認します。
3. installics プログラムが格納されている CD のディレクトリに移動し、installics を実行します。

4 「(U) Uninstall a Product」を選択して、表示されるプロンプトに答えます。

NBU クライアント ユーザーが Symantec Product Authentication Service を削除する方法

次に示す削除手順は、NBU クライアントのユーザーに適用されます。Symantec Product Authentication Service を削除する場合、ユーザーは次の手順を行う必要があります。

1 必要に応じて ~/.VRTSat をバックアップします。「~/」はユーザーのホームディレクトリを表します。

2 ~/.VRTSat を削除します。
rm -rf ~/.VRTSat を実行します。

コンソールの実行方法の参照先

管理コンソールの実行方法については、第 5 章「管理コンソールの実行」を参照してください。

3

Language Pack およびパッチの使用

このドキュメントには、Symantec Product Authentication Service の中国語および日本語の Language Pack およびパッチをインストールするためのガイドラインが記述されています。Language Pack をインストールする前に、最初にこの章を読む必要があります。製品ごとの README に記述されている個別の指示と併せて、次に示す手順を実行してください。

Symantec Product Authentication Service の基本パッケージをまだインストールしていない場合は、手順を実行する前にインストール方法を示したドキュメントを読み、基本パッケージをインストールしてください。

この章の主な内容は次のとおりです。

Language Pack およびパッチの目的

Symantec Product Authentication Service には、次のものが含まれます。

- 基本プログラム
- Language Pack
- Language Pack のパッチ

Symantec Product Authentication Service をインストールした後に、Language Pack をインストールすることにより、選択した言語で Symantec Authentication Service をローカライズできます。

Language Pack をインストールした後で、対応する Language Pack のパッチをインストールして、Language Pack そのものに存在する特定の問題を解決する必要があります。

Windows での Language Pack およびパッチのインストールおよびアンインストール

Language Pack およびパッチの場所

Windows 用の Language Pack は次の場所にあります。

```
CDROM_DRIVE:¥<version>-lang¥windows¥authentication¥pkgs
```

GUI を使用した Language Pack のインストール

GUI を使用してサービスの Language Pack をインストールする方法

1. インストールを開始するには、`VERITAS Authentication Service Chinese/Japanese Language pack.msi` をダブル クリックします。
2. 次のフィールドの内容が正しいことを確認します。
   - User name
   - Organization
   - Install this application for
3. 上記の項目が正しければ、「Next」をクリックします。
4. 「Custom」を選択して、「Next」をクリックします。
5. 「Click on a icon in the list below to change how a feature is installed」フィールドの下で「+」をクリックし、機能リストを展開します。
6. 「Server Message Catalog」のドロップダウン メニューから、「This feature will be installed on a local hard drive」を選択します。インストール先を変

更する場合は「Change」ボタンをクリックし、続いて「Next」をクリックします。インストール先が正しい場合は、「Next」をクリックして続行します。

7 変更する必要がある場合は、「Back」をクリックして修正を行います。インストールの準備が完了したら、「Next」をクリックします。

8 「Finish」をクリックして、インストールを終了します。

GUI を使用してクライアントの Language Pack をインストールする方法

1 インストールを開始するには、`VERITAS Authentication Service Client Chinese/Japanese Language pack.msi` をダブル クリックします。

2 次のフィールドの内容が正しいことを確認します。
- User name
- Organization
- Install this application for

3 上記の項目が正しければ、「Next」をクリックします。

4 「Custom」を選択して、「Next」をクリックします。

5 インストール先を変更する場合は「Change」ボタンをクリックし、続いて「Next」をクリックします。インストール先が正しい場合は、「Next」をクリックして続行します。

6 変更する必要がある場合は、「Back」をクリックして修正を行います。インストールの準備が完了したら、「Next」をクリックします。

7 「Finish」をクリックして、インストールを終了します。

CLI を使用した Language Pack のインストール

CLI を使用してサービスまたはクライアントの Language Pack をインストールする方法

CLI を使用して Language Pack をインストールする場合、次の 2 つの方法があります。

- コマンドライン インタフェースを使用したインストール
  コマンドラインから次のように入力します。
  ```
  msiexec /i "<package name>"
  ```
- サイレント インストール
  コマンドラインから次のように入力します。
  ```
  msiexec /qn /i "<package name>"
  ```

GUI を使用したパッチのインストール

GUI を使用してサービスのパッチをインストールする方法

1. インストールを開始するには VERITAS Authentication Service Chinese/Japanese Language pack.msi をダブル クリックします。(ファイル名は Language Pack と同じです。)
2. 次のフィールドの内容が正しいことを確認します。
   - User name
   - Organization
   - Install this application for
3. 上記の項目が正しければ、「Next」をクリックします。
4. 「Custom」を選択して、「Next」をクリックします。
5. 「Click on a icon in the list below to change how a feature is installed」フィールドの下で「+」をクリックし、機能リストを展開します。
6. 「Server Message Catalog」のドロップダウン メニューから、「This feature will be installed on a local hard drive」を選択します。インストール先を変更する場合は「Change」ボタンをクリックし、続いて「Next」をクリックします。インストール先が正しい場合は、「Next」をクリックして続行します。
7. 変更する必要がある場合は、「Back」をクリックして修正を行います。インストールの準備が完了したら、「Next」をクリックします。
8. 「Finish」をクリックして、インストールを終了します。

GUI を使用してクライアントのパッチをインストールする方法

1. インストールを開始するには、VERITAS Authentication Service Client Chinese/Japanese Language pack.msi をダブル クリックします。(ファイル名は Language Pack と同じです。)
2. 次のフィールドの内容が正しいことを確認します。
   - User name
   - Organization
   - Install this application for
3. 上記の項目が正しければ、「Next」をクリックします。
4. 「Custom」を選択して、「Next」をクリックします。
5. インストール先を変更する場合は「Change」ボタンをクリックし、続いて「Next」をクリックします。インストール先が正しい場合は、「Next」をクリックして続行します。

6 変更する必要がある場合は、「Back」をクリックして修正を行います。インストールの準備が完了したら、「Next」をクリックします。

7 「Finish」をクリックして、インストールを終了します。

CLI を使用したパッチのインストール

CLI を使用してサービスまたはクライアントのパッチをインストールする方法

CLI を使用して Language Pack のパッチをインストールする場合、次の 2 つの方法があります。

- コマンドライン インタフェースを使用したインストール
  コマンドラインから次のように入力します。
  `msiexec /i "<patch name>"`
- サイレント インストール
  コマンドラインから次のように入力します。
  `msiexec /qn /i "<patch name>"`

GUI を使用した Language Pack のアンインストール

GUI を使用して Language Pack をアンインストールする方法

1 インストールした Language Pack を右クリックします。

2 ポップアップ メニューから「アンインストール」を選択します。

CLI を使用した Language Pack のアンインストール

アンインストールを実行するには、システム上にどの MSI パッケージをインストールしたか (クライアントまたはサーバー用の Language Pack) を知る必要があります。MSI は「アプリケーションの追加と削除」には表示されません。

CLI を使用して Language Pack をアンインストールする方法

1 MSI パッケージが存在する適切なディレクトリに移動し、コマンドラインから次のように入力します。

```
C:¥msiexec /x "<package name>"
```

2 また、サイレント アンインストールを実行するには、コマンド ラインから次のように入力します。

```
C:¥msiexec /qn /x "<package name>"
```

UNIX の Language Pack の場所

UNIX では、次のディレクトリ レイアウトが使用されます。

```
CD/<language_code>/<platform または "doc">/<product>/pkgs
```

<language_code> には、次の値が使用されます。

- ja
- zh

<platform> には、次の値が使用されます。

- aix: AIX 4.3 および 5.x
- hpux: HP 11.00、HP 11i および HP 11.23
- linux: Linux x86 および Linux ia64 のバリアント
- tru64: OSF1/Tru64 5.x
- sun: Solaris 7、8、9 および 10

<product> には、次の値が使用されます。

- authentication
- authorization
- private_branch_exchange
- service_management_framework

したがって、Symantec Product Authentication Service の最終的なディレクトリ構造は、次のようになります。

```
<CD_MOUNT>/ja/sun/authentication/pkgs
```

Solaris での Language Pack およびパッチのインストールおよびアンインストール

Solaris での Language Pack のインストール

Solaris に Language Pack をインストールする方法

1. 3-6 ページの「UNIX の Language Pack の場所」を確認します。
2. 次のように入力して、`install_lp` スクリプトを実行します。
   ```
   ./install_lp
   ```
3. インストールする言語を選択するよう求められたら、言語を選択します。
4. インストールするシステムの名前を入力します。

インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。

5 終了するには、[Enter] キーを押します。

Solaris でのパッチのインストール

Solaris にパッチをインストールする方法

1 3-6 ページの「UNIX の Language Pack の場所」を確認します。

2 次のように入力して、`installvp` スクリプトを実行します。

```
./installvp
```

3 インストールする言語を選択するよう求められたら、言語を選択します。

4 インストールするシステムの名前を入力します。
インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。

5 終了するには、[Enter] キーを押します。

PATH の設定

Solaris では、起動時のプロファイルに `PATH` を追加する必要があります。この設定にはフルパスを使用する点に注意してください。

Solaris の Language Pack のアンインストール

Solaris の Language Pack をアンインストールするには、次のコマンドを入力します。

```
pkgrm VRTSatZH ( または VRTSatJA)
```

Solaris のパッチのアンインストール

Solaris の Language Pack のパッチをアンインストールするには、次のコマンドを入力します。

```
patchrm <patch name>
```

AIX での Language Pack およびパッチのインストールおよびアンインストール

AIX での Language Pack のインストール

AIX に Language Pack をインストールする方法

1. 3-6 ページの「UNIX の Language Pack の場所」を確認します。
2. 次のように入力して、`install_lp` という名前のインストール スクリプトを実行します。
   ```
   ./install_lp
   ```
3. インストールする言語を選択するよう求められたら、言語を選択します。
4. インストールするシステムの名前を入力します。
   インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。
5. 終了するには、[Enter] キーを押します。

AIX でのパッチのインストール

AIX に Language Pack のパッチをインストールする方法

1. 3-6 ページの「UNIX の Language Pack の場所」を確認します。
2. 次のように入力して、`installvp` スクリプトを実行します。
   ```
   ./installvp
   ```
3. インストールする言語を選択するよう求められたら、言語を選択します。
4. インストールするシステムの名前を入力します。
   インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。
5. 終了するには、[Enter] キーを押します。

PATH の設定

AIX プラットフォームでは、起動時のプロファイルに PATH を追加する必要があります。この設定にはフルパスを使用する点に注意してください。

AIX の Language Pack のアンインストール

- AIX の Language Pack をアンインストールするには、コマンド プロンプトで次のいずれかのコマンドを入力します。

```
installp -u VRTSatJA
installp -u VRTSatZH
```

AIX のパッチのアンインストール

Solaris のパッチは削除できますが、他の UNIX プラットフォームのパッチは削除できません。

HP での Language Pack およびパッチのインストールおよびアンインストール

HP での Language Pack のインストール

HP に Language Pack をインストールする方法

1. 3-6 ページの「UNIX の Language Pack の場所」を確認します。
2. 次のように入力して、`install_lp` という名前のインストール スクリプトを実行します。
   `./install_lp`
3. インストールする言語を選択するよう求められたら、言語を選択します。
4. インストールするシステムの名前を入力します。
   インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。
5. 終了するには、[Enter] キーを押します。

HP でのパッチのインストール

HP に Language Pack のパッチをインストールする方法

1. 3-6 ページの「UNIX の Language Pack の場所」を確認します。
2. 次のように入力して、`install_lp` という名前のインストール スクリプトを実行します。
   `./install_lp`
3. インストールする言語を選択するよう求められたら、言語を選択します。
4. インストールするシステムの名前を入力します。

インストール スクリプトによって、認証、認可またはその両方のパッケージがインストールされているかどうかが検証されます。その後、該当する Language Pack がシステムへ自動的にインストールされます。

5 終了するには、[Enter] キーを押します。

PATH の設定

HP プラットフォームでは、起動時のプロファイルに PATH を追加する必要があります。この設定にはフルパスを使用する点に注意してください。

HP の Language Pack のアンインストール

HP の Language Pack をアンインストールする方法

1 次のコマンドを入力します。

```
swremove VRTSatZH ( または VRTSatJA)
```

2 または swremove の CLI を使用します。

HP のパッチのアンインストール

Solaris のパッチは削除できますが、他の UNIX プラットフォームのパッチは削除できません。

4

高可用性インストール

サーバー クラスタは、アプリケーションおよびデータの高可用性を実現します。サーバー クラスタでは、2 台以上のサーバー (ノードと呼ばれる) がネットワークに接続され、すべてのノードから共有バスへのアクセスを可能にするためのクラスタ ソフトウェアが動作しています。共有バスへは、任意の数のディスクを接続できます。ノードが使用できなくなった場合、クラスタ リソースは使用可能なノードにマイグレートされます (この動作は、フェイルオーバーと呼ばれます)。フェイルオーバー中、共有バス上のディスクと仮想サーバーは使用可能のままですが、サービスへの割込みがわずかに発生します。

Symantec Product Authentication Service は、次のクラスタ環境で動作します。

表 4-1

クラスタ プラットフォーム	OS プラットフォーム
VCS 2.0	Windows 2000、Linux AS 2.1
VCS 3.5	HP-UX 11.0、AIX 5.1、Linux AS 2.1、Solaris 7
VCS 4.0	Solaris 7
VCS 4.1	Windows (2000、2003、XP)、Solaris (7、8、9、10)、HP-UX (11.0、11.11、11.23)、AIX (5.1、5.2)
HP Service Guard A.04.00	HP-UX (11.11、11.23)
MSCS 5.0	Windows 2000
SunCluster 3.1	Solaris 7、8、9 および 10
TruCluster 5.1	Tru64 5.1

この章では、高可用性を実現するための Symantec Product Authentication Service のインストールおよび構成方法について説明します。

Symantec Product Authentication Service のクラスタ機能

高可用性ソフトウェアの 2 つの主要な機能は、フェイルオーバー機能とデータの永続性の提供です。

フェイルオーバー機能

フェイルオーバー機能を提供するには、Symantec Product Authentication Service に、次のような方法を実施することを推奨します。

- 起動 / 停止のプロシージャまたはスクリプトの使用 (適用可能な場合)
- ホスト名の使用
  認証サービスでは、クラスタ名タグの構成が可能です。これは、プライベート ドメイン データベースでのドメイン名の一意性のために使用されます。
- 接続
  認証サービスおよび認可サービスでは、仮想 IP アドレスの構成が可能です。サービスは、ローカル ホストまたは仮想 IP への (ローカルまたはリモートからの) サービス要求をすべてのインタフェースで待機します。

データの永続性

データに永続性を持たせるには、Symantec Product Authentication Service に、次のような方法を実施することを推奨します。

- 認証プライベート ドメイン データベースは、2 つの部分に分割することができます。ローカル PDR は、ローカル ファイル システムに構成することができます。
- クレデンシャルとキー ストアは、共有ディスクに構成することができます。

メモ : 認可サービスに関するデータの永続性については、『Symantec Product Authorization Service インストール ガイド』を参照してください。

クラスタ環境の特別なシステム要件

クラスタ モードで Symantec Product Authentication Service をインストールするには、カスタム モードでインストールして、空白が含まれていないパス名を選択する必要があります。たとえば、
`c:¥program_files¥Veritas¥Security¥Authentication` を選択します。これは、完全なパスに空白が含まれると一部の Symantec Cluster Server コマンドが動作しないという問題が Symantec Cluster Server に存在するためです。こ

の問題によって、Symantec Product Authentication Service のクラスタ構成が失敗します。`c:¥program files` の場合は、「program」と「files」の間に空白が含まれるため、問題が発生します。

空白のあるパスに Symantec Product Authentication Service がインストールされている場合は、アンインストールして、適切なパスに再インストールする必要があります。

推奨の構成

メモ: Symantec Product Authentication Service には、個別のリソース (共有ディスク、IP、ネットワーク名) を割り当てることをお勧めします。こうすることで、リソースの障害の影響範囲を Symantec Product Authentication Service だけに抑えることができます。

次の 3 つのいずれかのモードで構成することができます。

- Root Only
- Root+AB
- AB Only

どのモードを選択した場合でも、クラスタ内のノードはすべて同じモードでインストールする必要があります。

プラットフォームにかかわらず、Root Only モードでブローカを構成した場合は、ルート ブローカをクラスタ上で実行する必要はありません。ルート ブローカは、ほとんど使用されることがないためです。唯一使用されるのは、認証ブローカの設定中です。

グループおよび依存関係

メモ: バージョン 4.1 以前の Symantec Cluster Server、MSCS、Sun Cluster、または TruCluster の場合、認証サービスおよび認可サービスはクラスタ内の同じノードに存在する必要があります。

認可サービスを使用している場合のグループおよび依存関係の確立については、『Symantec Product Authorization Service インストール ガイド』を参照してください。

Symantec Product Authentication Service と Microsoft Cluster Server の併用

Microsoft Cluster での VxAT の構成

C:¥Program Files¥VERITAS¥security¥Authentication¥bin ディレクトリに存在する VxATmscs.bat を実行します。このバッチ スクリプトには、2 つのオプションがあります。

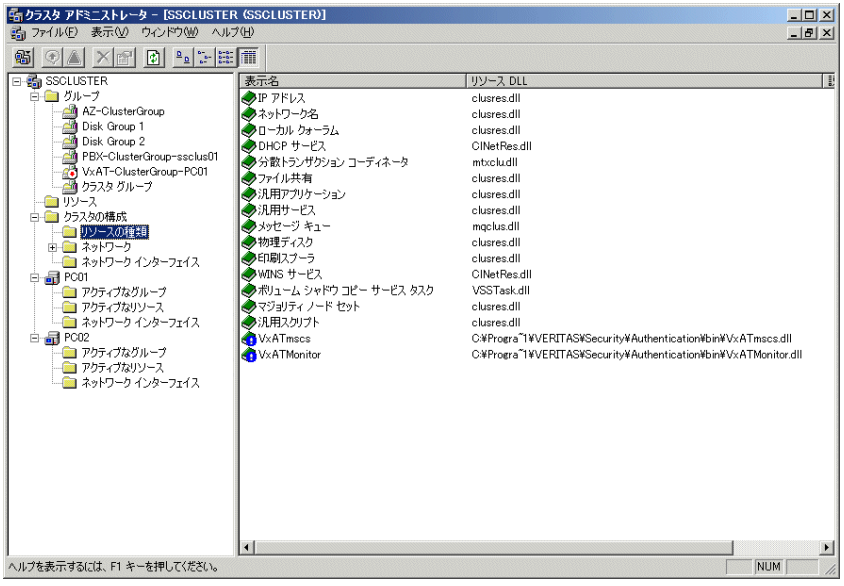
- -c: MSCS で VxAT を構成します。次に例を示します。
  VxATmscs.bat -c
- -u: MSCS から VxAT を構成解除します。次に例を示します。
  VxATmscs.bat -u

クラスタ構成の検証

バッチ スクリプトを実行すると、次のリソースおよびグループが MSCS に作成されます。

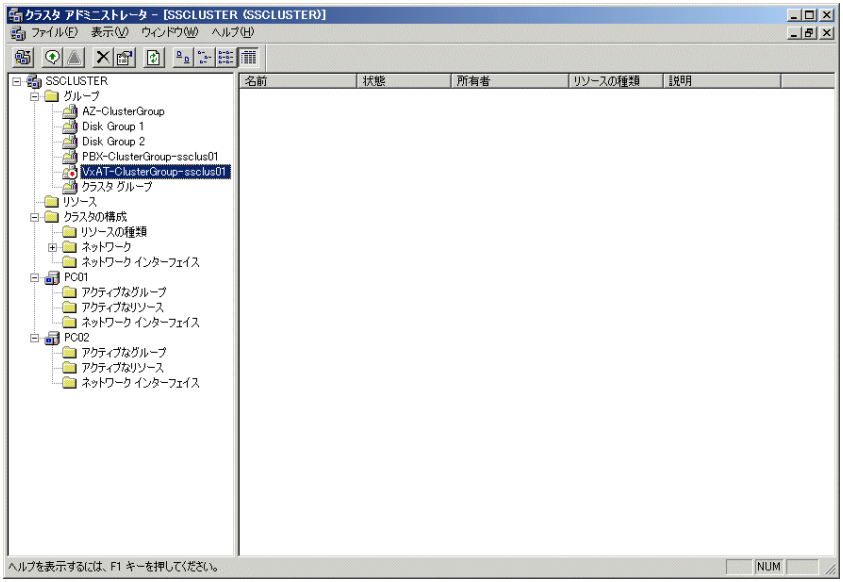
1 `VxATMonitor` および `VxATmscs` の 2 つのリソース形式が作成されます。

図 4-1 VxATMonitor および VxATmscs



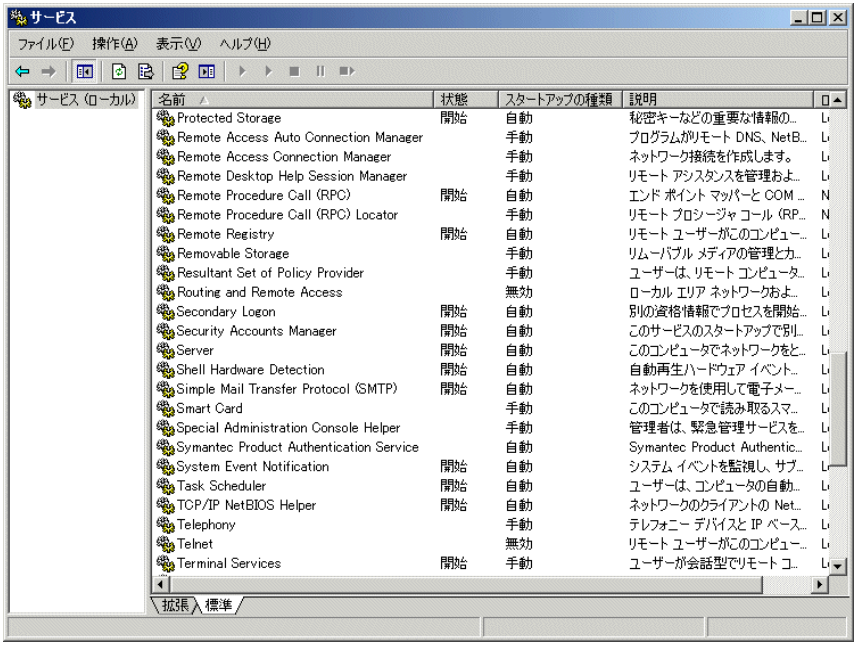
2 AT-ClusterGroup-<*host name*> グループに、「ATmscs」形式のリソース AT-<*hostname*> が作成されます。

図 4-2 VxAT リソース AT-ssclus01



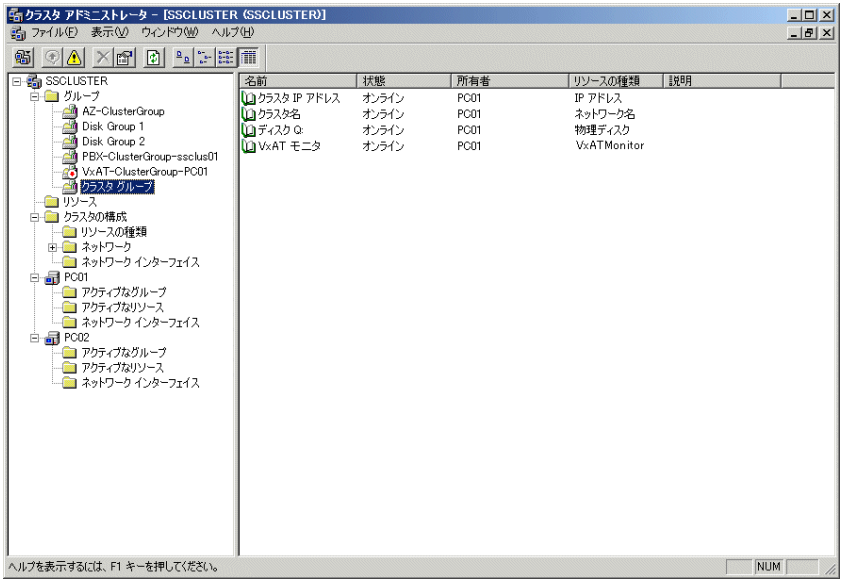
3 サービス タブを使用して、認証サービスが開始されているかどうかを確認します。

図 4-3 サービスの開始状態の表示



4 IP アドレス、クォーラム ディスクおよびクラスタ名リソースが含まれる Cluster Group に、別のリソース VxAT_Monitor が作成されます。このリソースは AT-ssclus01 リソースの状態を監視し、AT-ssclus01 リソースがオンライン以外の状態であることを検出した場合は、別のノードにクラスタ グループをフェイルオーバーします。

図 4-4 VxAT_Monitor のオンライン状態の表示



VxAT_Monitor リソースは AT-ssclus01 リソースの状態を監視し、AT-ssclus01 リソースがオンライン以外の状態であることを検出した場合は、別のノードにクラスタ グループをフェイルオーバーします。

Symantec Product Authentication Service と VCS の併用

この項では、すべてのプラットフォームの VCS で Symantec Product Authentication Service を構成する手順について説明します。

- すべてのプラットフォームの VCS で Symantec Product Authentication Service を構成するには、次のいずれかのディレクトリに存在する VxATclconf.pl を実行します。
  - Windows の場合 : C:¥Program Files¥veritas¥security¥Authentication¥bin
  - UNIX の場合 : /opt/VRTSat/bin

次のように指定します。

```
perl VxATclconf.pl -M[i/n]
```

引数の意味は次のとおりです。

- `-Mi`: 対話形式。
- `-Mn`: 同じディレクトリにある `clinput.txt` から入力を読み取ります。
- `-F<input file>` (デフォルトは、同じディレクトリにある VxATclinput.txt)
- `-I<VxAT install location>`
- `-V<VCS install location>`
- `-D<identification string>`: デバッグのみで、コマンドは実行されません。
- `-help`: ヘルプ情報が表示されます。

注意 : `-Mn` オプションを使用する場合、入力ファイル `VxATclinput.txt` は、Perl ファイルと同じディレクトリに存在している必要があります。このファイルには、VSC に Symantec Product Authentication Service を構成するために必要なすべての属性値が含まれています。

Symantec Product Authentication Service のリソース ツリーは、VCS のバージョンによって異なります。次の図で確認できます。

図 4-5　　バージョン 3.5 より前の VCS

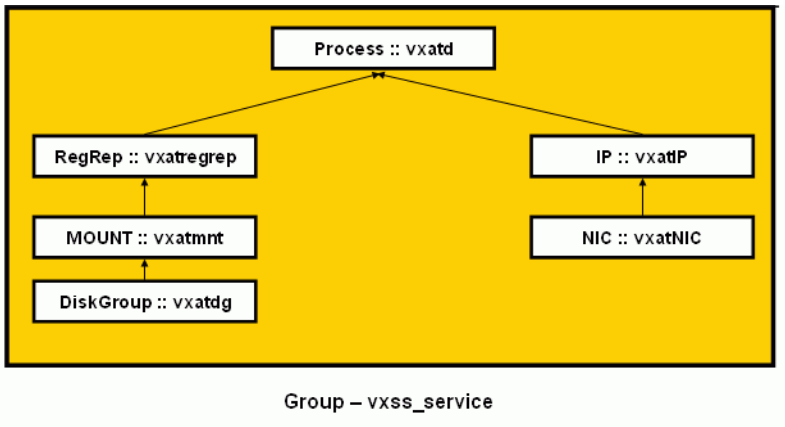
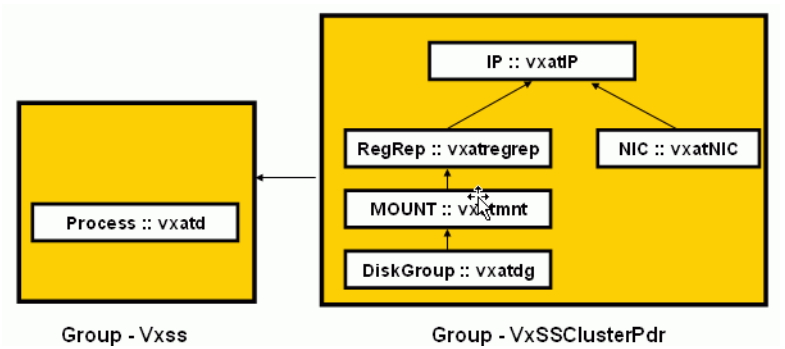


図 4-6　　バージョン 3.5 以上の VCS



`vxatregrep` は、Windows 固有のリソースです。UNIX プラットフォームの場合、このリソースは除外してください。このリソースは、レジストリ エントリの作成および更新に使用します。

VCS Java コンソールのスクリーンショット

次に、VCS 3.5 以上の Symantec Product Authentication Service 構成のスクリーンショットを示します。

図 4-7 Java スクリーンショット : VxSS グループ

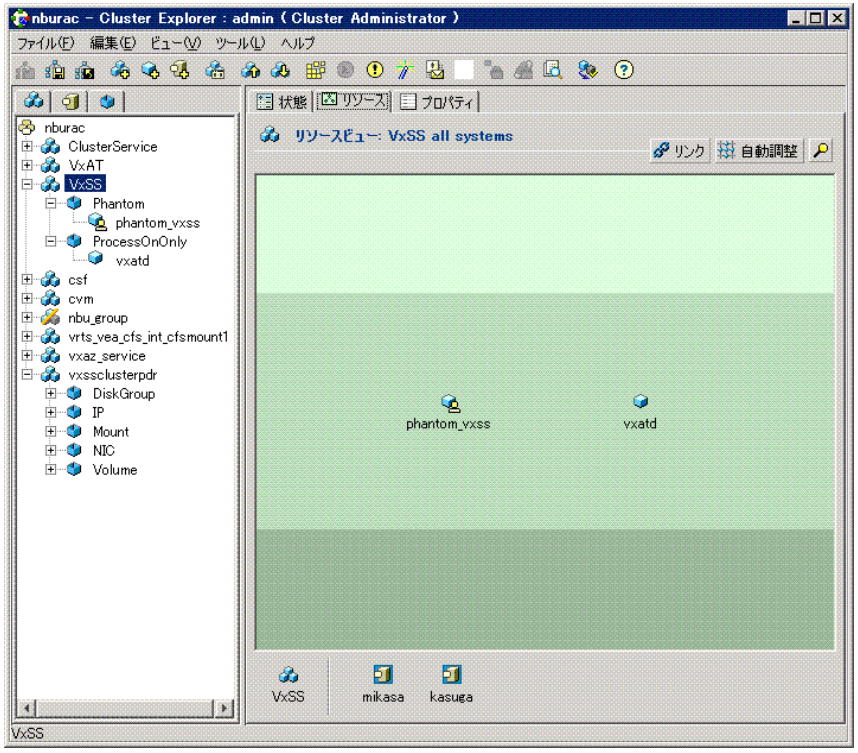
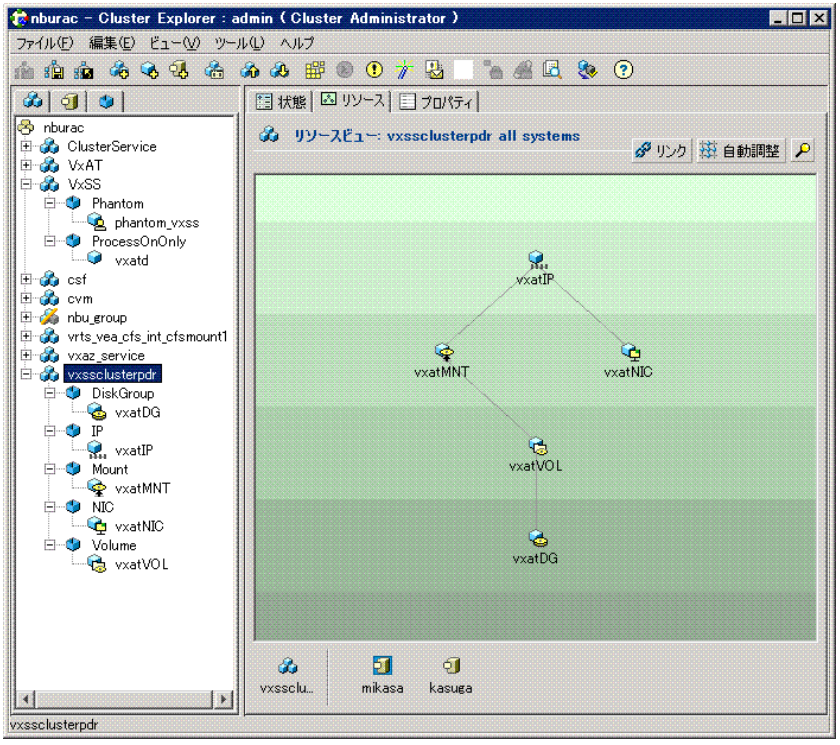


図 4-8　　Java スクリーンショット : vxssclusterpdr グループ



SunCluster での Symantec Product Authentication Service の使用

Sun Cluster 上で、Symantec Product Authentication Service をフェイルオーバー データ サービスとして構成できます。

構成のための準備

ノード間の共有データを保持するには、少なくとも 1 つの Sun Cluster グローバル デバイスを登録する必要があります。このデバイスは、Symantec Volume Manager ディスク グループか、またはクラスタ内のノード間でフェイルオーバーが可能であればどのようなデバイスでもかまいません。フェイルオーバーした場合、このデバイスはクラスタの他のノードに切り替えられます。そのためこのデバイスは、Symantec Product Authentication Service がフェイルオーバーする際にフェイルオーバーすべきサービス以外のサービスによって使用されていないことが重要です。(Symantec Product Authentication Service と Symantec

Product Authorization Service のフェイルオーバーは同時に行われるため、認証サービスと認可サービスのリソースには、同じグローバル デバイス グループを使用することができます。)

認証サービスの構成

scvxat スクリプトを使用するか、または第 2 章「標準インストール手順」および第 3 章「Language Pack およびパッチの使用」で説明されている UNIX の場合の手順を実行して、Sun Cluster で Symantec Product Authentication Service を構成することができます。

scvxat スクリプトを使用する場合の構成

メモ: クラスタの各ノードに、Symantec セキュリティ パッケージをインストールしておく必要があります。

Symantec Product Authentication Service を Sun Cluster で構成するには、次の 3 つの手順を実行します。

構成方法

1 クラスタ ノードを準備する。

2 サービスを構成する。

3 Sun Cluster リソースを作成する。

各手順で、/opt/VRTSat/bin に存在する構成スクリプト scvxat が使用されます。

手順 1: クラスタ ノードの準備

SUNW.HAStoragePlus リソースを作成するには、クラスタのすべてのノードの /etc/vfstab ファイルに、適切なマウント ポイント エントリが存在している必要があります。このエントリは、手動で作成することができます。また、クラスタの各ノードで、scvxat を -pernode オプションとともに使用して作成することもできます。

-pernode を指定して scvxat を実行する場合、次の 2 つの情報の入力が必要です。

- 共有ストレージとしてマウントするデバイス。
- 共有ストレージとしてマウントされたデバイスに対応するブロック デバイス。

共有ストレージ上に UFS ファイル システムが存在していることを想定しています。

たとえば、共有ストレージとしてディスク グループ shared_dg 内の Symantec Volume Manager ボリューム at_vol を使用する場合、次のコマンドを実行する必要があります。

```
# scvxat -pernode /dev/vx/dsk/shared_dg/at_vol /dev/vx/rdsk/shared_dg/at_vol
```

-pernode を指定して scvxat を実行すると、/etc/vfstab ファイルに次のエントリが作成されます。

```
/dev/vx/dsk/shared_dg/at_vol /dev/vx/rdsk/shared_dg/at_vol /var/VRTSat57 ufs 2 no -
```

作成されたエントリが設定と一致しない場合は、このファイルの内容を変更する必要があります。たとえば、使用しているファイル システムが UFS でない場合、対応するエントリを変更する必要があります。

手順 2: サービスの構成

2 番目の手順では、サービスを構成します。

メモ: リソースの作成中、scvxat によって、サービス構成ファイルおよび生成された鍵マテリアルが共有ストレージに移動されます。そのため、高可用性を実現するには、あらかじめサービスを構成しておく必要があります。

サービスの構成には、クラスタ名の設定および鍵マテリアルの生成が含まれます。デフォルトでは、Symantec Product Authentication Service は、プライベート ドメイン名の完全修飾されたホスト名 (FQHN) を使用します。クラスタ サービスを特定のホストに関連付けないようにするために、サービスが、ホスト名ではなくクラスタ名を使用するように指定します。これは、鍵を生成する前に行う必要があります。

クラスタ名の設定

scvxat を -setclustername オプションとともに使用して、クラスタ名を設定することができます。たとえば、クラスタ名が surya の場合、次のコマンドを使用してクラスタ名を登録できます。

```
# scvxat -setclustername surya
```

ブローカ ドメインは、root@< 完全修飾されたホスト名 > ではなく、root@surya および broker@surya になります。

鍵の生成

vxatd を -o オプションとともに実行して、鍵を生成することができます。詳細については、『Symantec Product Authentication Service 管理者ガイド』を参照してください。

次のコマンドを実行すると、ブローカの鍵が Root + AB モードで生成されます。

```
# vxatd -o -a -r
```

手順 3: Sun Cluster リソースの作成

構成の最後の手順では、リソースを作成します。

メモ: この手順は、クラスタの任意の 1 つのノードで実行する必要があります。(グローバル デバイスが現在オンラインになっているノードで実行することをお勧めします。)

`scvxat` を `-create` オプションとともに使用して、この手順を実行することができます。この形式の `scvxat` では、次の 2 つの情報の入力が必要です。

- 論理ホスト名
- 共有ストレージをホスティングするグローバル デバイス名

たとえば、クラスタに関連付けられている論理ホスト名が `surya` で、グローバル デバイス名が `shared_dg` の場合、次のコマンドを実行します。

```
scvxat -create surya shared_dg
```

このコマンドを実行すると、必要な認証サービスのリソースを含む `vxss_resource` というリソース グループが作成され、オンラインになります。リソース グループの状態は、SunPlex Manager GUI から、または次のコマンドを使用してコマンドラインから照会することができます。

```
scstat -g | grep "vxss_resources"
```

スクリプトを使用しない構成

クラスタ構成スクリプトを手動で実行せずに、Symantec Product Authentication Service をインストールおよび構成することができます。この場合、一連のメッセージに応答すると、バックグラウンドでコマンドラインが実行されます。

スクリプトを使用せずにインストールおよび構成する方法

1. 認証サービスのコンポーネントをインストールします。(第 2 章「標準インストール手順」を参照。)
2. サーバーのインストールおよび構成オプションを選択します。
3. クラスタの構成オプションを選択します。次のメッセージが表示されます。

```
You can choose to prepare this system as a cluster node.
Alternatively, if all other nodes are prepared, you can
choose to create resources on this node.
    1) Prepare this cluster node.
    2) Prepare this cluster node & create resources.
What do you want to do? [1-2,q]
```

4. 4-12 ページの「手順 1: クラスタ ノードの準備」で説明されている手順を実行する場合は 1 を選択します。また、クラスタのその他のすべてのノードの

準備が完了し、そのノードを使用してリソースを作成する準備ができている場合は 2 を選択します。

5 プラットフォーム固有のクラスタの構成に関する質問に答えます。次の情報の入力が求められます。

- 共有ストレージとしてマウントするデバイス。
- 共有ストレージとしてマウントされたデバイスに対応するブロック デバイス。共有ストレージ上に UFS ファイル システムが存在していることを想定しています。

入力が完了すると、認証サービスが起動します。

6 次のコマンドを実行して、認証サービスが起動していることを確認します。

```
scstat -g | grep "vxss_resources"
```

「State」が、「Online」である必要があります。

構成を再試行する場合の AT リソースの削除

エラーが発生した場合、構成を再試行する前にリソースを削除する必要があります。`scvxat` を使用して作成されたリソースを削除するには、このコマンドを `-clean` オプションとともに使用します。

たとえば、次のコマンドを使用して、認証サービスの構成時に作成された Sun Cluster リソースを削除することができます。

```
scvxat -clean
```

メモ: 認可サービスの構成手順については、『Symantec Product Authorization Service インストール ガイド』を参照してください。

TruCluster での Symantec Product Authentication Service の使用

TruCluster 上で、Symantec Product Authentication Service をフェイルオーバー データ サービスとして構成できます。

概要

TruCluster では、Symantec Product Authentication Service は単一インスタンスのアプリケーション リソースとして構成されます。つまり Symantec Product Authentication Service は、一度に 1 つのクラスタ メンバー上でのみ実行されます。サービスがインストールされているクラスタ メンバーに障害が発生した場合、Cluster Application Availability (CAA) サブシステムによって、実行中の他のメンバーにアプリケーションをフェイルオーバーすることができます。

TruCluster 上で Symantec Product Authentication Service を構成するには、次の 2 つの手順を実行します。

- アプリケーション リソースのプロファイルを作成する。
- CAA サブシステムを使用して、作成したプロファイルを登録する。

メモ: TruCluster のクラスタ ファイル システム (CFS) では、クラスタ間における単一の名前空間、およびクラスタ内のすべてのファイル システムへの一貫性のあるアクセスがサポートされます。そのため、Symantec Cluster Server および Sun Cluster での認証サービスの構成とは異なり、Tru64 では、個別の共有ストレージを構成する必要はありません。

Symantec Product Authentication Service の構成

`tcvxat` スクリプトを使用するか、または第 2 章「標準インストール手順」で説明されている UNIX の場合の手順を実行して、TruCluster で Symantec Product Authentication Service を構成することができます。

tcvxat スクリプトを使用する場合の構成

`/opt/VRTSat/bin` に存在する `tcvxat` を使用して構成を行うことができます。TruCluster 構成では、CAA サブシステムを使用して、アプリケーション リソースのプロファイルを作成および登録します。ただし、Symantec Product Authentication Service を起動する前にいくつかの構成が必要な場合があるため、リソース プロファイルを作成する前に、サービスの構成手順を実行する必要があります。

手順 1: 認証サービスの構成

デフォルトでは、`VRTSat` サービスは、プライベート ドメイン名の完全修飾されたホスト名 (FQHN) を使用します。クラスタ サービスを特定のホストに関連付けないようにするために、サービスが、ホスト名ではなくクラスタ名を使用するように指定します。これは、鍵を生成する前に行う必要があります。

`tcvxat` を `-setclustername` オプションとともに使用して、クラスタ名を設定します。

例

クラスタ名が `trucluster` の場合、次のコマンドを使用して登録します。

```
/opt/VRTSat/bin/tcvxat -setclustername trucluster
```

ブローカ ドメインは、`root@FQHN` ではなく `root@trucluster` および `broker@trucluster` になります。`vxatd` を `-o` オプションとともに実行して、鍵を生成することができます。`vxatd` の使用方法については、『Symantec Product Authentication Service 管理者ガイド』を参照してください。

例

次のコマンドを実行すると、ブローカの鍵が Root + AB モードで生成されます。

```
/opt/VRTSat/bin/vxatd -o -a -r
```

手順 2: アプリケーション リソースの作成および登録

サービスを構成し、鍵マテリアルを生成したら、VRTSat サービスのアプリケーション プロファイルを作成および登録する必要があります。次のように、tcvxat を -register オプションとともに使用して実行します。

```
/opt/VRTSat/bin/tcvxat -register
```

次のような内容が出力されます。

```
Creating VRTSat application profile
Validating profile
caa_profile -validate VRTSat
Registering profile
caa_register VRTSat
Starting VRTSat service
caa_start VRTSat
Attempting to start 'VRTSat' on member 'ssclus08'
Start of 'VRTSat' on member 'ssclus08' succeeded.
VRTSat successfully registered as a caa application
```

このコマンドを実行すると、VRTSat デーモンを含む VRTSat というリソース プロファイルが作成され、オンラインになります。リソースの状態を照会するには、次のコマンドを実行します。

```
/usr/sbin/caa_stat VRTSat
```

次のような内容が出力されます。

```
NAME=VRTSat
TYPE=application
TARGET=ONLINE
STATE=ONLINE on ssclus08
```

スクリプトを使用しない場合のインストールおよび構成

クラスタ構成スクリプトを手動で実行せずに、サービスをインストールおよび構成して、CAA を使用して登録することができます。この場合、一連のメッセージに応答すると、バックグラウンドでコマンドラインが実行されます。

スクリプトを使用せずにインストールおよび構成する方法

1. Symantec Product Authentication Service をインストールします。(第 2 章「標準インストール手順」を参照。)
2. サーバーのインストールおよび構成オプションを選択します。
3. クラスタの構成オプションを選択します。
4. プラットフォーム固有のクラスタの構成に関する質問に答えます。
   認証サービス クラスタ構成のクラスタ名の入力が求められる場合があります。入力が完了すると、認証サービスが起動します。

5 次のコマンドを実行して、サービスが起動していることを確認します。

```
/usr/sbin/caa_stat VRTSat
```

「State」が、「Online」である必要があります。

メモ: 認可サービスの構成手順については、『Symantec Product Authorization Service インストール ガイド』を参照してください。

CAA からの登録の削除

`tcvxat` を使用して作成および登録されたリソースを削除するには、コマンドに `-unregister` オプションを付けて使用します。

Symantec Product Authorization Service を登録した場合は、CAA から認証サービスの登録を削除する前に、認可サービスの登録を削除します。認可サービスの登録を削除するには、次のコマンドを実行します。

```
/opt/VRTSaz/bin/tcvxaz -unregister
```

次のコマンドを使用して、認証サービスの構成時に作成された TruCluster リソース プロファイルおよびスクリプトを削除することができます。

```
/opt/VRTSat/bin/tcvxat -unregister
```

注意: エラーが発生した場合、構成を再試行する前にリソースを削除する必要があります。

HP での Symantec Product Authentication Service の使用

HP ServiceGuard 上で、Symantec Product Authentication Service をフェイルオーバー データ サービスとして構成できます。

設計要件

HP ServiceGuard クラスタで Symantec Product Authentication Service を構成するための設計要件を次に示します。

- Symantec Product Authentication Service は、Symantec Product Authorization Service がインストールされていないクラスタに構成できます。Symantec Product Authorization Service は、後でインストール時に構成できます。
- クラスタ上の Symantec Product Authentication Service (使用している場合は Symantec Product Authorization Service も) は、フェイルオーバー モードで実行する必要があります。

- Symantec Product Authentication Service (使用している場合は Symantec Product Authorization Service も) は、同じノードに存在する必要があります。

設計機能

単一のパッケージに、Symantec Product Authentication Service と Symantec Product Authorization Service の両方が含まれます。これは、Symantec Product Authorization Service リソースが Symantec Product Authentication Service リソースに依存する Symantec Cluster Server の Symantec Product Authentication Service サービス グループの構成と同じです。

Symantec Product Authentication Service は Service[0] として追加され、Symantec Product Authorization Service は Service[1] として追加されます。認可サービスは、認証サービスの構成後にインストールおよび構成できます。

リソースの依存関係

HP ServiceGuard には、依存関係ツリーという概念はありません。その代わり、HP ServiceGuard では、サービスが起動する前に、パッケージに属する LV および IP アドレスが起動します。また、サービスは、リストされている順序で起動します。オフラインは、この逆の順序で行われます。

HP ServiceGuard クラスタでの認証サービスの構成

この項では、SGManager GUI を使用して HP ServiceGuard クラスタで認証サービスを構成する手順について説明します。

構成方法

1. クラスタ パッケージ vxss_service を作成します。
2. パッケージに、Symantec Product Authentication Service と Symantec Product Authorization Service の両方を追加します。
3. サービスに応じて、次のコマンドを実行します。
   - `/opt/VRTSat/bin/vxatd`
   - `/opt/VRTSaz/bin/vrtsaz`
4. サービスの 1 つで障害が発生したときに HP ServiceGuard がすぐに別のノードにパッケージをフェイルオーバーできるように、再試行間隔を 0 に設定します。
5. Symantec Product Authentication Service と Symantec Product Authorization Service の IP アドレスと LV を設定します。認証サービスが共有する LV は `/var/VRTsat` にマウントされるように設定する必要がありま

す。また、認可サービスが共有する LV は /var/VRTsaz/shared にマウントされるように設定する必要があります。

6 認証サービスの場合、/var/VRTSat フォルダ全体を一時的な場所にコピーします。認証サービスが共有する LV をマウントして、このフォルダを /var/VRTSat にコピーします。次のファイルを編集します。
/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
Security¥Authentication¥Authentication Broker¥ClusterName
キーの値にクラスタ名 (共有 IP アドレスの DNS 名) を設定します。この設定には、/opt/VRTSat/bin/vssregctl コマンドを使用します。

7 認可サービスの場合、/var/VRTSaz/objdb フォルダ全体を一時的な場所にコピーします。認可サービスが共有する LV をマウントして、このフォルダを /var/VRTSaz/shared にコピーします。

これで、クラスタ上でパッケージを起動する用意ができました。

5

管理コンソールの実行

この章では、インストールおよび構成した後で、管理コンソールを実行する方法について説明します。

内容は次のとおりです。

コンソールを使用して実行できる作業については、『VERITAS Security Services 管理者ガイド』を参照してください。

管理コンソールの実行の準備

注意：インストールした認証サービス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。

Symantec Product Authentication Service 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
  - 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
  - `libAtWrapper.so`、`AtWrapper.jar`、`vssatgui.jar`、`VxHelpViewer.jar` および `VxHelpViewerl10n.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
- 次のものがインストールされている必要があります。
  - 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は、Symantec Product Authentication Service および認可クライアントの両方をインストールします。コンソールでは認可クライアント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、それに応じて認可サービスの画面が表示されます。
  - 認証専用モードでコンソールを実行する場合は、Symantec Product Authentication Service をインストールします。
  - クライアント専用モードで実行 (クレデンシャル領域だけを参照および使用) する場合は、認証クライアントをインストールします。

認証コンソールのセキュリティの理解

Symantec Product Authentication Service 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

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。

管理コンソールを介して認証サービスを管理するには、Symantec Product Authentication Service 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。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。

Authentication 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、Symantec Product Authentication Service 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。
そのマシンの管理コンソールから管理作業を実行します。管理コンソールを介して認証サービスをリモート管理することはできません。

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」メニューからの選択。
    <*authentication install directory*>¥bin ディレクトリの runvssatgui.bat の実行。
- 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。

メモ : Symantec Product Authorization Service をインストールして認証 + 認可モードで実行する場合は、『Symantec Product Authorization Service インストール ガイド』を参照してください。

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。
- 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。

管理作業の実行

認証サービスの管理作業の詳細については、『Symantec Product Authentication Service 管理者ガイド』を参照してください。

A

UNIX の OS ツールを使用したインストール

このマニュアルの第 2 章「標準インストール手順」では、すべてのプラットフォームに対して同じ手順を使用して、Symantec Product Authentication Service を UNIX プラットフォームにインストールする方法について説明しました。この付録では、ユーザーが UNIX システムに固有の OS ツールを使用する場合を想定して、OS ツールを使用したインストール方法について説明します。

UNIX の OS ツールを使用した認証サービスのインストール

この項では、次の UNIX システムに、プラットフォーム固有の OS ツールを使用して Symantec Product Authentication Service をインストールする方法について説明します。

- AIX
- HP-UX
- Linux
- Solaris
- Tru64

UNIX の OS ツールを使用すると、Solaris、Linux および Tru64 では、クライアント専用モードで認証サービスをインストールできます。

AIX への認証サービスのインストール

この項では、Symantec Product Authentication Service を AIX プラットフォームにインストールする方法について説明します。

認証サービスをインストールする方法

1. 現在 root ユーザーであることを確認します。
2. 認証サービスが実行されている場合は、これを停止します。次に例を示します。
   ```
   $ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
   '{print $2}'`
   ```
3. 以前の認証サービスをアンインストールします。
   ```
   $ installp -u VRTSat
   ```
4. インストール CD が /cdrom にマウントされている場合、ディレクトリをインストール CD の /cdrom/aix/authentication/pkgs に移動します。
5. 認証サービスをインストールします。
   ```
   $ installp -aXd ./VRTSat.image VRTSat
   ```
6. 認証サービスの構成および起動については、第 2 章「標準インストール手順」を参照します。第 2 章「標準インストール手順」に記載されている方法は、すべての UNIX プラットフォームに適用されます。

HP-UX への認証サービスのインストール

この項では、Symantec Product Authentication Service を HP-UX プラットフォームにインストールする方法について説明します。

インストールする方法

1. 現在 root ユーザーであることを確認します。
2. 認証サービスが実行されている場合は、これを停止します。次に例を示します。
   ```
   $ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
   '{print $2}'`
   ```
3. 以前の認証サービスをアンインストールします。
   ```
   $ swremove VRTSat
   ```
4. インストール CD が /cdrom にマウントされている場合、ディレクトリをインストール CD の /cdrom/hpux/authentication/pkgs に移動します。
5. 認証サービスをインストールします。
   ```
   $ swinstall -s /cdrom/hpux/authentication/pkgs/VRTSat
   VRTSat
   ```
6. 認証サービスの構成および起動については、第 2 章「標準インストール手順」を参照します。第 2 章「標準インストール手順」に記載されている方法は、すべての UNIX プラットフォームに適用されます。

Linux への認証サービスのインストール

この項では、Symantec Product Authentication Service を Linux プラットフォームにインストールする方法について説明します。

インストールおよび実行する方法

1. 現在 root ユーザーであることを確認します。
2. 認証サービスが実行されている場合は、これを停止します。次に例を示します。

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
'{print $2}'`
```

3. 以前の認証サービスをアンインストールします。

```
$ rpm -e --nodeps VRTSatServer
$ rpm -e --nodeps VRTSatClient
```

4. インストール CD が /cdrom にマウントされている場合、ディレクトリをインストール CD の /cdrom/linux/authentication/rpms に移動します。
5. 認証サービスをインストールします。

```
$ rpm -i *.rpm
```

6. 認証サービスの構成および起動については、第 2 章「標準インストール手順」を参照します。第 2 章「標準インストール手順」に記載されている方法は、すべての UNIX プラットフォームに適用されます。

Solaris への認証サービスのインストール

この項では、Solaris システムでの Symantec Product Authentication Service のインストール、実行およびアンインストール方法について説明します。

インストールする方法

1. 現在 root ユーザーであることを確認します。
2. 認証サービスが実行されている場合は、これを停止します。次に例を示します。

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
'{print $2}'`
```

3. 以前の認証サービスをアンインストールします。

```
$ pkgrm -n VRTSat
```

4. インストール CD が /cdrom にマウントされている場合、ディレクトリをインストール CD の /cdrom/sun/authentication/pkgs に移動します。
5. 認証サービスをインストールします。

```
$ pkgadd -d . VRTSat
```

6 認証サービスの構成および起動については、第 2 章「標準インストール手順」を参照します。第 2 章「標準インストール手順」に記載されている方法は、すべての UNIX プラットフォームに適用されます。

Tru64 への認証サービスのインストール

この項では、Symantec Product Authentication Service を Tru64 システムにインストールする方法について説明します。

インストールする方法

1 現在 root ユーザーであることを確認します。

2 認証サービスが実行されている場合は、これを停止します。次に例を示します。

```
$ kill -9 `ps -ef | grep vxatd | grep -v
grep | awk '{print $2}'`
```

3 以前の認証サービスをアンインストールします。

a ホストに認証サービスがインストールされている場合は、最初に、そのバージョンを確認します。

```
$ setld -i | grep VATSER
```

認証サービスがホストにインストールされている場合は、次のように表示されます。バージョンは、VATSER の後の 3 桁の数字です。次の例では、バージョンは 427 です。

```
VATSER427 installed VERITAS Authentication Server
(Version 4.1.1.17)
```

b 次のコマンドを発行して、認証サービスを削除します。

```
$ setld -d VATSER### VATCLI###
```

には、バージョン番号を指定します。

4 インストール CD が /cdrom にマウントされている場合、ディレクトリをインストール CD の /cdrom/osf1/authentication/pkgs に移動します。

5 認証サービスをインストールします。

```
$ setld -l ./VRTSat
```

6 認証サービスの構成および起動については、第 2 章「標準インストール手順」を参照します。第 2 章「標準インストール手順」に記載されている方法は、すべての UNIX プラットフォームに適用されます。

B

Storage Foundation and High Availability Solutions インストーラを使用した Symantec Product Authentication Service のインストール

この付録では、Storage Foundation and High Availability Solutions 製品のインストーラへのアクセス方法および使用方法について説明します。Symantec Product Authentication Service を配備する方法の決定に役立つ基本情報、概念および定義については、システム要件、推奨事項およびプラットフォーム固有のインストール手順に関する章を参照してください。

様々なオプションを考慮した後で、製品のインストーラを使用してインストールまたはアンインストールを実行します。

ソフトウェア ディスクのマウント

Veritas ソフトウェア ディスクをマウントする方法、およびインストールを実行する前にセキュア シェルを設定する方法については、『Storage Foundations and High Availability Solutions スタート ガイド』を参照してください。

Root + AB モードでのインストールまたはアップグレード

Root + AB モードで Symantec Product Authentication Service をインストールまたはアップグレードする方法

1. UNIX コンソールを開いて、root ユーザーとしてターゲット ホストにログインします。
2. Symantec Product Authentication Service のインストールを実行する前に、この製品を使用するすべてのアプリケーションまたはサービスを終了します。
3. Veritas ソフトウェア ディスクを挿入およびマウントします。
4. ソフトウェア ディスクのマウント ポイント配下にある適切なオペレーティング システム ディレクトリに移動して、製品のインストーラを起動します。
   ```
   ./installer
   ```
5. 製品のリストから、「Symantec Product Authentication Service」を選択します。
6. タスク メニューから、「製品のインストールまたはアップグレード (Install/Upgrade a Product)」を選択します。
7. 画面に表示されるモード選択用の情報を確認します。
8. 「Root + AB モード (Root + AB mode)」モードを選択します。
9. システム名を入力します。
10. 表示されたインストール対象のパッケージのリストを確認します。
11. [Return] キーを押して続行します。
12. 進捗バーを確認します。インストールが完了したことを通知するメッセージが表示されます。構成するかどうかを指定します。
13. ホスト *host* 上のルート ブローカのルート ブローカ管理者のパスワードを入力します。
14. ホスト *host* 上の認証ブローカの認証ブローカ管理者のパスワードを入力します。

    メモ: インストールが完了したら、認証ブローカ管理者のパスワードを変更します。

15. Symantec Product Authentication Service プロセスを今すぐ起動するかどうかを指定します。

16 応答ファイル内のパスワードを暗号化するには、5 文字以上の文字列を指定する必要があります。暗号化鍵として使用する文字列を 5 文字以上で入力します。この鍵は、セキュリティ保護されたファイルに保存しておく必要があります。生成された応答ファイルを再度使用する場合に、`-enckeyfile` オプションを使用して参照します。

17 [Return] キーを押して続行します。

18 様々なファイルの位置を通知するメッセージを確認します。このメッセージが表示されたら、インストールは完了です。

Root モードでのインストールまたはアップグレード

Root モードで Symantec Product Authentication Service をインストールまたはアップグレードする方法

1 UNIX コンソールを開いて、root ユーザーとしてターゲット ホストにログインします。

2 Symantec Product Authentication Service のインストールを実行する前に、この製品を使用するすべてのアプリケーションまたはサービスを終了します。

3 Veritas ソフトウェア ディスクを挿入およびマウントします。

4 ソフトウェア ディスクのマウント ポイント配下にある適切なオペレーティング システム ディレクトリに移動して、製品のインストーラを起動します。

```
./installer
```

5 製品のリストから、「Symantec Product Authentication Service」を選択します。

6 タスク メニューから、「製品のインストールまたはアップグレード (Install/Upgrade a Product)」を選択します。

7 画面に表示されるモード選択用の情報を確認します。

8 「Root モード (Root mode)」を選択します。

9 システム名を入力します。

10 表示されたインストール対象のパッケージのリストを確認します。

11 [Return] キーを押して続行します。

12 進捗バーを確認します。インストールが完了したことを通知するメッセージが表示されます。構成するかどうかを指定します。

13 ホスト *host* 上のルート ブローカのルート ブローカ管理者のパスワードを入力します。

14 Symantec Product Authentication Service プロセスを今すぐ起動するかどうかを指定します。

15 応答ファイル内のパスワードを暗号化するには、5 文字以上の文字列を指定する必要があります。暗号化鍵として使用する文字列を 5 文字以上で入力します。この鍵は、セキュリティ保護されたファイルに保存しておく必要があります。生成された応答ファイルを再度使用する場合に、*-enckeyfile* オプションを使用して参照します。

16 [Return] キーを押して続行します。
様々なファイルの位置を通知するメッセージを確認します。このメッセージが表示されたら、インストールは完了です。

AB モードでのインストールまたはアップグレード

AB モードで Symantec Product Authentication Service をインストールまたはアップグレードする方法

1 UNIX コンソールを開いて、root ユーザーとしてターゲット ホストにログインします。

2 Symantec Product Authentication Service のインストールを実行する前に、この製品を使用するすべてのアプリケーションまたはサービスを終了します。

3 Veritas ソフトウェア ディスクを挿入およびマウントします。

4 ソフトウェア ディスクのマウント ポイント配下にある適切なオペレーティング システム ディレクトリに移動して、製品のインストーラを起動します。
`./installer`

5 製品のリストから、「Symantec Product Authentication Service」を選択します。

6 タスク メニューから、「製品のインストールまたはアップグレード (Install/Upgrade a Product)」を選択します。

7 画面に表示されるモード選択用の情報を確認します。

8 「AB モード (AB mode)」を選択します。

9 進捗バーを確認します。ルート ブローカのホスト名を入力します。完全修飾されたホスト名である必要があります。たとえば、machinename.company.com と入力します。

10 認証サービスで PBX が使用されている場合は、ブローカ ポート 1556 を入力します。使用されていない場合は、2821 を使用します。

11 ルート ブローカのハッシュを含むファイルへの完全なパスを入力します。たとえば、`/tmp/root_hash` と入力します。

12 表示された入力値のリストを確認します。

13 入力した値が正しいことを確認します。

14 認証ブローカの識別情報を入力します。
これは、ルート ブローカで識別情報を準備したときに作成した AB の名前です。

15 認証ブローカの識別情報のパスワードを入力します。

メモ: インストールが完了したら、認証ブローカ管理者のパスワードを変更します。

16 認証ブローカの識別情報のドメイン名を入力します。たとえば、`root@machinename.company.com` と入力します。

17 表示された入力値のリストを確認します。

18 入力した値が正しいことを確認します。

19 ホスト *host* 上の認証ブローカの認証ブローカ管理者のパスワードを入力します。

20 Symantec Product Authentication Service プロセスを今すぐ起動するかどうかを指定します。

21 応答ファイル内のパスワードを暗号化するには、5 文字以上の文字列を指定する必要があります。暗号化鍵として使用する文字列を 5 文字以上で入力します。この鍵は、セキュリティ保護されたファイルに保存しておく必要があります。生成された応答ファイルを再度使用する場合に、`-enckeyfile` オプションを使用して参照します。

22 [Return] キーを押して続行します。

23 様々なファイルの位置を通知するメッセージを確認します。このメッセージが表示されたら、インストールは完了です。

Symantec Product Authentication Service のアンインストール

Symantec Product Authentication Service をアンインストールする方法

1 製品のリストから、「Symantec Product Authentication Service」を選択します。

2 タスク メニューから、「製品のアンインストール (Uninstall a Product)」を選択します。

3 アンインストールするシステムの名前を入力します。

4 アンインストールすることを確認します。

インストール完了の確認

インストールが完了したことを確認する方法 (次のいずれかを実行)

1 プロセスを起動している場合は、次のプロセス状態コマンドを入力して、認証サービスが実行されていることを確認します。

ps -ef | grep vxatd

次のような内容が出力されます。

```
root 24369 1 0 18:48:59 ?0:01 vxatd
```

2 起動していない場合は、認証サービス プロセスを起動します。

/opt/VRTSat/bin/vxatd

C

Web コンソールを使用するための構成

多くのリソース管理アプリケーションに対して、Symantec 社は Web コンソールを提供しています。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 コンソールでは認証の方法が異なるため、説明しておく必要があります。

この付録では、Web コンソールを使用するときに製品 Web クレデンシャルが必要となる理由について説明します。また、Veritas Enterprise Administrator と Web コンソールを併用するための構成例についても示します。

製品 Web クレデンシャルが必要となる場合とその理由

通常の製品クレデンシャルは、ユーザー名 / パスワードを提供すると、ブローカから取得できるデジタル証明書です。これは、そのブローカで検証することができます。製品クレデンシャルは、秘密鍵と公開鍵の 2 つの鍵で構成されます。

両方の鍵は、クライアントがサービスへの SSL 接続を確立する場合に必要となります。通常、エンティティが認証を求めると、Symantec ライブラリは公開鍵のみを戻します。秘密鍵はライブラリ自体によって保護されています。

ただし、Web コンソールでは、クライアントはブラウザになります。このため、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。この場合、ブラウザの代わりに Web コンソールがクレデンシャルを取得する必要があります。

ある Web コンソールから別の Web コンソールにシングル サインオンを実行するには、最初の Web コンソールによって取得されたクレデンシャルを、もう一方の Web コンソールの URL の末尾に追加する必要があります。この URL をクリックすると、クレデンシャルは HTTP 要求の一部として 2 番目の Web コンソールに送信されます。2 番目の Web コンソールは、クレデンシャルを抽出し、プリンシパルを認証します。

ただし、次の 2 つの事項を考慮する必要があります。

- 別々の Web コンソールが、異なるマシンで動作する可能性があります。
- クレデンシャルは、公開鍵のみで構成されています。このため、プリンシパルの代わりにサービスとのセキュリティ保護された接続を確立するために、クレデンシャル自体が 2 番目の Web コンソールで使用されることはありません。

これらの理由により、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取得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。

製品 Web クレデンシャル

製品 Web クレデンシャルは、Symantec ライブラリ内に対応する秘密鍵が存在しないことをライブラリに示します。この製品 Web クレデンシャルは、単独で使用することはできません。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。

プロキシ権限を持つクレデンシャル

プロキシ権限を持つクレデンシャルは、構成中に Web コンソールによって取得されます。これは、コンソールがアクセスするように設定されている各サービスに対する、特殊な長期間のクレデンシャルです。この特殊な形式のクレデンシャルは、プロキシ権限を持っています。つまり、このプロキシ権限を持つクレデンシャルによって、Web コンソール プロキシを実際のユーザーの代わりに使用できます。これは、次のように行われます。

- ユーザーがログインすると、Web コンソールは、最初に自身のクレデンシャルを使用して、サービスへのセキュリティ保護された接続を確立します。
- 次に、セキュリティ保護されたチャネルを介して、ユーザーの製品 Web クレデンシャルを転送します。このようにして、サービスは、アクセスを試行しているプリンシパルを認識し、それに応じて認可を適用します。

例 : VEA にアクセスするための Web コンソールの構成

次の手順では、Web コンソールの構成処理について説明します。この例では、Veritas Enterprise Administrator と連携できるよう構成することを想定しています。

VEA を使用するために Web コンソールを構成する方法

1. Symantec Product Authentication Service に対応した、Web コンソールを備えたサービスをインストールする場合は、プロキシ権限を持つ認証ブローカにユーザーを作成する必要があります。たとえば、Veritas Enterprise Administrator をインストールする場合は、「veawebconsole」というアカウントを認証ブローカのプライベート ドメインに作成し、そのアカウントにプロキシ権限を割り当てます。ユーザーは、このアカウントのパスワードを覚えておく必要があります。
2. 同じシステムまたはリモート システムの Web コンソールを、サービスにアクセスするように構成すると、コンソールによって、サービスをインストールしたときに作成したプロキシ アカウント veawebconsole の識別情報 / パスワードの入力が求められます。

メモ : Web クライアントと Web サーバー間の最初の通信、つまりクライアントによるユーザー名 / パスワードの転送には、セキュリティ保護されたチャネル (https) を使用する必要があります。

---

3. Web コンソールは、提供された識別情報 / パスワードを使用して、そのサービスの認証ブローカから長期間のクレデンシャルを取得します。このクレデンシャルはプロキシ権限が付加されており、サービスへの SSL 接続を確立するために使用できます。
4. プロキシ権限を持つクレデンシャルを取得すると、Web コンソールはパスワードを破棄して、サービスにアクセスするように設定されます。1 つのコンソールが、異なる ROOT 階層で複数のサービスにアクセスするように設計されている場合、サービスごとにこのクレデンシャルを取得する必要があります。

Web コンソールを使用したアプリケーションへのアクセス

Web コンソールが、VEA にアクセスするようにすでに構成されている場合、次の処理を行う必要があります。

1. ユーザーが初めてコンソールにアクセスするときに、コンソールによって、サービスへのアクセスが認可されている有効な識別情報 / パスワードの入力が求められます。
2. コンソールはサービスの認証ブローカに問い合わせ、指定された識別情報 / パスワードを提供してユーザーの製品 Web クレデンシャルを取得します。
3. コンソールは、ユーザーの製品 Web クレデンシャルではなく、コンソール自身のプロキシ権限を持つクレデンシャルを使用して、サービスへの SSL 接続を確立します。
4. サービスはその接続を受け入れて、コンソールのプロキシ権限を持つクレデンシャルを確認します。クレデンシャルから、Web コンソールがユーザーの代わりに接続を試行していることがわかっているため、サービスは、コンソールが次にユーザーの製品 Web クレデンシャルを送信してくるまで待機します。
5. コンソールは、セキュリティ保護されたチャネルを使用して、ログインしたユーザーの製品 Web クレデンシャルを送信します。このデータが転送される実際の方法は、アプリケーション固有です。
6. サービスは、`vrtsAtWebCredentialVerify()` メソッドを使用して、製品 Web クレデンシャルを確認します。確認が成功すると、製品 Web クレデンシャルから情報を抽出します。この情報に基づいて、適切な認可が適用されます。

用語集

メモ: この用語集では、Symantec Product Authentication Service および Symantec Product Authorization Service の両方に該当する用語について説明します。

AT

CLI コマンドおよび特定の画像で Authentication を示す略語。

Authenticated Principals

すべての認証されたプリンシパルを含む特別な認可グループ。このグループは、認証されているかどうかにかかわらず使用可能なすべてのプリンシパルを保持する Everyone グループとは異なります。

AZ

CLI コマンドおよび特定の画像で Authorization を示す略語。

CLI

コマンドライン インタフェース。

Everyone

認証されているかどうかにかかわらず、すべてのプリンシパルを含む特別な認可グループ。

OS グループ (OS Group)

「認証グループ (Authentication Group)」を参照。

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。

Symantec Product Authorization Service
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 社製品に認可決定サービスを提供するコンポーネント。

アカウント名 (Account Name)
「認証プリンシパル」のこと。

アクセス制御情報のデータ リポジトリ (Access Control Information Data Repository)
認可決定サービスをサポートするために必要な情報を含む、認可サービスのデータベースのマスター コピー。このデータベースには、リソース管理アプリケーションによって通知されるリソースのデータ、およびセキュリティ管理者によって設定されたアクセス制御ポリシーのデータが含まれます。アクセス制御情報のデータ リポジトリは、Symantec Product Authorization Service の初期アクセス制御ポリシーを定義するアクセス制御リストと関連付けられています。

アクセス制御ポリシー (Access Control Policy)
リソースを不正使用から保護する方法を定義する規則の集合。特に、セキュリティ保護されたオブジェクトに対してセキュリティ プリンシパルが持つ権限を定義します。アプリケーション リソースに対してアクセス制御ポリシーを設定するには、まず、アクセス制御ポリシーによって影響を受ける、アプリケーション固有のリソース コレクションを作成します。次に、そのコレクションにアクセス制御リストを関連付けて、コレクション内のセキュリティ保護されたすべてのオブジェクトに対してセキュリティ プリンシパルが持つ権限を定義します。

アクセス制御リスト (Access Control List)
0 (ゼロ) または 1 つ以上のアクセス制御エントリの集まり。エントリ全体で、セキュリティ保護が可能なオブジェクトまたはその属性情報に適用する権限および保護を定義します。

アクセス制御リスト エントリ (Access Control List Entry)
アクセス制御リスト内の個々の規則。アクセス制御リスト エントリは、個々の認証プリンシパルに対して付与される権限および拒否される権限を示します。

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。

アプリケーション権限空間 (Application Permission Space)
個々のアプリケーション ドメインに関連するすべての権限およびそれらの権限を適用するリソースのタイプを識別する概念。たとえば、NetBackup と SANPoint Control の両方を実行している場合、NetBackup に関連する権限およびリソースは NetBackup のアプリケーション権限空間に存在することになります。

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。

オブジェクト レベルの認可 (Object-Level Authorization)
アクセス決定の形式の 1 つ。特定のセキュリティ プリンシパル (要求元) が、特定のオブジェクト (リソース コレクション) 上で特定の操作に対して認可されているか (権限) が判断されます。リソース コレクションには、一連のすべてのオブジェクトまたは 1 つのオブジェクトが含まれる場合があります。オブジェクト レベルの認証を使用すると、認可をきめ細かく行うことができます。

管理アクセス制御情報 (Administrative Access Control Information)
リソース管理アプリケーションによって通知されるリソースではなく、Symantec Product Authorization Service 自身のリソースに関連するアクセス制御情報のデータ リポジトリの一部。リソース管理アプリケーションによって通知される、リソースに関連するアクセス制御情報のデータ リポジトリは、サービス アクセス制御情報のデータ リポジトリと呼ばれます。

管理コンソール (Administration Console)
Authentication および Authorization の両方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、様々なコンポーネントの位置、信頼関係、プラグイン、Symantec プライベート ドメインを表示する目的で使用します。

権限 (Permission)
セキュリティ保護された特定のオブジェクトに対してなんらかの操作を実行するために、セキュリティ プリンシパルに対して付与する必要がある一意の名称が付与された正式な承諾 (許可)。すべての権限はアプリケーション権限空間で定義されます。すべてのアプリケーション権限空間で一意に名前付けされます。

権限セット (Permission Set)
0 (ゼロ) または 1 つ以上の権限からなる名前付きのコレクション。アクセス制御リスト エントリ内では 1 つの権限として処理されます。権限セットを使用すると、複数の権限を 1 つずつ指定しなくても設定できます。

権限の暗黙的な拒否 (Implicit Denial of Permission)
権限が明示的に拒否されているためではなく、権限が明示的に付与されていないために、セキュリティ保護されたオブジェクトに対する権限が拒否されること。

権限の明示的な拒否 (Explicit Denial of Permission)
セキュリティ保護された特定のオブジェクト上で特定の機能を実行するための権限を明示的に拒否すること。

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。

サービス アクセス制御情報 (Service Access Control Information)
リソース管理アプリケーションによって通知されるリソースに関連するアクセス制御情報のデータ リポジトリの一部。データ リポジトリ内のその他の情報は、Symantec Product Authorization Service 自身のリソースに関連し、管理アクセス制御情報のデータ リポジトリと呼ばれます。

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。

事前定義済みの権限セット (Pre-Defined Permission Set)
アプリケーション権限空間で定義されている編集不可能な権限セット。特定のポイント製品またはアプリケーションに固有の機能の役割を定義します。

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。

所有者 (Owner): セキュリティ保護されたオブジェクト
セキュリティ保護されたオブジェクトまたはコレクションを保護するアクセス制御リストを変更する権限が付与されたセキュリティ プリンシパル。

スレッド (Thread)
セキュリティ保護されたプリンシパルの代わりに機能し、セキュリティ保護されたオブジェクト上での操作の実行権限を付与または拒否することができるプロセスまたはプロセスの一部。

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。

セキュリティ管理者 (Security Administrator)
Symantec Product Authentication Service および Symantec Product Authorization Service によって保護されるリソース上のアクセス制御ポリシーの設定および管理に責任を有するユーザー。このユーザーは、リソース コレクション上またはアクセス制御情報のデータ リポジトリ自身のアクセス制御リストを変更するために必要な権限を持っています。セキュリティ管理者の権限は、ポイント製品の特定のインスタンスに委譲することができます。

セキュリティ記述子 (Security Descriptor)
セキュリティ保護されたオブジェクトについてのセキュリティ情報を保持するデータ構造。オブジェクトの所有者のセキュリティ識別子が含まれます。セキュリティ保護されたオブジェクトに対してアクセス制御規則が構成されている場合、セキュリティ記述子には随意アクセス制御リストと呼ばれる固有のアクセス制御リストも含まれます。随意アクセス制御リストには、セキュリティ保護されたオブジェクトへのアクセスを許可または拒否されているプリンシパルに対するセキュリティ識別子が含まれます。

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。

セキュリティ プリンシパル (Security Principal)
セキュリティ保護されたオブジェクトに対する権限の付与または拒否を、セキュリティ管理者が行う対象となるエンティティ。セキュリティ プリンシパルには、認証プリンシパル、認証グループまたは認可グループがあります。セキュリティ プリンシパルは、すべてが検証できるわけでもなく、その処理の責任を必ずしも負うわけではない点で、認証プリンシパルとは異なります。

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。

セキュリティ保護されたオブジェクト (Secured Object)
Symantec Product Authorization Service が認可決定を行うことができるオブジェクト。このオブジェクトには、アクセス制御ポリシーの設定に使用する内部オブジェクトや、リソース管理アプリケーションによって保護する必要があるオブジェクトが含まれます。後者のオブジェクトはリソースと呼ばれ、Symantec Product Authorization Service に通知して存在が認識されるようにする必要があります。

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。

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。

ドメイン (Domain)
「認証プライベート ドメイン (Authentication Private Domain)」を参照。
「認証ドメイン (Authentication Domain)」および「認証プライベート ドメイン (Authentication Private Domain)」を参照。

内部オブジェクト (Internal Object)
アクセス制御情報のデータ リポジトリに格納される、プログラムで使用するエンティティ。内部オブジェクトの種類には、認証ドメイン、認可グループ、権限セットおよびリソース コレクションがあります。

認可 API (Authorization API)
アプリケーション クライアントによって、Symantec Product Authorization Service にアクセスする際に使用されるアプリケーション プログラム インタフェース。ヘッダー ファイル、ライブラリおよびその他のコンポーネントで構成されます。これらはアプリケーション ホスト上にインストールされている必要があります。

認可グループ (Authorization Group)
別の認証ドメインに存在するメンバーを含めることができるグループの形式。認可グループは、異なるドメインにおいて、同等の権限を持つグループを、名前を付けて定義することができます。このグループは Symantec Product Authorization Service でサポートされ、他の認証ドメインでは同等になることはありません。

認可権限空間 (Authorization Permission Space)
その他のリソース管理アプリケーションではなく、Symantec Product Authorization Service 自身に関連するすべての権限を保持する特別な権限空間。特に、アクセス制御リストを管理するために必要な権限およびアクセス制御情報のデータ リポジトリにリソースを通知するための権限を定義します。

認可ライブラリ (Authorization Library)
Symantec Product Authorization Service の一部。認可サービス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。

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。

認証ドメイン (Authentication Domain)
認証プリンシパルに対して一連の識別情報を定義したもの。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+、NTLM、Active Directory ドメイン内の名前などです。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。

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。

プリンシパル (Principal)
「認証プリンシパル (Authentication Principal)」を参照。
「認証プリンシパル (Authentication Principal)」および「セキュリティ プリンシパル (Security Principal)」を参照。

分散認可 (Distributed Authorization)
登録されている最上位レベルのリソース コレクションのアクセス制御情報データをマスター認可サーバーから定期的にコピーして、ローカルにキャッシュするサービス。これによって、ローカル認可決定要求の処理の速度が向上し、ネットワークの独立性が提供されます。ローカルにキャッシュされたデータは変更できません。変更は、アクセス制御情報のマスター データ リポジトリに対して行われます。

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。

マスター認可サービス (Master Authorization Service)
アクセス制御情報のデータ リポジトリの保持および管理を行います。

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。

有効な権限 (Effective Permission)
指定および継承されたグループ メンバーシップや制約をすべて評価した後に、セキュリティ プリンシパルがセキュリティ保護されたオブジェクトに対して実際に所有する権限のこと。

リソース (Resource)
リソース管理アプリケーションによって Symantec Product Authorization Service に通知される、一意に識別されるオブジェクト。アクセス制御ポリシーを設定してリソースが表すエンティティを保護できます。セキュリティ保護されたオブジェクトという用語には、リソースの概念が含まれます。

リソース管理アプリケーション (Resource Management Application)
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。

リソース管理アプリケーション認可グループ (Resource Management Applications Authorization Group)
Symantec 社のすべてのリソース管理製品の識別情報を含めるために作成する特別な認可グループ。このグループには、アクセス制御情報のデータ リポジトリにリソースを通知する権限が付与されます。

リソース管理クライアント (Resource Management Client)
リソース管理アプリケーションを使用し、Symantec Product Authorization Service によってリソースへのアクセスが制御および保護されているエンティティ。

リソース コレクション (Resource Collection)
コレクションに関連付けられたアクセス制御リストによって定義されている、同じアクセス制御ポリシーの影響を受けるリソースのコレクション。リソース コレクションを使用すると、複数のセキュリティ保護されたオブジェクトを 1 つずつ指定する必要がなくなります。これにより、定義するアクセス制御ポリシーの数を削減できます。リソース コレクションにはサブコレクションを含めることができます。サブコレクションは、親のアクセス制御リストを継承しますが、継承されたアクセス制御リストは拡張または変更可能です。

リソース識別子 (Resource Identifier)
特定の形式のリソースを識別し、2 つの異なるアプリケーションによって存在が通知される場合でも、作成されたリソース オブジェクトのコピーが 1 つだけであることを保証する一意の文字列。

リソース タイプ (Resource Type)
リソースが属するカテゴリの定義に使用する、説明的な一意の文字列 (DISK_ARRAY、TAPE_DRIVE など)。

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。

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。

ローカル認可サービス (Local Authorization Service)
アクセス制御情報のデータ リポジトリ内に存在するポリシー情報のコピーを保持します。この情報はマスター認可サーバーからインポートされ、正確性を保つため、定期的に同期化されます。

索引

る