



SAP Control Center for Data Assurance

3.3

ドキュメント ID：DC01899-01-0330-01

改訂：2014年2月

Copyright © 2014 by SAP AG or an SAP affiliate company. All rights reserved.

このマニュアルの内容を SAP AG の明示的許可を得ずに、いかなる手段によっても、複製、転載することを禁じます。ここに記載された情報は事前の通知なしに変更されることがあります。

SAP AG およびディストリビュータが販売しているソフトウェア製品には、他のソフトウェアベンダー独自のソフトウェアコンポーネントが含まれているものがあります。国内製品の仕様は変わることがあります。

これらの資料は SAP AG および関連会社 (SAP グループ) が情報のみを目的として提供するものであり、いかなる種類の表明または保証も行わないものではなく、SAP グループはこの資料に関する誤りまたは脱落について責任を負わないものとします。SAP グループの製品およびサービスに関する保証は、かかる製品およびサービスに付属している明確な保証文書がある場合、そこで明記されている保証に限定されます。ここに記載されているいかなる内容も、追加保証を構成するものとして解釈されるものではありません。

ここに記載された SAP および他の SAP 製品とサービス、ならびに対応するロゴは、ドイツおよび他の国における SAP AG の商標または登録商標です。その他の商標に関する情報および通知については、<http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> を参照してください。

目次

SAP Sybase Control Center for Data Assurance について	1
SAP Control Center for Data Assurance の新機能	2
ユーザインタフェース概要	2
ツールバーアイコン	3
ステータスアイコン	4
共通の表示オプション	5
Keyboard Shortcuts (キーボードショートカット)	8
SCC コンポーネントのバージョンの表示	10
スタイルと構文の規則	10
アクセシビリティ機能	11
SAP Control Center のアクセシビリティに関する情報	12
使用開始にあたって	13
評価のための簡易起動	13
運用環境での使用	20
SAP Control Center の起動	59
Windows での ODBC ドライバの登録	60
Windows での SAP Control Center の起動と停止	60
UNIX での SAP Control Center の起動と停止	64
メモリ使用の設定	68
scc コマンド	72
SAP Control Center へのログイン	76
SAP Control Center のログアウト	77
セキュリティのセットアップ	78
セキュリティ	79
Windows 認証の設定	80

UNIX 用のプラグ可能認証モジュール (PAM) の 設定	81
LDAP 認証モジュールの設定	83
LDAP または OS グループに対する SAP Control Center の役割のマッピング	93
パスワードの暗号化	95
ポートの設定	96
自動ログアウトタイマの設定	99
ユーザ承認	99
ログインまたはグループへの役割の割り当て ..	100
ログインまたはグループからの役割の削除	101
グループの追加	101
グループの削除	102
グループへのログインアカウントの追加	103
グループからのログインアカウントの削除	103
システムへのログインアカウントの追加	104
システムからのログインアカウントの削除	105
ユーザプロファイルの変更	106
ログイン、役割、グループ	106
設定	109
Data Assurance サーバのモニタリング設定	110
Data Assurance サーバの登録	110
一括登録のためのリソースのインポート	111
管理対象リソースのログインアカウントの認証	113
統計収集のセットアップ	114
統計について	115
Data Collections for SAP Replication Server Data Assurance のオプション	116
Data Assurance の主要パフォーマンス指標	117
Data Assurance サーバ、エージェント、デー タベース接続のステータス	117
エージェント接続の作成	117

データベース接続の作成	118
interface ファイルからの単一接続またはクラスタ接続の作成	120
オプションの設定手順	121
データローとスキーマの比較	123
comparesets	123
Compareset の作成	123
compareset の編集	124
Compareset の削除	125
すべての compareset の表示	126
データパーティション境界値の表示	126
Data Assurance のジョブ	126
ロー比較ジョブ	126
スキーマ比較ジョブ	134
Data Assurance のジョブの管理と実行	136
Data Assurance のジョブの実行	136
Data Assurance ジョブの削除	137
Data Assurance のジョブの比較を削除する	137
Data Assurance のすべてのジョブの表示	137
Data Assurance のジョブのステータスおよびレポートの表示	138
Data Assurance ジョブ履歴	138
管理とモニタ	139
リソースの可用性の表示: ヒートチャート	139
パフォーマンスカウンタのグラフ表示: 統計チャート	140
SAP Control Center の管理	142
管理コンソール	142
ジョブスケジューリング	144
リソース	149
パースペクティブ	152
ビュー	153

レポジトリ	155
ロギング	161
SAP Control Center コンソール	165
Data Assurance 環境の管理とモニタ	168
Data Assurance エージェント	169
データベース接続	171
Data Assurance サーバ	173
SAP Control Center for Data Assurance のトラブルシュー	
ティング	177
比較で LOB カラムの差異を検出できない	177
外部ソート・オプションの設定	177
DA サーバ・メモリ不足エラー	178
SAP Control Center の基本機能に関する問題	179
SAP Control Center が起動しない	179
ログインできない	179
ブラウザを再表示 ([F5] キー) するとログアウトしてしまう	180
十分な期間のパフォーマンス統計が表示されない	180
オンラインヘルプのリセット	180
データ収集が完了しない	181
起動時のメモリ警告	182
SCC メモリ不足エラー	182
用語解説: SAP Control Center for Data Assurance	183
索引	187

SAP Sybase Control Center for Data Assurance について

SAP Control Center for Data Assurance (DA) は、DA サーバ環境を管理および監視するための Web ベースのツールです。

SAP Control Center for Data Assurance により、可用性、履歴、リアルタイムのモニタリング機能を、その他の SAP 製品の管理モジュールと統合された拡張可能な Web アプリケーションの形態で使用できるようになります。さまざまな場所にある異機種リソースの共有統合管理、リアルタイムの可用性とパフォーマンスの通知、およびパフォーマンスと使用量の傾向を特定するインテリジェントツールを提供します。これらのツールはすべて、シンクライアントなリッチインターネットアプリケーション (RIA) を介して Web ブラウザから配布されます。

SAP Control Center for Data Assurance では、プライマリデータベースを 1 つ以上の複製データベースと比較できます。また、タスクスケジューリングもサポートし、各比較タスクを指定したスケジュールに基づいて実行できます。システムと構成の設定、タスク、タスク履歴を保存する独自の SAP SQL Anywhere データベースを使用して展開できます。自動調整オプションにより、DA ジョブの作成時に、ローの欠落、孤立、および矛盾が示されます。

DA モニタ、トポロジビュー、ヒートチャート、管理コンソールを使用して、サーバとエージェントを監視できます。比較タスクと統計の履歴レポートにより、データの不一致を監視でき、一般的な繰り返し発生する問題を特定できます。

SAP Control Center for Data Assurance を SAP Replication Server と統合して、大規模なテーブルを比較できます。SAP Control Center ウィザードを使用して Replication Server システムデータベース (RSSD) に基づいて DA ジョブを作成する場合は、レプリケーション定義やサブスクリプション情報がウィザードに自動的に読み込まれる、最適な設定のジョブを簡単に作成できます。

SAP Control Center for Data Assurance の新機能

新機能と拡張された機能のそれぞれの簡単な説明と、関連トピックへのリンクを記載しています。

表 1 : SAP Control Center for Data Assurance の新機能と機能強化

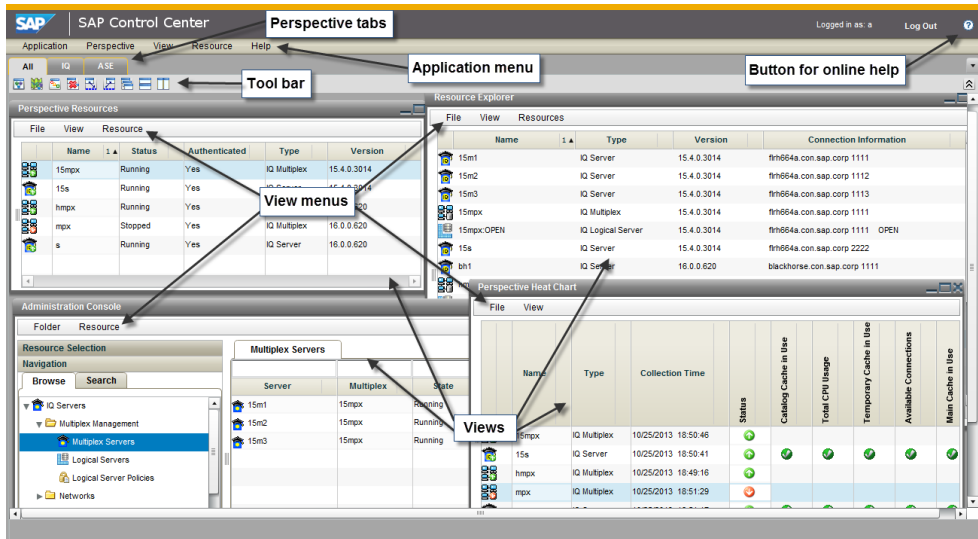
Feature	Topics
SCC for Data Assurance バージョン 3.2.8 SP01 で新しくサポートされたデータベースプラットフォーム: <ul style="list-style-type: none">• Microsoft SQL• IBM DB2	データベース接続の作成 (118 ページ) 『Replication Server Data Assurance Option ユーザーズガイド』の「異機種間での比較」を参照してください。

ユーザインタフェース概要

次の図には、SAP Control Center ユーザインタフェースの重要な要素がラベルで示されており、他のヘルプトピックで参照されている場合にそれらがどれであるかを識別できます。

ヒント：一部のビューメニューのオプションは、アプリケーションメニューのオプションと似ているか、まったく同じです ([View] や [Resource] など)。オプションの名前は同じでも、そのサブオプションは異なります。予期しない結果を防ぐには、ヘルプに説明されているように、アプリケーションまたはビューメニューのオプションを調べます。

図 1 : SAP Control Center ユーザーインターフェース







ツールバーアイコン

ビューを起動して管理する、SAP Control Center ツールバーのアイコンについて説明します。

表 2 : ツールバーアイコン

アイコン	名前	説明
	[Show/Hide Perspective Resources View]	この観点に登録されているリソースをリストする [Perspective Resources] ビューを表示または最小化する。
	[Launch Resource Explorer]	使用可能なリソース (登録済みと未登録の両方) をリストする Resource Explorer を開く。
	[Launch Heat Chart]	このパースペクティブに登録されているリソースのステータスの概要を示す、パースペクティブのヒートチャートを開きます。
	[Close All Open Views]	すべての開いているビューと最小化されているビューを閉じます。
	[Minimize All Open Views]	すべての開いているビューを最小化する。

アイコン	名前	説明
	[Restore All Mini-mized Views]	すべての最小化されているビューを元のサイズに戻す。
	[Cascade All Open Views]	開いているビューを互いに重ねます。
	[Tile All Open Views Vertically]	開いているビューを上下に並べます。
	[Tile All Open Views Horizontally]	開いているビューを左右に並べます。





ステータスアイコン



SAP Control Center では、アイコンを使用してリソースのステータスと主要パフォーマンス指標 (KPI) を示します。

[*Perspective Resources*] ビューとヒートチャートのリソースステータスアイコン
リソースステータスアイコンは、ヒートチャートの各リソースの状態を示します。さらに、ヒートチャートと [*Perspective Resources*] ビューの両方で、サーバアイコン上のバッジ (小さなオーバーレイ) として使用されます。また、[*Perspective Resources*] ビューには、バッジと同じステータスを英語のテキストで示す [Status] カラムがあります。

ヒートチャートでは、[Status] カラムのアイコンにマウスを合わせると、英語のテキストでステータスが表示されます。

表 3 : リソースステータスアイコン

アイコン	ステータス	説明
	Running	リソースは稼働中である。
	Pending	ステータスの変更中。再度クリックする必要がある。
	Stopped	リソースは停止している。
	Warning	リソースで有害な状況が発生している可能性がある。

アイコン	ステータス	説明
	Error	リソースで深刻な問題が発生した。
	Unknown	リソース使用不可能。ステータスを判断できない。

KPI ステータスアイコンとヒートチャート

ヒートチャートは、KPI ステータスアイコンを使用して、表示する KPI の状態を示します。

[Status] カラムの右側にある任意のカラムの KPI アイコンの上にマウスを合わせると、KPI の値が表示されます。

表 4 : KPI ステータスアイコン

アイコン	ステータス	説明
	Normal	パフォーマンス指標の値は、正常範囲内である。
	Warning	パフォーマンス指標の値は、警告範囲内である。
	Critical	パフォーマンス指標の値は、重大範囲内である。

共通の表示オプション

データ表示機能を使用して、リソースのステータスの表示、リソース名とタイプによるソートと検索、ステータス情報の並べ替えを行います。

カラムのオプション












[Perspective Resources] ビュー、Resource Explorer、管理コンソール、Alert Monitor、ヒートチャート、SAP Control Center (製品モジュールを含む) 内のその他のビューは、表形式のグリッド形式を使用して、管理対象リソースに関する情報を表示します。グリッド形式で提供されるオプションを使用して、表示されるデータをソートおよび整理できます。

表 5: カラムのソートオプション

ソートオプション	説明
カラムベースの単純なソート	カラム名をクリックすると、カラム名の昇順または降順で表がソートされます。カラムのソートタブの矢印(カラム名の右側にあります)は、データが昇順にソートされているときは上向き、データが降順にソートされているときは下向きです。
カラムベースのソート順を逆にする	カラムのソートタブをクリックすると、ソートの昇順と降順が切り替わります。
複数のカラムを対象にしたネストされたソート	プライマリソートのカラム名をクリックする。セカンダリソート以降のソートについては、カラムのソートタブをクリックする。以降のソートのカラムを適用順に選択する。ソートタブをクリックすると、ソートレベル(プライマリソートは1、セカンダリソートは2、など)が表示される。ネストされたソートをクリアするには、対応するカラム名をクリックする。
カラムの並べ替え	カラムをドラッグアンドドロップして移動します。

以下の図は、リソースタイプ、ソフトウェアバージョン、サーバ名のソート順でソートされたサーバの表を示しています。[Type] カラムと [Name] カラムは昇順にソートされ、[Version] カラムは降順にソートされています。

図 2: タイプ、バージョン、名前でソートされたリソース

	Name	3 ▲	Type	1 ▲	Version	2 ▼
	mira8		ASE Server		15.0.2	
	mira9		ASE Server		15.0.2	
	LondonDR		ASE Server, Replication Only		12.5	
	LondonEx		ASE Server, Replication Only		12.5	
	NYEx		ASE Server, Replication Only		12.5	
	lint10dev_mpx		IQ Multiplex		15.3.0.6038	
	lint10dev_mpx		IQ Multiplex		15.3.0.6038	
	sun7bar_iqdemo		IQ Multiplex		15.3.0.6035	
	lamd6supt_r2		IQ Server		15.3.0.6038	
	lint10dev_cn		IQ Server		15.3.0.6038	
	lint10dev_r1		IQ Server		15.3.0.6038	


カラムによるフィルタ

管理コンソールの各カラムの先頭にフィルタリングフィールドがあります。フィルタリングワードを入力して、表示されるオブジェクトの範囲を絞り込みます。次に例を示します。

- サーバ、データベース、グループ、その他の名前が付いたオブジェクトを表示するには、[Name] カラムの先頭にリソースの名前を入力します。文字を入力するごとに候補が表示されるので、場合によっては名前全体を入力する必要はありません。
- ソフトウェアの特定のバージョンを実行するリソースのみを表示するには、[Version] カラムの先頭にバージョン番号を入力します。


複数のカラムをフィルタリングできます。たとえば、サーバのリストで、[Status] カラムを使用して実行中のサーバのみを表示し、[Version] カラムを使用して、目的のソフトウェアバージョンを使用しているサーバを表示できます。元の表示に戻るには、フィルタリングワードを削除します。フィルタリングワードでは、大文字が小文字を区別されません。

全画面モード

SCC でビューと観点に使用できる画面領域を増やすには、観点領域の右上隅にある  アイコンをクリックします。元の画面設定に戻すには、このアイコンを再度クリックします。

ヒント： SCC で使用できる画面領域を増やすには、[F11] を押して Internet Explorer または Firefox を全画面モードに切り替えます。元のブラウザ設定に戻すには、[F11] を再度押します。

ビューのセクションの最大化

ビュー内部の一部の領域の右上隅には、四角の最小化/最大化アイコン () があります。そのアイコンをクリックすると、その領域がビュー全体に拡大されます。アイコンを再度クリックすると、領域が元のサイズに戻ります。

[View] メニュー

[Perspective Resources] ビュー、Resource Explorer、[Alert Monitor]、ヒートチャートには、それぞれ [View] メニューがあります。[View] メニューから、次の操作を実行できます。

- 検索用のフィルタリングツールを表示します (ヒートチャートの [Filter] オプションでは、カラム選択ツールも表示されます)
- リソースのアイコンビューと詳細ビューを切り替えます ([Perspective Resources] ビューのみ)

- 表示を更新します (Resource Explorer のみ)

注意： これらのタスクでは、SCC ウィンドウ上部にあるアプリケーションレベルの [View] メニューではなく、ビューウィンドウの [View] メニューを使用します。

フォントサイズの変更

SCC の画面でフォントのサイズを変更するには、次の手順を実行します。

- [Ctrl-Alt +] を押すと、表示フォントが大きくなります。
- [Ctrl-Alt -] を押すと、表示フォントが小さくなります。

Keyboard Shortcuts (キーボードショートカット)

SAP Control Center Web インタフェースで使用頻度の高いキーシーケンスは次のとおりです。

キーシーケンス	アクション
Ctrl-Alt-F12	一番上のビューまたは SCC メニューバーの最初のメニューのプルダウン。繰り返して使用すると、最初の 2 つのメニューの切り替えが行われる。
Ctrl-Alt-Shift-F12	SCC メニューバーの最初のメニュー (アプリケーション) のプルダウン。
Space	強調表示されたオプションの選択。マウスでのクリックに相当する。
ESC	<ul style="list-style-type: none">• ドロップダウンメニューの解放。• 編集可能セルまたはフィールドの終了。• ウィンドウを閉じる。
矢印キー	<ul style="list-style-type: none">• 指示された方向の次の項目またはメニューオプションを強調表示する。たとえば下矢印キーは、メニュー内の次の項目を強調表示し、右矢印はメニュー内で右側にある項目を強調表示する。• ツリー構造では、右矢印によってノードが展開され、左矢印で圧縮される。

キーシーケンス	アクション
タブ	<ul style="list-style-type: none"> ビュー内で、タブ順序に従って次の項目を強調表示する (タブ順序は、アクセス可能なフィールドを左上から順に、左から右、上から下に進む)。 2つのウィンドウ枠のビューで、左ウィンドウ枠のツリー階層から、右ウィンドウ枠にジャンプする。 表またはグリッド表示が含まれるビューで [Tab] キーを 2 回押すと、表が強調表示され、下矢印を押すと中に入る。
Shift-Tab	<ul style="list-style-type: none"> ビュー内で、タブ順序に従って前の項目を強調表示する。 2つのウィンドウ枠のビューで、右ウィンドウ枠から、左ウィンドウ枠のツリー階層に戻る。
Home	たとえば表内の 1 行目など、アクティブなビュー (またはビュー内のアクティブなセクション) の最初の項目を強調表示する。
終了	たとえば表内の最終行など、アクティブなビュー (またはビュー内のアクティブなセクション) の最後の項目を強調表示する。
SCC メニューバーの、[View] > [Select] > [<各自のビュー>]	開いているビューを選択し、前面に表示する。
Ctrl-Alt- 矢印キー	選択したビューを指示した方向に移動する。
Ctrl-Alt +	表示テキストのサイズを拡大する。
Ctrl-Alt -	表示テキストのサイズを縮小する。
F11	ブラウザの全画面モードの有効と無効を切り替える。
SCC メニューバーの、[Application] > [Display] > [Full Screen]	SAP Control Center の全画面モードの有効と無効を切り替えます。

SAP Control Center は Adobe Flex 上に構築されています。Adobe Flex のキーボードショートカットの完全な説明については、http://livedocs.adobe.com/flex/3/html/help.html?content=accessible_5.html を参照してください。

SCC コンポーネントのバージョンの表示

SAP Control Center にインストールされたコンポーネントとそのバージョンのリストを表示します。

SCC インストールの製品モジュールのバージョンをチェックして、インストールが最新の状態であるかどうかを確認します。SCC リリースノートには、使用可能な製品モジュールバージョンが一覧表示されます。SCC リリースノートは、SAP Help Portal (<http://help.sap.com/database>) にあります。SCC で管理されている製品のマニュアルセットを参照してください。

1. SCC にログインして、[Help] > [About SAP Control Center] を選択します。
2. 製品モジュールのバージョン (管理エージェントプラグインとしてリスト表示) と最新の『SCC-product-name リリースノート』で公開されているバージョンを比較します。

スタイルと構文の規則

コマンド構文を表現し、システム出力とユーザ入力 of 要素を表すフォントと特殊文字のリファレンス。

表 6 : 表記規則

キー	定義
等幅 (固定幅)	<ul style="list-style-type: none"> • SQL とプログラムコード • 示されているとおりに正確に入力されるコマンド • ファイル名 • ディレクトリ名
斜体等幅	SQL またはプログラムコードスニペットでの、ユーザ指定値のプレースホルダ (以降の例を参照)
斜体	<ul style="list-style-type: none"> • ファイル名と変数名 • 他のトピックまたはマニュアルへの相互参照 • テキストでの、ユーザ指定値のプレースホルダ (以降の例を参照) • テキストでの用語解説

キー	定義
太字体 sans-serif	<ul style="list-style-type: none"> コマンド、関数、ストアドプロシージャ、ユーティリティ、クラス、メソッドの名前 用語解説エントリ (用語解説内) メニューオプションパス 番号付きタスクまたはプロシージャ手順での、ボタン、チェックボックス、アイコンなど、クリック対象のユーザインタフェース (UI) 要素。

プレースフォルダは、指定するシステムまたは環境固有の値を表します。次に例を示します。

```
installation directory/start.bat
```

installation directory は、アプリケーションがインストールされる場所です。

表 7：構文の表記規則

キー	定義
{ }	中カッコで囲まれたオプションの中から必ず 1 つ以上を選択する。コマンドを入力する場合、カッコを入力しない。
[]	角カッコは、オプションを選択しても省略してもよいことを意味する。コマンドを入力する場合、カッコを入力しない。
()	このカッコはコマンドの一部として入力する。
	中カッコまたは角カッコの中の縦線で区切られたオプションのうち 1 つだけを選択できることを意味する。
,	カンマは、表示されているオプションを必要な数だけ選択でき、選択したものをコマンドの一部として入力するときにカンマで区切ることを意味する。
...	省略記号 (...) は、直前の要素を必要な回数だけ繰り返し指定できることを意味する。省略記号はコマンドには入力しない。

アクセシビリティ機能

アクセシビリティ機能を使用すると、身体障害者を含むすべてのユーザーが電子情報に確実にアクセスできます。

Sybase 製品のマニュアルには、アクセシビリティを重視した HTML 版もあります。

オンラインマニュアルは、スクリーンリーダーで読み上げる、または画面を拡大表示するなどの方法により、視覚障害を持つユーザがその内容を理解できるよう配慮されています。

Sybase の HTML マニュアルは、米国のリハビリテーション法第 508 条のアクセシビリティ規定に準拠していることがテストにより確認されています。第 508 条に準拠しているマニュアルは通常、World Wide Web Consortium (W3C) の Web サイト用ガイドラインなど、米国以外のアクセシビリティガイドラインにも準拠しています。

注意：アクセシビリティツールを効率的に使用するには、設定が必要な場合もあります。一部のスクリーンリーダーは、テキストの大文字と小文字を区別して発音します。たとえば、すべて大文字のテキスト (ALL UPPERCASE TEXT など) はイニシャルで発音し、大文字と小文字の混在したテキスト (Mixed Case Text など) は単語として発音します。構文規則を発音するようにツールを設定すると便利かもしれません。詳細については、ツールのマニュアルを参照してください。

Sybase のアクセシビリティに対する取り組みについては、Sybase Accessibility サイト (<http://www.sybase.com/products/accessibility>) を参照してください。このサイトには、第 508 条と W3C 標準に関する情報へのリンクもあります。

製品マニュアルには、アクセシビリティ機能に関する追加情報も記載されていません。

SAP Control Center のアクセシビリティに関する情報

SAP Control Center では Adobe Flex アプリケーションを使用します。

Adobe Flex のキーボードショートカットに関する最新の情報については、http://livedocs.adobe.com/flex/3/html/help.html?content=accessible_5.html を参照してください。

注意：JAWS 付き SAP Control Center (Windows 版) のスクリーン読み上げソフトウェアを効率的に使用するには、適切な Adobe スクリプトをダウンロードしてインストールします。<http://www.adobe.com/accessibility/products/flex/jaws.html> を参照してください。

使用開始にあたって

SAP® Control Center を設定します。

評価のための簡易起動

(オプション) セキュリティ機能のフルセットを必要としない場合は、SAP Control Center を使用して直ちに起動できます。この簡略化したプロセスは、小規模環境での一時的な評価や概念実証プロジェクト、またはインストールの検証に適しています。

前提条件

SAP Control Center をインストールします。

手順

SAP Control Center の起動、ログイン、サーバの登録とサーバからの認証、サーバのモニタを実行するには、以下のタスクを使用します。

注意：以下のタスクを完了し、SCC が動作していることを確認してから、さらに継続して使用する場合は、運用環境用に SCC をセットアップします。

1. Windows での ODBC ドライバの登録

Windows で、管理者権限を使用して scc.bat を実行し、ODBC ドライバを登録します。

2. SAP Control Center の起動

scc コマンドを使用して SAP Control Center を起動します。

3. インストール後の設定

インストールが完了したら、テストと設定を行います。

4. Data Assurance サーバの登録

リソース (モニタ対象として使用可能なサーバなど) を登録して、SAP Control Center がそのリソースと接続情報を認識できるようにします。

5. 管理対象リソースのログインアカウントの認証

SAP Control Center がサーバまたはエージェントに接続して監視データを収集したりリソースを管理したりする場合に使用するログインアカウントとパスワードを指定します。

6. リソースの可用性の表示: ヒートチャート

使用開始にあたって

ヒートチャートを使用して、現在のパースペクティブのサーバのステータスと可用性を表示します。

7. Data Assurance サーバおよびエージェントのステータスの表示

Data Assurance (DA) モニタには、サーバやエージェントに関する高レベルの情報が表示されます。

参照：

- 運用環境での使用 (20 ページ)

Windows での ODBC ドライバの登録

Windows で、管理者権限を使用して **scc.bat** を実行し、ODBC ドライバを登録します。

Windows マシンで SAP Control Center を初めて起動すると、ODBC ドライバが登録されます。ODBC ドライバの自動登録では、レジストリ設定が編集されるため、引き上げた管理者権限を使用して **scc.bat** を実行する必要があります。十分な権限なしで初回の起動を行うと、エラーが発生し起動に失敗します。

Windows 2008、Windows 7、および Windows 8 では、すでに管理者権限を持っている場合でも [管理者として実行] 設定を使用して SCC を起動する必要があります。このプロセスについて次に説明します。

Windows のその他のバージョンでは、初めて SCC を起動する場合、管理者としてログインしている必要があります。次の手順に従う必要はありません。

1. Windows 2008、Windows 7、または Windows 8 では、管理者権限を使用してコマンドプロンプトウィンドウを開きます。
 - [スタート]>[すべてのプログラム]>[アクセサリ]を選択します。[コマンドプロンプト]を右クリックし、[管理者として実行]を選択します。
 - または、[スタート]メニューの [検索] ボックスに **cmd** と入力し、文にカーソルを合わせ、[Shift+Ctrl+Enter] キーを押します。
2. **scc.bat** を実行します。

SAP Control Center の起動

scc コマンドを使用して SAP Control Center を起動します。

前提条件

SAP Control Center に使用するブラウザに Adobe Flash Player をインストールします。

手順

1. SAP Control Center を起動します。

- Windows - <install_location>\\$SCC-3_3\bin に移動して **scc.bat** をダブルクリックします。
- UNIX - **scc.sh** を実行します。

起動の進捗に関するメッセージがコマンドウィンドウに表示されます。SAP Control Center が実行されていると、コマンドウィンドウは SAP Control Center コンソールになります。コマンドを発行して、SCC とそのポート、プラグイン、サービスに関するステータス情報を取得できます。

2. Web ブラウザを起動し、<https://<hostname>:8283/scc> を入力します。

インストール後の設定

インストールが完了したら、テストと設定を行います。

前提条件

SAP Control Center を起動します。

手順

1. SCC への接続に使用する Web ブラウザに Adobe Flash Player 10.1 以降をインストールします。

Flash Player は無償のプラグインです。最新バージョンを <http://get.adobe.com/jp/flashplayer/> からダウンロードできます。

Flash Player がすでにインストールされていても、そのバージョンが不明な場合は、Adobe テストサイト (<http://www.adobe.com/jp/shockwave/welcome/>) にアクセスしてください。[Adobe Flash Player のインストール状況をテスト] というリンクをクリックします。次に表示されるページのバージョン情報ボックスにお使いの Flash Player のバージョンが表示されます。

2. SCC に接続するには、ブラウザに次の URL を入力します。

https://<scc_server_hostname>:8283/scc

注意： インストール時にデフォルトの HTTPS ポートを変更した場合は、8283 ではなく新しいポート番号を使用します。

3. (オプション) セキュリティ証明書に関するエラーが表示された場合は、ブラウザの [信頼済みサイトゾーン] (Internet Explorer) に SCC を追加するか、セキュリティ例外 (Firefox) を追加します。
4. ログインします。

使用開始にあたって

SCC では、初期設定および永久認証の設定用としてデフォルトのログインアカウント `sccadmin` が用意されています。パスワードはインストール時に設定します。

注意： `sccadmin` アカウントとその基となる事前設定されたログインモジュールは、運用環境での使用を目的としていません。オンラインヘルプの [使用開始にあたって] > [セキュリティの設定] セクションに説明したとおり、認証はオペレーティングシステムまたは LDAP に任せることをおすすめします。

認証の設定とテストの完了と同時に `sccadmin` を無効にすることをおすすめします。また、認証をすぐに設定してテストしない場合は、`sccadmin` アカウントのパスワードを変更することをおすすめします。

5. (オプション) パスワードを変更するか、`sccadmin` を無効にします。詳細については、`SCC-product-name` インストールガイドを参照してください。

Data Assurance サーバの登録

リソース (モニタ対象として使用可能なサーバなど) を登録して、SAP Control Center がそのリソースと接続情報を認識できるようにします。

1. [Resource Explorer] で、[Resources] > [Register] を選択します。
2. 以下を指定します。

フィールド	説明
Resource Name	(必須) 登録するリソースの名前。大文字と小文字を使用して管理対象サーバの実際の名前を入力する。SAP Control Center に登録された名前が、サーバ名と完全一致しないと、トポロジビューなどの一部のモニタ機能が機能しない。
Resource Type	リソースタイプを選択する。 <ul style="list-style-type: none">• Data Assurance Server - Data Assurance サーバをモニタする。
Description	リソースの識別に役立つ簡単な説明。

3. [Next] をクリックします。
4. リソースの接続情報を指定します。

フィールド	説明
Host Name	ローカルのホスト名。
Port Number	ローカルのポート番号。

5. (オプション) SCC で当該リソースの認証に使用可能なユーザ名とパスワードを入力して、そのソフトウェアバージョンを検索します。クレデンシャルはこの目的のみに使用され、使用後は破棄されます。

ここで認証を行いたくない場合は、[I do not want to supply authentication information] をクリックします。

この手順により、サーバが公式に認証を受ける (後の設定プロセス) 前に SCC でそのサーバの正しいバージョン情報を表示できるようになります。

6. [Next] をクリックします。
7. (オプション) [Add this resource to the current perspective] をクリックします。リソースの管理やモニタを可能にするには、リソースをパースペクティブ (現在のパースペクティブである必要はない) に追加する必要があります。
8. (オプション) [Open the resource explorer to view this new resource] をクリックします (このオプションは、Resource Explorer が開いているときは存在しません)。
9. [Finish] をクリックします。

管理対象リソースのログインアカウントの認証

SAP Control Center がサーバまたはエージェントに接続して監視データを収集したりリソースを管理したりする場合に使用するログインアカウントとパスワードを指定します。

SAP Control Center に登録されている各リソースごとにこのタスクを実行します。

注意： アラートまたは収集ジョブの作成などの管理タスクの間にサーバを認証することもできます。

1. ブラウザを SAP Control Center に接続し、ログインします。
2. [Perspective Resources] ビューが開いていない場合は、ツールバーの [Show/Hide Perspective Resources View] アイコンをクリックします。
3. [Perspective Resources] ビューでリソースを選択し、ビューメニューから [Resource] > [Authenticate] を選択します。
4. [Use my current SCC login] または [Specify different credentials] を選択します。

注意： [Use my current SCC login] オプションは SCC for Replication では使用できません。

5. [Specify different credentials] を選択した場合は、リソースへの接続に使用する SAP Control Center のログインとパスワードを入力します。
6. 選択したリソースが Replication Server の場合は、RSSD ユーザ名とパスワードを入力します。
7. [OK] をクリックして、保存してダイアログを終了します。

リソースの可用性の表示: ヒートチャート

ヒートチャートを使用して、現在のパースペクティブのサーバのステータスと可用性を表示します。

ヒートチャートには、パースペクティブ内のリソースの状態 (リソースが実行中、中断中、停止中) が表示されます。これに加え、ヒートチャートには、各リソースのタイプが一覧表示され、最後のデータ収集の開始時間などの統計データが表示されます。

表示するリソースをフィルタリングしたり、検索したり、結果をカラムでソートすることができます。また、リソースを選択して、コンテキストメニューでプルダウンし、リソースタイプに基づいて異なる監視および管理オプションを表示できます。

ヒートチャートのデータは、管理対象サーバから直接収集され、収集されたときの日時でタグ付けされ、SAP Control Center リポジトリに保存されます。

1. アプリケーションのメニューバーで、[View] > [Open] > [Heat Chart] を選択します。
2. (オプション) チャートのアイコンが示すステータスの情報を表示するには、マウスをアイコンに合わせます。
 - [Status] カラム - アイコンのツールチップでリソースのステータスを説明します (実行中や停止など)。
 - [Status] の右側のすべてのカラム - アイコンのツールチップで、カラム上部に一覧表示された KPI の値を示します。
3. (オプション) フィルタリング (ヒートチャートのリソースのリストを絞り込む) やカラムを変更するためのツールを表示するには、[Perspective Heat Chart] メニューバーから [View] > [Filter] を選択します。
[Filter and Column tools] が左側のペインに表示されます。
4. (オプション) フィルタリングを使用するには、ビューのメニューバーから [View] > [Filter] を選択し、[Filter string] フィールドに検索ワードを入力します。
検索単語には、サーバまたはリソースのタイプの名前または名前の一部など、ヒートチャートのテーブル部分に表示される任意の文字列を入力できます。たとえば、「ASE Server」と入力できます。
5. (オプション) フィルタリング設定として以下のいずれかを選択します。
 - [Match case] - 表示されるデータに、大文字と小文字を含む検索ワードが含まれているリソースを検索します。または
 - [Exact match] - 表示されるデータに、検索ワードと完全に一致する項目を含むリソースを検索します。

6. (オプション) [Filter on] リストからカラムを選択すると、カラムの検索を制限できます。
7. (オプション) [Columns] をクリックして、ヒートチャートのオプションをカスタマイズします。
8. (オプション) ヒートチャートに表示しないすべてのカラムを選択解除します。
9. (オプション) カラムヘッダのソート矢印をクリックして、カラム値を昇順または降順にソートします。
10. (オプション) リソースのローをクリックし、リソース名の右側のメニューをプルダウンして、選択したリソースで利用できるオプションを表示します。
11. (オプション) [Filter and Columns tools] ペインの大きさを調整するには、ツールのペインとリソーステーブルとの間の枠線の上でカーソルを移動します。カーソルの形がサイズ変更アイコンに変化したら、クリックして、枠線を左方向または右方向に移動します。
12. (オプション) [Filter and Columns] ツールを非表示にするには、[View] > [Filter] を選択解除します。

Data Assurance サーバおよびエージェントのステータスの表示

Data Assurance (DA) モニタには、サーバやエージェントに関する高レベルの情報が表示されます。

前提条件

- モニタするサーバを登録し、[Perspective Resources] ビューに追加します。
- サーバを認証します。

手順

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Monitor] を選択します。

注意： [Perspective Resources] ビュー、[Heat Chart] ビュー、[Resource Explorer] ビュー、およびトポロジビューにあるサーバアイコンのステータスパッジを使用してサーバステータスを表示することもできます。

運用環境での使用

ユーザ認証の設定やその他の一度だけの設定作業など、SAP Control Center の設定をすべて実行します。

前提条件

SAP Control Center をインストールし、SCC-product-name インストールガイドに記載されている後続作業を完了しておきます。

1. Windows での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントを起動および停止する方法は複数あります。SAP Control Center または SCC エージェントは手動で起動できます。これは、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

2. UNIX での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントは手動で起動できます。これは、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

3. メモリ使用の設定

(オプション) SAP Control Center によって使用されるメモリサイズを設定する必要があるかどうか、および必要がある場合に使用する設定方法を決定します。

4. SAP Control Center へのログイン

SAP Control Center の Web コンソールにログインします。

5. セキュリティのセットアップ

ログイン認証を設定し、役割をマップします。

6. 自動ログアウトタイマの設定

(オプション) ユーザが長時間にわたって非アクティブな場合にログインセッションを停止するように、SAP Control Center を設定します。

7. ユーザ承認

SAP Control Center での権限メカニズムには、ログインアカウントとタスクベースの役割が使用されます。

8. 設定

SAP Sybase Control Center for Data Assurance を設定します。

Windows での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントを起動および停止する方法は複数あります。SAP Control Center または SCC エージェントは手動で起動できます。これ

は、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

このトピックは、SAP Control Center (管理 UI を含むサーバ) および SCC で管理される各製品サーバで実行される SCC エージェントの両方に適用されます。インストーラで両方のオプションを選択して同じディレクトリに SCC と SCC エージェントをインストールした場合、単一のコマンドを実行するか、単一のサービスを制御することで、常にそれらを一緒に起動および停止します。このトピックは、シングルトンインストール (共有ディスクを使用しない)、および共有ディスクから実行されている SCC エージェントとサーバのインスタンスの両方に適用されません。

SAP Control Center または SCC エージェントを手動で実行する場合、起動または停止のたびにコマンドを発行する必要があります。サービスとして実行する場合 (推奨)、それが自動的に起動および再起動されるように設定することができます。オプションは次のとおりです。

- **scc.bat** コマンドを使用して SCC または SCC エージェントを手動で起動します。このコマンドにより、SCC コンソールにアクセスできます。このコンソールを使用して、サービスを停止したり、サービス、ポート、システムプロパティ、および環境変数に関する情報を表示できます。さらに、**scc.bat** は、トラブルシューティングの目的でログレベルを変更するために使用することもできます。**scc.bat** を使用すると、サービスで使用可能な自動起動と再起動の機能を利用できません。
- SCC サーバまたはエージェントの SAP Control Center サービスを起動、停止、設定するには、Windows の [コントロールパネル] の [サービス] リストを使用します。
- **net start** コマンドと **net stop** コマンドを使用します。これは、サービスとして実行されるように SAP Control Center または SCC エージェントを設定するもう 1 つの方法です。

注意： SCC エージェントまたはサーバをサービスとして起動するには、次の手順を実行します。

- シングルトンインストールでサービスとしてエージェントまたはサーバをインストールするには、インストーラで [はい] を選択しておく必要があります。
 - 共有ディスクインストールの場合、エージェントやサーバは、**sccinstance** コマンドの **-service** オプションを使用して展開されている必要があります。
-

シングルトンインストールでは、SCC または SCC エージェントをサービスとして起動することができ、サービスが自動的に再起動されるように設定します。起動の前に、Windows の [サービス] リストに SAP Control Center サービスがあることを確認します。

次に、起動/停止オプションごとの手順を説明します。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) を起動します。**

a) (SCC エージェントの場合はこの手順を省略します。) Windows 2008、Windows 7、または Windows 8 で初めて SAP Control Center を起動する場合、SAP Control Center の ODBC ドライバを登録できるようにコマンドプロンプトで [管理者として実行] オプションを設定します (これは、システム管理者としてログインしている場合にも必要です)。

b) **scc** コマンドを入力します。

シングルトンインストールの場合:

```
%SYBASE%\SCC-3_3\bin\scc.bat
```

インスタンスの場合:

```
%SYBASE%\SCC-3_3\bin\scc.bat -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) を停止します。**

a) **scc --stop** コマンドを入力します。

シングルトンインストールの場合:

```
%SYBASE%\SCC-3_3\bin\scc.bat --stop
```

インスタンスの場合:

```
%SYBASE%\SCC-3_3\bin\scc.bat --stop -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

注意: また、`scc-console>` プロンプトで、**shutdown** を入力することもできます。

- **Windows の [コントロール パネル] から起動または停止し、自動起動と再起動を設定します。**

a) Windows の [コントロール パネル] を開きます。

b) [Administrative Tools] > [Services] を選択します。

- c) [サービス] リストで “SAP Control Center” を見つけます。インスタンス用のサービスの場合はリリース番号が付いている場合があります。またインスタンス名が付いている場合もあります。サービス名では、エージェントとサーバは区別されません。サービスが実行されている場合、[状態] 列には [開始] と表示されます。
 - d) サービスを起動または停止するには、[Services] リストで [SAP Control Center] エントリを右クリックし、[Start] または [Stop] を選択します。
 - e) 自動起動を設定するには、サービスをダブルクリックします。
 - f) マシンの起動時にサービスが自動的に起動するように設定するには、[Startup type] を [Automatic] に変更します。
 - g) 障害が発生した場合にサービスを再起動するには、[Recovery] タブを選択し、[First]、[Second]、[Subsequent] のエラーを [Restart Service] に変更します。
 - h) [Apply] をクリックして変更を保存してから、ダイアログボックスを閉じます。
- **Windows のコマンドラインから SAP Control Center サービス (SAP Control Center と SCC エージェントのいずれか一方または両方を制御する) を起動または停止します。**

- a) サービスを起動するには、**net start** コマンドを入力します。

シングルトンインストールの場合:

```
net start "SAP control center 3.3"

The SAP Control Center 3.3 service is starting.....
The SAP Control Center 3.3 service was started
successfully.
```

インスタンスの場合、インスタンス名 (この例では Boston-1) をカッコに含めます。

```
net start "SAP control center 3.3 (Boston-1)"

The SAP Control Center 3.3 (Boston-1) service is
starting.....
The SAP Control Center 3.3 (Boston-1) service was started
successfully.
```

- b) サービスを停止するには、**net stop** コマンドを入力します。

シングルトンインストールの場合:

```
net stop "SAP control center 3.3"

The SAP Control Center 3.3 service is stopping.....
The SAP Control Center 3.3 service was stopped
successfully.
```

使用開始にあたって

インスタンスの場合、インスタンス名(この例では Boston-1)をカッコに含めます。

```
net stop "SAP control center 3.3 (Boston-1)"

The SAP Control Center 3.3 (Boston-1) service is
stopping.....
The SAP Control Center 3.3 (Boston-1) service was stopped
successfully.
```

UNIX での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントは手動で起動できます。これは、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

このトピックは、SAP Control Center (管理 UI を含むサーバ) および SCC で管理される各製品サーバで実行される SAP Control Center エージェントの両方に適用されます。インストーラで両方のオプションを選択して同じディレクトリに SCC と SCC エージェントをインストールした場合、単一のコマンドを実行するか、単一のサービスを制御することで、それらを一緒に起動および停止します。このトピックは、シングルインストール (共有ディスクを使用しない)、および共有ディスクから実行されている SCC エージェントとサーバのインスタンスの両方に適用されます。

SAP Control Center または SCC エージェントを手動で起動する場合、起動または停止のたびにコマンドを発行する必要があります。サービスとして実行する場合 (推奨)、それが自動的に起動および再起動されるように設定することができます。オプションは次のとおりです。

- **scc.sh** スクリプトを使用して SAP Control Center または SCC エージェントを手動で起動します。次のいずれかの方法を使用できます。
 - フォアグラウンドで **scc.sh** を実行し、SCC コンソールにアクセスします。このコンソールを使用して、サービスを停止したり、サービス、ポート、システムプロパティ、および環境変数に関する情報を表示できます。
 - バックグラウンドで **scc.sh** を実行し、SCC コンソールが表示されないようにします。
トラブルシューティングのためにデフォルト以外のログレベルで SAP Control Center を実行するには、**scc.sh** を使用します。**scc.sh** を使用して手動で起動すると、サービスで使用可能な自動起動と再起動の機能を利用できません。
- **sccd** スクリプトを使用して SCC または SCC エージェントが自動的に起動されるように設定します。

次に、起動/停止オプションごとの手順を説明します。

- **SAP Control Center または SCC エージェントを初めて起動する前に、環境変数を設定します。** これは、一度だけ行います。

- a) SAP Control Center インストールディレクトリの親ディレクトリに変更します (通常、親ディレクトリは /opt/sap または opt/sybase です)。
- b) 次のいずれかを実行して、環境変数を設定します。

Bourne シェル :

```
. SYBASE.sh
```

C シェル :

```
source SYBASE.csh
```

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) をフォアグラウンドで実行します。**

フォアグラウンドでの実行は、手動で起動する場合の方法です。SCC または SCC エージェントを停止して再起動するには、コマンドを発行する必要があります。

- a) SCC または SCC エージェントを起動し、起動シーケンスの終了時にコンソールにそれをドロップするには、**scc** コマンドを入力します。

シングルトンインストールの場合:

```
$SYBASE/SCC-3_3/bin/scc.sh
```

インスタンスの場合:

```
$SYBASE/SCC-3_3/bin/scc.sh -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) をバックグラウンドで実行します。**

nohup、**&**、および **>** を使用すると、SAP Control Center または SCC エージェントをバックグラウンドで実行し、出力とシステムエラーをファイルにリダイレクトし、SCC コンソールを非表示にすることができます。バックグラウンドでの実行は、手動で起動する場合の方法です。SCC または SCC エージェントを停止して再起動するには、コマンドを発行する必要があります。

- a) シェルに対応する次のサンプルと同様のコマンドを実行します。サンプルコマンドはどちらも `scc-console.out` ファイルに出力をダイレクトします。出力ファイルがすでに存在する場合は、その他のシェル演算子を使用してファイルに追加したり、ファイルをトランケートすることが必要になることがあります。

Bourne shell (sh) または Bash

シングルトンインストールの場合 :

```
nohup ./scc.sh 2>&1 > scc-console.out &
```

使用開始にあたって

インスタンスの場合：

```
nohup ./scc.sh -instance <instance-name> 2>&1 > scc-console-  
your-instance.out &
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

C シェル

シングルトンインストールの場合：

```
nohup ./scc.sh >& scc-console.out &
```

インスタンスの場合：

```
nohup ./scc.sh -instance <instance-name> >& scc-console.out &
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) を停止します。**

a) `scc-console>` プロンプトから停止するには、次のように入力します。

```
shutdown
```

警告！ UNIX のプロンプトで **shutdown** と入力しないでください。入力すると、オペレーティングシステムがシャットダウンしてしまいます。

UNIX コマンドラインから停止するには、**scc --stop** コマンドを入力します。

シングルトンインストールの場合:

```
$(SYBASE)/SCC-3_3/bin/scc.sh --stop
```

インスタンスの場合:

```
$(SYBASE)/SCC-3_3/bin/scc.sh --stop -instance <instance-  
name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **サービスとして実行されるように SAP Control Center または SCC エージェントを設定します。**

UNIX サービスは、マシンの起動後に自動的に開始され、バックグラウンドで実行されるデーモンプロセスです。SCC の UNIX インストールには、シェルスクリプト **sccd** が含まれています。このシェルスクリプトを使用して SCC サービスを設定できます (一部の UNIX プラットフォームでは、サービスの設定を容易にするツールが提供されています。Linux **chkconfig** はその例です)。

注意： SAP では、UNIX でのサービスの設定に慣れていないユーザは、この作業をシステム管理者に任せるか、UNIX プラットフォームのシステム管理のマニュアルを参照することをおすすめします。

a) `$SYBASE/SCC-3_3/bin/sccd` を次のディレクトリにコピーします。

- AIX (SCC エージェントのみ)： `/etc/rc.d/init.d`
- HP-UX (SCC エージェントのみ)： `/sbin/init.d`
- その他のプラットフォーム： `/etc/init.d`

b) `sccd` を開き、次の変更を加えます。

- `SYBASE` 変数を設定する行を SAP Sybase インストールのロケーション (SAP Control Center インストールディレクトリ `SCC-3_3` の親) に変更します。 Sybase 製品または環境変数がすでに存在するマシンに SCC がインストールされている場合、このディレクトリ名はデフォルトで `/opt/sybase` です。それ以外の場合、デフォルトの親ディレクトリは `/opt/sap` です。
- 共有ディスクモードを使用していない場合、または共有ディスクモードを使用してホスト名と同じ名前の単一インスタンスを実行している場合は、手順 5.c (27 ページ) または手順 5.d (28 ページ) にスキップします。
- 共有ディスクモードを使用してホスト名とは異なる名前の単一インスタンスを実行している場合、または同じホスト上で複数のインスタンスを実行している場合は、スクリプト名にインスタンス名を追加します。

```
SCRIPT_NAME=scc.sh
```

上記を次のように変更します。

```
SCRIPT_NAME="scc.sh -instance <instance-name>"
```

- 共有ディスクモードを使用して同じホスト上で複数のインスタンスを実行している場合は、出力ログファイルの名前にインスタンス名を追加します。

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-service.out &
```

上記を次のように変更します。

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-service_<instance-name>.out &
```

- 共有ディスクモードを使用して、同じホストで複数のインスタンスを実行する場合、インスタンスごとに `sccd` スクリプトのコピーを一意の名前で保存します。各コピーで、スクリプト名にインスタンス名を追加し、さらにインスタンス名を前述のように出力ログファイル名に追加します。 `sccd` のコピーごとに残りの手順を実行します。

c) Linux の場合は、サービスがランレベル 2、3、4、5 で実行されるように設定します。

使用開始にあたって

```
/usr/sbin/chkconfig --add sccd  
/usr/sbin/chkconfig --level 2345 sccd
```

sccd スクリプトは、`/usr/sbin/service sccd status` を使用してテストできます (**service** コマンドでは次のオプションが受け入れられます。

start | stop | status | restart)。

d) Linux 以外のプラットフォームでは、次のディレクトリを検索します。

- AIX (SCC エージェントのみ) : `/etc/rc.d/rc<X>.d`
- HP-UX (SCC エージェントのみ) : `/sbin/rc<X>.d`
- Solaris の場合 : `/etc/rc<X>.d`

ここで、`<X>` はランレベル (たとえば 3) です。ご使用のプラットフォームのディレクトリに 2 つのソフトリンクを作成して、次を参照するようにリンクを設定します。

- AIX (SCC エージェントのみ) :
`/etc/rc.d/init.d/sccd: S90sccd および`
`/etc/rc.d/init.d/sccd: K10sccd`
- HP-UX (SCC エージェントのみ) :
`/sbin/init.d/sccd: S90sccd および`
`/sbin/init.d/sccd: K10sccd`
- Solaris の場合 :
`/etc/init.d/sccd: S90sccd および`
`/etc/init.d/sccd: K10sccd`

S90sccd リンクはサービスを起動し、K10sccd リンクはサービスを停止します。リンク内の 2 桁の数値は、サービスの起動と停止の優先度を示します。

e) S90sccd リンクと K10sccd リンクを使用してサービスの起動と停止をテストします。リンクは、マシンの起動時または停止時に自動的に呼び出されます。

メモリ使用の設定

(オプション) SAP Control Center によって使用されるメモリサイズを設定する必要があるかどうか、および必要がある場合に使用する設定方法を決定します。

通常は、SAP Control Center のメモリの使用量を設定する必要はありません。この表では、設定できるメモリのオプションと、変更を考える必要がある状況を示します。

変更する値	状況	ガイドライン
<p>最大メモリ</p> <ul style="list-style-type: none"> • <code>jvmopt=-Xmx</code> - SAP Control Center を Windows サービスとして実行している場合 • <code>SCC_MEM_MAX</code> - SCC を UNIX サービスとして実行している場合 • <code>SCC_MEM_MAX</code> - コマンドラインから SCC を起動している場合 	<ul style="list-style-type: none"> • 指定したサイズよりも多くのメモリが SAP Control Center によって使用されるのを防ぐ必要がある場合 • SAP Control Center fails to start and may display an error: Could not create the Java virtual machine. • OutOfMemory エラーが、SAP Control Center のヒープスペースが不足していることを示している。 • 起動プロセス時にシステムメモリについての警告メッセージが表示される場合 • SAP Control Center がインストールされているマシンのメモリが 4GB 未満である (メモリが 4GB 未満のマシンで SAP Control Center を起動すると、システムメモリに関する起動警告メッセージがトリガされる)。 	<p>メモリが 4GB 未満のマシンでは、最大メモリを 256MB 以上に設定する。</p> <p>デフォルト値：なし (メモリが 4GB 以上のマシンでは、最大メモリは動的に設定され、システムメモリの量によってのみ効率的に制限される)。</p>

変更する値	状況	ガイドライン
永続メモリ <ul style="list-style-type: none"> • <code>jvmopt=-XX:MaxPermSize</code> - SAP Control Center を Windows サービスとして実行している場合 • <code>SCC_MEM_PERM</code> - SCC を UNIX サービスとして実行している場合 • <code>SCC_MEM_PERM</code> - コマンドラインから SCC を起動している場合 	OutOfMemory エラーが、SAP Control Center の永続的な生成領域が不足していることを示している。	32MB 単位でメモリを増やす。デフォルト値の 2 倍に設定しても OutOfMemory エラーが表示される場合、SAP テクニカルサポートに問い合わせる。 デフォルト値：128MB

メモリオプションは、次の 2 つの方法で変更できます。

- コマンドラインから起動された SAP Control Center の場合 - `scc` コマンドを実行して SAP Control Center を起動する前に、コマンドを実行して 1 つ以上の環境変数を設定します。この方法を使用する場合、メモリオプションの変更は現在のログインセッションの間だけ続きます。この方法は、新しいオプションの値をテストする場合に便利です。
- SAP Control Center サービスの場合 - SAP Control Center サービスに使用されるファイルを変更します。この方法を使用する場合、メモリオプションの変更は永続的です。SAP Control Center がサービスとして起動するたびに変更したオプションが使用されます。

参照：

- SAP Control Center へのログイン (32 ページ)

コマンドラインでのメモリオプションの変更

コマンドラインから SAP Control Center を起動する前に、メモリオプションの値を一時的に変更するコマンドを発行できます。

この方法を使用して行った変更は、現在のログインセッションの間のみ続きます。この方法は、新しいオプションの値をテストする場合に便利です。

1. SAP Control Center が起動している場合は停止します。
2. 環境変数を設定します。サイズをメガバイトで指定しますが、コマンドでは単位を指定しません。

Windows の例:

```
> set SCC_MEM_MAX=512
```

UNIX の例:

```
bash$ export SCC_MEM_MAX=512
```

3. **scc** コマンドを使用して SAP Control Center を起動します。

参照：

- SAP Control Center Windows サービスのメモリオプションの変更 (31 ページ)
- SCC UNIX サービスのメモリオプションの変更 (31 ページ)

SAP Control Center Windows サービスのメモリオプションの変更

jvmopt コマンドを `scc.properties` ファイルに追加して、SAP Control Center Windows サービスのメモリオプション (`-Xmx` または `-XX:MaxPermSize`) を変更します。

この方法を使用してメモリオプションを設定する場合、変更は永続的になります。つまり、これらのオプションは、SAP Control Center がサービスとして起動するごとに使用されます。

1. SAP Control Center が起動している場合は停止します。
2. SAP Control Center プロパティファイルを開きます。

```
<SAP Control Center-install-directory>%SCC-3_3%bin
%sc.properties
```

3. メモリサイズを Java フォーマットで指定する **jvmopt** 行を追加 (すでに存在する場合は変更) します。メガバイトの場合は `m` を、ギガバイトの場合は `g` を使用します。

例を示します。

```
jvmopt=-Xmx512m
```

4. ファイルを保存し、SAP Control Center Windows サービスを起動します。

参照：

- コマンドラインでのメモリオプションの変更 (30 ページ)
- SCC UNIX サービスのメモリオプションの変更 (31 ページ)

SCC UNIX サービスのメモリオプションの変更

SAP Control Center UNIX サービスのメモリ設定を変更するには、該当する環境変数 (`SCC_MEM_MAX` または `SCC_MEM_PERM`) を `sccd` スクリプトに追加します。

この方法を使用してメモリオプションを設定する場合、変更は永続的になります。つまり、これらのオプションは、SAP Control Center がサービスとして起動するごとに使用されます。

1. SAP Control Center が起動している場合は停止します。

使用開始にあたって

2. sccd ファイルを開きます。 /etc/init.d/sccd
3. 環境変数をファイルの先頭(コメントの後)に追加します。サイズをメガバイト単位で指定します。ただし、コマンドには単位を指定しません。
例を示します。

```
SCC_MEM_MAX=512
```
4. ファイルを保存し、SAP Control Center UNIX サービスを起動します。

参照：

- コマンドラインでのメモリオプションの変更 (30 ページ)
- SAP Control Center Windows サービスのメモリオプションの変更 (31 ページ)

SAP Control Center へのログイン

SAP Control Center の Web コンソールにログインします。

前提条件

SCC 用に使用するブラウザに Adobe Flash Player をインストールします。『SCC-product-name インストールガイド』を参照してください。

手順

通常、SAP Control Center では、オペレーティングシステムまたは LDAP ディレクトリサービスからユーザを認証します。SCC で使用するログインアカウントが不明な場合は、SCC 管理者に問い合わせてください。

1つのアカウントに同時に許可されるログインセッションは1つのみです。同じアカウントで複数のユーザが同時にログインすることはできません。

注意：新たにインストールされた SAP Control Center にセキュアな認証がまだ設定されていないときは、sccadmin アカウントを使用します。パスワードはインストール時に設定されています。詳細については、『SCC-product-name インストールガイド』を参照してください。

1. SAP Control Center サーバに接続します。Web ブラウザで、`https://scc-hostname:8283/scc` と入力します。
2. ログイン名とパスワードを入力して、[Login] をクリックします。

ヒント： Windows アカウントを使用して SCC にログインする場合は、`username@domain` の形式でユーザ名を入力します。上位レベルのドメイン拡張子 (.com や .net など) は省略します (例: fred@sap.com ではなく、fred@sap と入力します)。

参照：

- メモリ使用の設定 (28 ページ)

セキュリティのセットアップ

ログイン認証を設定し、役割をマップします。

SAP Control Center 製品モジュールを設定する前に、セキュリティに関するトピックを確認して以下の手順を実行します。

注意：以下のセキュリティに関するトピックは、実際の運用環境での使用を想定していません。SCC を評価またはテストしている場合は、「評価のクイックスタート (13 ページ)」を参照してください。

1. セキュリティ

SAP Control Center は LDAP サーバまたはオペレーティングシステム、あるいはその両方を使用してユーザログインを認証できます。

2. Windows 認証の設定

Windows オペレーティングシステムを利用する認証はデフォルトで有効化されています。古いバージョンの SAP Control Center からアップグレードし、古いバージョンの認証設定を使用せず、認証に Windows を使用せず、ログインアカウントを手動で作成する場合のみ設定が必要です。SAP では、SCC でアカウントを自動作成することをおすすめします。

3. UNIX 用のプラグ可能認証モジュール (PAM) の設定

UNIX オペレーティングシステムのアカウントを使用して、ユーザ名とパスワードのログインがサポートされるように SAP Control Center を設定します。

4. LDAP 認証モジュールの設定

SAP Control Center の LDAP 認証モジュールは、正しい LDAP サーバを指定するようにセキュリティ設定ファイルを編集して設定します。

5. LDAP または OS グループに対する SAP Control Center の役割のマッピング

LDAP またはオペレーティングシステムを介して認証されたユーザに SAP Control Center 権限を付与するには、SAP Control Center で使用される役割を LDAP またはオペレーティングシステムのグループに関連付けます。

6. パスワードの暗号化

テキストファイルに保存している間、安全に保つ必要があるパスワードなどの値を暗号化するには、passencrypt ユーティリティを使用します。

7. ポートの設定

(オプション) `scc --port` コマンドを使用して、SAP Control Center サービスを新しいポートに割り当てます。

参照：

- 自動ログアウトタイマの設定 (54 ページ)

セキュリティ

SAP Control Center は LDAP サーバまたはオペレーティングシステム、あるいはその両方を使用してユーザログインを認証できます。

- SAP Control Center は、inetOrgPerson (RFC 2798) スキーマをサポートする任意の LDAP サーバを使用して認証を行うよう設定できます。
- SAP Control Center は、オペレーティングシステムを使用して認証を行う場合、SAP Control Center サーバマシン (クライアントではない) のオペレーティングシステムを使用します。

SCC でネイティブユーザアカウントを作成することもできますが、この方法で認証を行うことは推奨されません。既存の LDAP、Windows、または UNIX ログインアカウントを使用して認証を行うよう SCC を設定した方が簡単かつ安全です。

SAP では、SCC および SCC によって管理される SAP データベース製品に共通の認証プロバイダを使用することを強くおすすめします。共通の認証プロバイダを使用することにより、シングルサインオンが SAP Control Center とそのマネージドサーバのユーザに対して機能します。

SCC は各認証ログインアカウントを要求し、事前に定義する役割を持ちます。ログインが認証されれば、ログインの役割がセキュリティモジュールによって取得され SCC の事前に定義される役割にマップされます。許可はセキュリティモジュールネイティブ役割と SCC 役割の間をマップすることで決定されます。マッピングは使用されている OS または LDAP サーバで「sybase」グループを作成し、すべての SCC ユーザに加えることにより可能です。または SCC role-mapping.xml ファイルを修正し SCC 役割にネイティブの役割のマッピングを設定することによって可能です。セキュリティモジュールはログインを認証し、管理リソースに対するアクセスを承認します。

SAP Control Center は認証に対する事前定義されたログインモジュールを提供します。すべてのログインモジュールは <install_location>/SCC-3_3/conf/csi_config.xml ファイルの中で定義されます。構文は SAP Common Security Infrastructure (CSI) フレームワークにより定義されます。別のログインモジュールを設定してセキュリティの強さをカスタマイズすることができます。ログインモジュールは、次のとおりです。

- 事前設定ユーザログイン - ユーザ名、パスワード、役割のリストを定義します。デフォルトのユーザ名は sccadmin であり、このパスワードはインストール時に設定されます。ネイティブの役割は SCC 管理者で、sccAdminRole にマップされています。事前設定ユーザログインモジュールを csi_config.xml に追加することによって、追加のアカウントを作成できま

す。ただし SAP では、運用環境での認証では事前ユーザログインモジュールの使用をおすすめしていません。

- NT プロキシログイン - 基本となる Windows オペレーティングシステムに認証を委任します。NT プロキシログインモジュールから SCC へログインする場合は、フォーマット `username@nt-domain-name` でユーザ名を入力してください。たとえば、`user@sap` を入力します。Windows 認証はデフォルトで有効化されていますが、SCC 3.2.5 以前からのアップグレード後は、若干の設定作業が必要です。
- UNIX プロキシログイン - Pluggable Authentication Modules (PAM) を使用して基本となる UNIX または Linux オペレーティングシステムに認証を委任します。UNIX PAM を通して SCC にログインするときは、UNIX のユーザ名とパスワードを入力してください。UNIX 認証はデフォルトで有効化されていますが、若干の設定が必要となります。
- LDAP ログイン - 指定の LDAP サーバに認証を委任します。LDAP サーバを通して SCC にログインするときは、LDAP のユーザ名とパスワードを入力してください。LDAP 認証はデフォルトでは有効化されていません。ログインモジュールを設定する必要があります。

Windows 認証の設定

Windows オペレーティングシステムを利用する認証はデフォルトで有効化されています。古いバージョンの SAP Control Center からアップグレードし、古いバージョンの認証設定を使用せず、認証に Windows を使用せず、ログインアカウントを手動で作成する場合のみ設定が必要です。SAP では、SCC でアカウントを自動作成することをおすすめします。

このタスクは任意です。ただし、SAP Control Center アカウントの自動作成を選択しない場合は、手動で入力する必要があります。LDAP やローカルオペレーティングシステムを使用して SCC ユーザの認証を行う場合も、SCC で権限 (ユーザの権利) を設定するには、アカウントが必要です。

1. SCC の管理者権限を持つアカウントを使用して、SCC にログインします。(ログインアカウントまたはそのグループに `sccAdminRole` が設定されている必要があります)。
2. [Application] > [Administration] > [Security] を選択します。
3. [Automatically add SCC login records for authenticated logins] のラベルが表示されたボックスをクリックして選択または選択解除します。
4. [Automatically grant sccUserRole to newly created logins] のラベルが表示されたボックスをクリックして選択または選択解除します。
5. [OK] をクリックして [Security] ダイアログを閉じます。

次のステップ

この後は2とおりの手順があります。

- SCC ログインアカウントの自動作成を選択しなかった場合は、それぞれのアカウントを SCC に手動で入力します。
- 基本的なユーザアクセス以上の権限が必要な場合は、ログインアカウントに権限を付与します。権限を付与するには、SCC の役割をログインアカウントに直接割り当てるか、ログインアカウントをグループに割り当て、SCC の役割をそのグループにマッピングします。一般に、グループを使用する方法のほうが効率的です。

UNIX 用のプラグ可能認証モジュール (PAM) の設定

UNIX オペレーティングシステムのアカウントを使用して、ユーザ名とパスワードのログインがサポートされるように SAP Control Center を設定します。

1. root 権限を持つログインアカウントを使用して、プラットフォームの PAM を設定します。

プラットフォーム	アクション
Solaris	<SCC-install-dir>/utility/<sunos>/pam.conf ファイル (SAP Control Center に付属) の内容を Solaris プラットフォーム上の /etc/pam.conf ファイルに追加する。
Linux	<SCC-install-dir>/utility/<linux>/sybase-csi ファイル (SAP Control Center に付属) を Linux プラットフォーム上の /etc/pam.d ディレクトリにコピーする。 注意： SAP Control Center に付属の sybase-csi ファイルは、最新の SUSE バージョンおよび Red Hat Linux バージョンとの互換性がない。詳細については、このトピックの最後にある例を参照のこと。

注意： 上記の表で、オペレーティングシステムを示すパスの箇所は、実際に表示される内容と多少異なる場合があります。

2. ホストの UNIX システムがディレクトリルックアップ認証 (yp、NIS など) を使用しておらず、認証がローカルの /etc/passwd ファイルに照らして実行される場合は、/etc/shadow のパーミッションを変更して、SCC を実行するログインアカウントに読み込みアクセスを付与します。
3. (SAP Control Center の起動前に PAM を設定した場合は省略) SAP Control Center を再起動します。
4. (オプション) アカウント作成オプションを変更します。

- a) 管理者権限 (sccAdminRole) を持つアカウントを使用して、SAP Control Center にログインします。
- b) [Application] > [Administration] > [Security]を選択します。
- c) [Automatically add SCC login records for authenticated logins] のラベルが表示されたボックスをクリックして選択または選択解除します。(SCC 3.2.6 以降はこのオプションがデフォルトで有効化されています。)
- d) [Automatically grant sccUserRole to newly created logins] のラベルが表示されたボックスをクリックして選択または選択解除します。(SCC 3.2.6 以降はこのオプションがデフォルトで有効化されています。)
- e) [OK] をクリックして [Security] ダイアログを閉じます。

例: SUSE Linux 11、Red Hat Enterprise Linux 6.0 用の PAM

SUSE 11 以降は、SAP Control Center に付属している sybase-csi ファイルを使用しないでください。代わりに、/etc/pam.d ディレクトリで、次の記載がある sybase-csi ファイルを作成します。

```
# sybase-csi PAM Configuration (SUSE style)
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

Red Hat 6.0 以降は、SAP Control Center に付属している sybase-csi ファイルを使用しないでください。代わりに、/etc/pam.d ディレクトリで、次の記載がある sybase-csi ファイルを作成します。

```
# sybase-csi PAM Configuration (Red Hat style)
auth      include      system-auth
account   include      system-auth
password  include      system-auth
session   include      system-auth
```

次のステップ

この後は 2 とおりの手順があります。

- SAP Control Center ログインアカウントの自動作成を選択しなかった場合は、それぞれのアカウントを SAP Control Center に手動で入力します。SAP Control Center で権限 (ユーザの権利) を設定するには、アカウントが必要です。
- 基本的なユーザアクセス以上の権限が必要な場合は、ログインアカウントに権限を付与します。権限を付与するには、SAP Control Center の役割をログインアカウントに直接割り当てるか、ログインアカウントをグループに割り当て、

SAP Control Center の役割をそのグループにマッピングします。一般に、グループを使用する方法のほうが効率的です。

LDAP 認証モジュールの設定

SAP Control Center の LDAP 認証モジュールは、正しい LDAP サーバを指定するようにセキュリティ設定ファイルを編集して設定します。

1. <SCC-install-dir>%conf%csi_config.xml ファイルを開きます。
2. 囲んでいる <!-- と --> 文字を削除して設定ファイル内の LDAP モジュールのコメント化を解除します (または必要に応じて LDAP モジュールをファイルに追加します)。次のサンプルモジュールでは、ユーザ認証を提供する LDAP サーバを指定します。

サンプルモジュールには、OpenDS LDAP サーバに使用されるプロパティが示されます。ActiveDirectory で機能する値については、このタスクの最後に示されている例を参照してください。LDAP モジュールで使用可能な設定プロパティは、サブトピックで説明されています。

```
<authenticationProvider controlFlag="sufficient"
name="com.sybase.security.ldap.LDAPLoginModule">
  <options name="BindDN" value="cn=Directory Manager"/>
  <options name="BindPassword" value="secret"/>
  <options name="DefaultSearchBase" value="dc=example,dc=com"/>
  <options name="ProviderURL" value="ldap://localhost:10389"/>
  <options name="ServerType" value="openldap"/>
</authenticationProvider>
<provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer"/>
```

注意：太字で示された値のみを変更します。BindPassword が暗号化されている場合 (SAP の推奨)、それを定義する行に encrypted="true" を含める必要があります。この行は次のようになります。

```
<options name="BindPassword" encrypted="true"
value="lsnjikfwregfqr43hu5io..." />
```

3. ファイルを保存します。
4. 使用する LDAP サーバの SSL 証明書に、標準以外の認証局による署名がある場合 (自己署名証明書である場合など) は、**keytool** ユーティリティを使用して、JVM または JDK がその証明書を信頼するように設定します。次のコマンドを実行します。

Windows の場合：

```
keytool -import -keystore %SAP_JRE7%\lib%security%cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

UNIX の場合：

```
keytool -import -keystore $SAP_JRE7/lib/security/cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

ActiveDirectory に使用される LDAP 設定値

ActiveDirectory server については、LDAP ログインモジュールの設定プロパティに次の値を使用します。

```
ServerType: msad2K
DefaultSearchBase: dc=<domainname>,dc=<tld> or o=<company
name>,c=<country code>
    E.g. dc=sybase,dc=com or o=Sybase,c=us
ProviderUrl: ldaps://<hostname>:<port>
    E.g.: ldaps://myserver:636
AuthenticationFilter: (&(userPrincipalName={uid})
(objectclass=user))
BindDN: <User with read capability for all users>
BindPassword: <Password for BindDN user>
RoleFilter: (|(objectclass=groupofnames) (objectclass=group))
controlFlag: sufficient
```

次のステップ

SCC の役割を LDAP グループにマッピングします。

参照：

- LDAP または OS グループに対する SAP Control Center の役割のマッピング (48 ページ)

LDAP Configuration Properties (LDAP 設定プロパティ)

SAP Control Center LDAP サービスを制御するには、csi_config.xml ファイルで次のプロパティを使用します。

注意： 次の文字が LDAP 内の名前で使用された場合は特別な意味を持ちます。、(カンマ)、=(等号)、+(プラス記号)、<(小なり)、>(大なり)、#(番号またはハッシュマーク)、;(セミコロン)、¥(バックスラッシュ/円マーク)、/(スラッシュ)、LF(改行)、CR(復帰改行)、“(二重引用符)、'(一重引用符)、*(アスタリスク)、?(疑問符)、&(アンパサンド)、および文字列の先頭または末尾のスペース。LDAP プロバイダは、これらの特殊文字が設定プロパティの名前または DN に含まれていると処理することができません。また、以下に示す一部のプロパティではこれらの特殊文字を共通名に使用することができません。

使用開始にあたって

プロパティ	デフォルト値	説明
ServerType	なし	<p>(省略可能) 接続先の LDAP サーバのタイプ。</p> <ul style="list-style-type: none"> • sunone5 - SunOne 5.x または iPlanet 5.x • msad2k - Microsoft Active Directory、Windows 2000 • nsds4 - Netscape Directory Server 4.x • openldap - OpenLDAP Directory Server 2.x <p>選択する値によって、以下の認証プロパティのデフォルト値が設定される。</p> <ul style="list-style-type: none"> • RoleFilter • UserRoleMembership • RoleMemberAttributes • AuthenticationFilter • DigestMD5Authentication • UseUserAccountControl
ProviderURL	ldap://local-host:389	<p>LDAP サーバへの接続に使用される URL。サーバが次に該当する場合は、デフォルト値を使用する。</p> <ul style="list-style-type: none"> • 共通のセキュリティインフラストラクチャで有効になっている製品と同じマシンに置かれている。 • デフォルトポート (389) を使用するよう設定されている。 <p>それ以外の場合、値を設定する次の構文を使用する。</p> <p>ldap://<hostname>:<port></p>

プロパティ	デフォルト値	説明
Default-SearchBase	なし	<p>認証、役割、属性、自己登録に他の検索ベースが指定されていない場合に使用される LDAP 検索ベース。</p> <ol style="list-style-type: none"> dc=<domainname>,dc=<tld> たとえば、mycompany.com ドメインにあるマシンには dc=mycompany,dc=com の検索ベースがある。 o=<company name>,c=<country code> たとえば、Mycompany 組織内のマシンの場合、o=mycompany,c=us となる。 <hr/> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
SecurityProtocol	なし	<p>LDAP サーバへの接続に使用されるプロトコル。暗号化されたプロトコルを使用するには、URL で ldaps の代わりに ssl を使用する。</p>
AuthenticationMethod	Simple	<p>LDAP に対するすべての認証要求で使用される認証方法。一般に有効値は java.naming.security.authentication JNDI プロパティと同じ。次のいずれかを選択します。</p> <ul style="list-style-type: none"> simple - クリアテキストのパスワード認証を指定する。 DIGEST-MD5 - よりセキュアなハッシュパスワード認証。この方法では、サーバでプレーンテキストのパスワード記憶領域が使用される。また、JRE 1.4 以降でのみ機能する。

使用開始にあたって

プロパティ	デフォルト値	説明
AuthenticationFilter	ほとんどの LDAP サーバの場合: (&uid={uid})(objectclass=person) または Active Directory 電子メールのルックアップの場合: (&userPrincipalName={uid})(objectclass=user) [ActiveDirectory] Active Directory Windows ユーザ名のルックアップの場合: (&sAMAccountName={uid})(objectclass=user)	ユーザのルックアップ時に使用するフィルタ。 ユーザ名に基づいた検索を実行するときに、このフィルタを使用して、指定されたユーザ名と一致する LDAP エントリが判別される。 フィルタの文字列 "{uid}" は、指定されたユーザ名に置き換えられる。 注意: このプロパティを使用して SCC を認証するときの注意点: <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
AuthenticationScope	onelevel	認証の検索スコープ。サポートされる値は、次のとおり。 <ul style="list-style-type: none"> onelevel subtree 値が指定されていない場合、または無効な値が指定された場合、デフォルト値が使用される。

プロパティ	デフォルト値	説明
AuthenticationSearchBase	なし	<p>ユーザの認証に使用される検索ベース。このプロパティを設定しない場合は、DefaultSearchBase の値が使用される。</p> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
BindDN	なし	<p>初期 LDAP 接続を構築するときにバインドするユーザ DN。</p> <p>多くの場合、このユーザはすべてのユーザレコードでの読み込みパーミッションを必要とする。値を設定しない場合、匿名バインドが使用される。匿名バインドは、ほとんどのサーバで追加の設定なしで機能する。</p> <p>ただし、LDAP アトリビュータは、この DN を LDAP サーバのユーザの作成にも使用する可能性がある。自己登録機能が使用される場合、そのユーザにユーザレコードの作成に必須のパーミッションが必要な場合もある。このような動作は、useUserCredentialsToBind を true に設定していない場合に発生する可能性がある。この場合、LDAP アトリビュータは、この DN を使用して、ユーザ属性を更新する。</p>

プロパティ	デフォルト値	説明
BindPassword	なし	<p>任意のユーザの認証に使用される、BindDN のパスワード。 BindDN と BindPassword によって、LDAP 接続がユニットに分離される。</p> <p>AuthenticationMethod プロパティは、この初期接続に使用されるバインドメソッドの決定に使用される。</p> <p>SAP はパスワードの暗号化を推奨し、パスワード暗号化ユーティリティを提供している。 BindPassword を暗号化する場合は、オプションを設定する行に encrypted=true を含める。次に例を示します。</p> <pre><options name="BindPassword" encrypted="true" value="1snjikfwregfqr43hu5io..."/></pre> <p>BindPassword を暗号化しない場合、このオプションは次のようになる。</p> <pre><options name="BindPassword" value="s3cr3T"/></pre>
RoleSearch-Base	なし	<p>役割のリストの取得に使用される検索ベース。このプロパティを設定しない場合は、DefaultSearchBase の値が LDAP に使用される。</p> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。

プロパティ	デフォルト値	説明
RoleFilter	<p>SunONE/iPlanet の場合: (<code>&objectclass=ldapsubentry</code>) (<code>objectclass=nsrolededefinition</code>)</p> <p>Netscape Directory Server の場合: (<code> objectclass=groupofnames</code>) (<code>objectclass=groupofunique-names</code>)</p> <p>ActiveDirectory の場合: (<code> objectclass=groupofnames</code>) (<code>objectclass=group</code>)</p>	<p>役割検索フィルタ。このフィルタは役割検索ベースと役割スコープと組み合わせて使用すると、LDAP サーバ内の全役割のリストを返す。選択されたサーバタイプによってはいくつかのデフォルト値が存在する。サーバタイプを選択せず、このプロパティが初期化されていない場合は、役割を利用できない。</p> <hr/> <p>注意: このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
RoleMember-Attributes	<p>Netscape Directory Server と OpenLDAP サーバの場合: <code>member,uniquemember</code></p>	<p>この役割を付与されたユーザの DN を導出する際に LDAP で使用される役割属性のカンマ区切りリスト。これらの値は、ユーザの役割リストを決定するため、アクティブなユーザと相互参照される。このプロパティの使用例として、LDAP グループを役割のプレースホルダとして使用する場合がある。このプロパティには、Netscape サーバタイプが選択されたときのみデフォルト値がある。</p>
RoleNameAttribute	<code>cn</code>	<p>役割名として使用される役割エントリの属性。これは、役割リストに表示されるか、認証されたユーザに付与される役割名である。</p>
RoleScope	<code>onelevel</code>	<p>役割の検索スコープ。サポートされている値は次のとおり。</p> <ul style="list-style-type: none"> <code>onelevel</code> <code>subtree</code> <p>値が指定されていない場合、または無効な値が指定された場合、デフォルト値が使用される。</p>

プロパティ	デフォルト値	説明
SkipRole- Lookup	false	<p>RoleSearchBase および RoleFilter を使用してルックアップされた役割と相互参照しないで、プロパティ UserRoleMembershipAttributes によって指定された属性を使用してルックアップされた役割を付与するには、このプロパティを true に設定する。</p> <p>LDAP 設定の検証は、利用可能なすべての役割の一覧表示でエラーが発生しても、正常に完了する。エラーは検証時にサーバログに記録されるが、SCC にはレポートされず、設定の保存が可能になる。これは、役割マッピング用の物理的な役割を一覧表示するとき、および SCC に影響する。ユーザの認証を正常に行うには、SkipRoleLookup プロパティを true に設定する。</p>
UserRole- Membershi- pAttributes	<p>iPlanet/SunONE の場合: nsRoleDN</p> <p>Active Directory の場合: memberOf</p> <p>その他すべての場合: none</p>	<p>ユーザがメンバとして属するすべての役割の DN が含まれるユーザ属性を定義する。</p> <p>これらのカンマ区切り値は、役割検索ベースと検索フィルタで取得された役割と相互参照され、ユーザの役割のリストが生成される。</p> <p>SkipRoleSearch プロパティが true に設定されている場合、これらのカンマ区切り値は、役割検索ベースおよび役割検索フィルタで取得された役割と相互参照されない。「SkipRoleLookup」を参照。</p> <p>注意： ActiveDirectory でネストされたグループを使用する場合は、このプロパティを tokenGroups に設定する必要がある。</p>
UserFreeform- RoleMember- shipAttributes	なし	<p>自由形式の役割メンバシップ属性リスト。このカンマ区切りリストにある属性を持つユーザは、属性値と等しい名前を持つ役割へのアクセスが自動的に許可される。たとえば、このプロパティの値が department で、ユーザの LDAP レコードにおける department 属性の値が {sales, consulting} である場合、ユーザには sales と consulting という役割が付与される。</p>
Referral	ignore	<p>referral が発生したときの動作。有効な値は、LdapContext によって決定される値。ただし、follow、ignore、throw が含まれる場合がある。</p>

プロパティ	デフォルト値	説明
Di-gestMD5Authentication-Format	DN OpenLDAP の場合: User name	DIGEST-MD5 バインド認証 ID 形式。
UseUserAccountControlAttribute	Active Directory の場合: true	このプロパティを true に設定すると、UserAccountControl 属性で、無効化されたユーザアカウント、アカウントの期限切れ、パスワードの期限切れなどが検出される。ActiveDirectory ではこの属性を、上記情報の格納にも使用する。
EnableLDAP-Connection-Trace	False	LDAP 接続トレースを有効化する。出力は、temp ディレクトリのファイルに記録される。このファイルのロケーションはサーバログに記録される。
ConnectTimeout	0	LDAP サーバへの接続を確立しようとするときのタイムアウトをミリ秒単位で指定する。このプロパティ値により、設定された LDAP サーバへの接続を確立しようとするときに JNDI com.sun.jndi.ldap.connect.timeout プロパティが設定される。LDAP プロバイダが設定された期間内に接続を確立できない場合は、接続の試行がアボートされる。0 以下の整数値を使用すると、ネットワークプロトコルのタイムアウト値が使用される。
ReadTimeout	0	サーバへの初期接続の確立後、読み込み操作に対するサーバの応答をクライアントが待機する期間をミリ秒単位で制御する。このプロパティ値により、設定された LDAP サーバへの接続を確立しようとするときに JNDI com.sun.jndi.ldap.read.timeout プロパティが設定される。LDAP プロバイダが設定された期間内に LDAP 応答を取得できない場合は、読み込みの試行がアボートされる。読み込みタイムアウトは、サーバとの初期接続が確立された後のサーバからの LDAP 応答に適用される。0 以下の整数値は、読み込みタイムアウトが指定されないことを意味する。

プロパティ	デフォルト値	説明
LDAPPool- MaxActive	8	LDAP サーバへの同時 LDAP 接続の数を制限する。正の数値以外の数値は、制限がないことを示す。このオプションが複数の LDAP プロバイダに設定されていると、最初の LDAP プロバイダによって設定された値がロードされ、他のすべての値よりも優先される。LDAPPoolMaxActive に達すると、その後で LDAP プロバイダクラスがプールから LDAP 接続を借用しようとしても、新しいオブジェクトまたはアイドル状態のオブジェクトがプールで利用可能になるまで、無期限にブロックされる。接続プールによって、設定された LDAP サーバに確立される TCP 接続の数が管理されるため、LDAP プロバイダのパフォーマンスとリソース使用率が向上する。
controlFlag	オプション	複数の認証プロバイダを設定する場合は、各プロバイダに controlFlag を使用して、ログインシーケンスでの認証プロバイダの使用方法を制御する。 controlFlag は、LDAP 設定プロパティよりも一般的なログインモジュールである。

LDAP または OS グループに対する SAP Control Center の役割のマッピング

LDAP またはオペレーティングシステムを介して認証されたユーザに SAP Control Center 権限を付与するには、SAP Control Center で使用される役割を LDAP またはオペレーティングシステムのグループに関連付けます。

前提条件

- LDAP と UNIX に必要: 認証モジュールの設定。
- オプション: SCC 認証を提供するシステム (LDAP または OS) に以下のグループを作成して SAP Control Center ユーザに割り当てます。
 - sybase - sccUserRole を付与します。すべての SCC ユーザを sybase グループに割り当てます。
 - SCC Administrator - sccAdminRole を付与します。SCC 管理者ユーザのみをこのグループに割り当てます。

手順

SAP Control Center は、ローカルオペレーティングシステムまたは LDAP サーバを介してユーザを認証できるように設定できます。このタイプの認証作業を実行す

るには、認証を提供するシステム (LDAP またはオペレーティングシステム) に存在するグループに SCC の役割をマッピングする必要があります。

sybase および SCC 管理者グループは、role-mapping.xml で事前定義されているため、便利に使用できます。sybase および SCC 管理者グループを LDAP システムに追加して、SCC ユーザおよび管理者にその値を入力すると、次のタスクを省略できます。つまり、下記の手順を実行する必要がなくなります。

次の表は、SCC の役割に対する LDAP と OS グループのデフォルトのマッピングのリストです。ログインモジュールは、csi_config.xml で定義されています。

ログインモジュール	OS グループ	SAP Control Center の役割
UNIX プロキシ	root	uaAnonymous、uaAgentAdmin、uaOSAdmin
	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	user	uaAnonymous
	guest	uaAnonymous
NT プロキシ	Administrators	uaAnonymous、uaAgentAdmin、uaOSAdmin
	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	Users	uaAnonymous
	Guests	uaAnonymous
LDAP	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	SCC Administrator	uaAnonymous、sccAdminRole

マッピングの実行には次の 2 つの方法があります。

- (推奨) SAP Control Center がユーザの認証に使用するオペレーティングシステムまたは LDAP サーバに "sybase" グループと "SCC Administrator" グループを追加し、SAP Control Center にアクセスする必要があるすべてのユーザをこれらのグループの一方または両方に追加します。
- role-mapping.xml ファイルを編集して、LDAP またはオペレーティングシステムの既存グループを使用するように SAP Control Center を設定します。このオプションについて次に説明します。

1. SAP Control Center が起動している場合は停止します。
2. テキストエディタで次のファイルを開きます。

```
<SCC-install-directory>/conf/role-mapping.xml
```

3. ファイルで `sccUserRole` セクションを探します。

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
</Mapping>
```

4. SCC ユーザの認証に使用している LDAP または OS グループの `MappedName` 行を追加します。 `sccUserRole` セクションは次のようになります。

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
  <MappedName>my_SCC_group</MappedName>
</Mapping>
```

5. ファイルで `sccAdminRole` セクションを探します。

```
<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
</Mapping>
```

6. SCC 管理者の認証に使用している LDAP または OS グループの `MappedName` 行を追加します。 `sccAdminRole` セクションは次のようになります。

```
<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>my_SCC_admin_group</MappedName>
</Mapping>
```

7. ファイルを保存して終了します。

8. (LDAP のみ) LDAP レポジトリで定義された役割が `role-mapping.xml` で定義された役割と一致していることを確認します。

9. `<SCC-install-dir>%conf%csi_config.xml` ファイルで、`BindPassword` プロパティと `ProviderURL` プロパティを配備内で使用される値に設定します。
Sybase では、機密情報に関連する値を暗号化してから `csi_config.xml` に保存することをおすすめします。

10. SAP Control Center を起動します。

参照：

- LDAP 認証モジュールの設定 (38 ページ)

パスワードの暗号化

テキストファイルに保存している間、安全に保つ必要があるパスワードなどの値を暗号化するには、**passencrypt** ユーティリティを使用します。

暗号化パスワードは設定ファイルに安全に保存できます。**passencrypt** の実行時、およびログイン時に、パスワードをクリアテキスト (暗号化されていない) で入力します。

SAP Control Center の bin ディレクトリにある **passencrypt** は、`csi_config.xml` の `PreConfiguredLoginModule` で使用されるパスワードに SHA-256 ハッシュアルゴリズムを使用します。

1. コマンドウィンドウを開き、bin ディレクトリに移動します。

Windows の場合： `cd <SCC-install-directory>\bin`

UNIX の場合： `cd <SCC-install-directory>/bin`

2. パスワードを暗号化するには、**passencrypt -csi** と入力します。その結果表示されたプロンプトで、新しいパスワードを入力します。
passencrypt は、入力したパスワード (画面には表示されません) を暗号化し、暗号化した形式でパスワードを表示します。
3. 暗号化されたパスワードをコピーします。
4. 暗号化されたパスワードを必要な場所に貼り付けます。

ポートの設定

(オプション) **scc --port** コマンドを使用して、SAP Control Center サービスを新しいポートに割り当てます。

前提条件

SAP Control Center と、同じホストで実行されているその他のソフトウェアとの間のポートの競合を確認します。

手順

SAP Control Center は、他のサービスがポートを使用していると適切に動作できません。右カラムの下に一覧表示されているポートで競合を発見したら、他のサービスのポートを再設定するか、ここで説明するように SAP Control Center を再設定します。

使用開始にあたって

ポート名	説明	サービス名	プロパティ名	デフォルトのポート
db	データベースポート SCC サーバ上に存在	SccSADataserver メッセージング アラート スケジューラ	com.sybase.asa. server.port messaging.db. port alert.database. port org.quartz.data- Source.ASA. URL	3638
http	Web HTTP ポート SCC サーバ上に存在	EmbeddedWeb- Container	http.port	8282
https	Web HTTPS (セキュア HTTP) ポート SCC サーバ上に存在	EmbeddedWeb- Container	https.port	8283
jiniHttp	JINI HTTP サーバ SCC サーバと SCC エージェントに存在	Jini	httpPort	9092
jiniRmid	JINI リモートメソッド呼び出しデー モン SCC サーバと SCC エージェントに存在	Jini	rmidPort	9095
msg	メッセージングポート SCC サーバ上に存在	メッセージング	messaging.port	2000
rmi	RMI ポート SCC サーバと SCC エージェントに存在	RMI	port	9999
tds	Tabular Data Stream™ ポート (他の SAP データベース製品との通信に使用さ れる) SCC サーバと SCC エージェントに存在	Tds	tdsPort	9998

1. SAP Control Center を停止します。
2. **scc --info ports** を実行して、SAP Control Center サービスのリストとそのプロパティおよび割り当てられているポートを表示します。
3. ポートを再割り当てするには、コマンドを次の形式のいずれかで入力します。

```
scc --port port-name=port-number
```

```
scc --port service-name:property-name=port-number
```

データベースサービスが別のポートを使用するように設定する場合を除き、最初の簡潔な形式を使用します(デフォルトでは、すべてが同じポートを使用します)。
4. SAP Control Center を起動します。
5. **scc --info ports** を再度実行して、ポートが再割り当てされたことを確認します。

例

4つのデータベースサービス(データサーバ、メッセージング、データベースアラート、およびスケジューラ)のすべてを同じポート 3639 に設定します(データベースは、SAP Control Center 内部レポジトリに使用される SAP® SQL Anywhere®)。

```
scc --port db=3639
```

データベースメッセージングサービスだけをポート 3639 に設定します。

```
scc --port Messaging:messaging.db.port=3639
```

HTTP ポートを 9292 に設定します。

```
scc --port http=9292
```

Jini RMI デーモンをポート 9696 に設定します。

```
scc --port jiniRmid=9696
```

メインの SAP Control Center メッセージングサービスをポート 2001 に設定します。

```
scc --port msg=2001
```

RMI ポートを 9991 に設定します。

```
scc --port rmi=9991
```

Tabular Data Stream ポートを 9997 に設定します。

```
scc --port tds=9997
```

注意： **scc** コマンドでポート設定オプション (**-p** または **--port**) を使用すると、SAP Control Center は起動しません。SCC を起動するには、別の **scc** コマンドを実行します。

自動ログアウトタイマの設定

(オプション) ユーザが長時間にわたって非アクティブな場合にログインセッションを停止するように、SAP Control Center を設定します。

前提条件

SAP Control Center を起動して、管理者権限を持つアカウントでログインします。(ログインアカウントまたはそのグループに `sccAdminRole` が設定されている必要があります)。

手順

1. アプリケーションのメニューバーから、[Application] > [Administration] を選択します。
2. [General Settings] を選択します。
3. [Auto-Logout] タブをクリックします。
4. アイドルユーザが自動的にログアウトされるまでの経過時間を分単位で入力します。
自動ログアウトを無効にするには、0 を入力するか、ボックスを空のままにします。
5. [OK] をクリック (変更内容を適用して、プロパティダイアログを閉じる) するか、[Apply] をクリック (変更内容を適用して、ダイアログは閉じない) します。

参照:

- セキュリティのセットアップ (33 ページ)

ユーザ承認

SAP Control Center での権限メカニズムには、ログインアカウントとタスクベースの役割が使用されます。

SAP Control Center へのアクセスはログインアカウントによって制御されます。パーミッションでは、特定のタイプのサーバの管理とモニタリングなど、ユーザが SCC で実行できるタスクを制御する、定義済みの役割が割り当てられます。これらの役割は、ログインアカウントまたはグループに直接割り当てることができます。ログインアカウントの役割は、そのログインアカウントが属するグループの役割を継承します。コンポーネント製品モジュールで、一部の役割は自動的に割り当てられます。

SAP Control Center では役割が次のように分類されます。

- システム標準の役割 - ユーザがどのように SCC と対話できるようにするかを定義します。
- 製品ごとの役割 - SCC で管理されている特定のリソース (たとえば、RepBoston01 という名前の Replication Server) とユーザがどのように対話できるようにするかを定義します。

注意： ここで説明されているツールは、SCC 対応のログインアカウントを管理するためのツールです。管理対象リソースで作成されたアカウントとグループは、これらのツールで管理できません。

参照：

- 設定 (58 ページ)

ログインまたはグループへの役割の割り当て

セキュリティ設定オプションを使用して、1つ以上の役割を SAP Control Center のログインアカウントまたはグループに追加します。これらの役割は、ユーザがサーバのモニタや SAP Control Center の管理などのタスクを実行できるようにします。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。サーバのモニタリング役割を割り当てるには、まずサーバを登録します。

手順

SAP Control Center で管理タスクを実行する任意のログインアカウントに sccAdminRole を割り当てます。

1. アプリケーションのメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Logins] または [Groups] をクリックします。
4. 表から、役割を割り当てるログインアカウントまたはグループを選択します。
5. [役割] タブをクリックします。
6. [Available roles for resource] リストで、ロールを選択してから [Add] をクリックします。たとえば、管理者権限を付与するには、SCC サービス sccAdminRole を追加します。モニタ権限を付与するには、該当するサーバとサーバタイプの MonitorRole を追加します。

注意： SAP Control Center 製品モジュールでは特定の役割が自動的に割り当てられるため、MonitorRole の追加が不要な場合もあります。

使用開始にあたって

[Has following roles] リストに役割が表示される場合、このアカウントまたはグループがその役割にすでに設定されています。

7. [OK] をクリックします。

参照：

- グループの追加 (56 ページ)
- グループへのログインアカウントの追加 (56 ページ)
- ログイン、役割、グループ (57 ページ)

グループの追加

新しいグループを作成するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

グループを使用すると、役割が管理しやすくなります。役割を個々のユーザに割り当ててではなく、役割をグループに割り当て、必要に応じて、そのグループにユーザを追加するか、またはグループからユーザを削除します。

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Groups] を選択します。
4. [Create Group] をクリックします。
5. グループ名と説明を入力します。
6. [Finish] をクリックします。

参照：

- ログインまたはグループへの役割の割り当て (55 ページ)
- グループへのログインアカウントの追加 (56 ページ)
- ログイン、役割、グループ (57 ページ)

グループへのログインアカウントの追加

1つ以上のログインアカウントをグループに追加するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Groups] をクリックします。
4. アカウントを割り当てるグループを選択します。
5. [Membership] タブをクリックします。
6. アカウントを選択し、[Add] をクリックします。
7. [OK] をクリックします。

参照：

- ログインまたはグループへの役割の割り当て (55 ページ)
- グループの追加 (56 ページ)
- ログイン、役割、グループ (57 ページ)

ログイン、役割、グループ

SAP Control Center には、事前に定義されたログインアカウントと役割があります。

ログインアカウントは、SAP Control Center に接続可能なユーザを特定します。アカウントには、そのユーザが実行できるタスクを制御する役割があります。ネイティブの SCC アカウントを使用してユーザを認証できますが、オペレーティングシステムまたは LDAP ディレクトリサービスに認証を委任する方法のほうが安全です。

SCC には事前定義されたログインアカウントが付属しています。事前定義されたアカウントは、SAP Control Center のインストール、設定、およびテストのみに使用することをおすすめします。このアカウントは、実際の運用環境での使用を想定していません。

表 8：事前定義されたログインアカウント

ログイン名	説明
sccadmin	SAP Control Center の管理機能のすべてを使用できる。設定およびテストに使用する。

役割は、ログインアカウントまたはグループに割り当てることができる、事前定義されたプロファイルです。役割は、ログインアカウントのアクセス権を制御します。SCC には、実際の運用環境での使用を想定した事前定義された役割が付属しています。

表 9 : 事前定義された役割

役割	説明
sccUserRole	SAP Control Center の管理作業以外のアクセスを提供する。すべてのユーザに必須で、認証されたすべてのユーザに自動的に割り当てられる。
sccAdminRole	SAP Control Center を管理するための管理権限を提供する。

SCC 製品モジュールのモニタ権限は、自動的に割り当てられます。

グループは、1つ以上のログインアカウントで構成されます。1つのグループ内のすべてのアカウントに、そのグループに付与された役割が割り当てられます。SCC では、ビジネス要件に応じてグループを作成できます。

参照：

- ログインまたはグループへの役割の割り当て (55 ページ)
- グループの追加 (56 ページ)
- グループへのログインアカウントの追加 (56 ページ)

設定

SAP Sybase Control Center for Data Assurance を設定します。

注意： SAP Control Center を運用環境用に設定する前に、ヘルプの「使用開始にあたって」セクションのタスクを完了しておきます。セキュリティの設定は、特に重要です。

1. Data Assurance サーバのモニタリング設定

SAP Control Center を使用して監視する Data Assurance (DA) サーバを認証します。リソースが認証されると、SAP Control Center によって DA サーバ監視オプションが有効になります。

2. Data Assurance サーバの登録

リソース (モニタ対象として使用可能なサーバなど) を登録して、SAP Control Center がそのリソースと接続情報を認識できるようにします。

3. 一括登録のためのリソースのインポート

(オプション) 複数のサーバを interfaces または sql.ini ファイルからインポートして登録します。

4. 管理対象リソースのログインアカウントの認証

SAP Control Center がサーバまたはエージェントに接続して監視データを収集したりリソースを管理したりする場合に使用するログインアカウントとパスワードを指定します。

5. 統計収集のセットアップ
データ収集ジョブを作成し、スケジュールをジョブに追加するには、管理対象リソースの [Properties] ビューを使用します。
6. エージェント接続の作成
compareset およびスキーマジョブの作成に必要な Data Assurance (DA) エージェント接続を作成します。
7. データベース接続の作成
Data Assurance (DA) サーバにプライマリデータベース接続および複製データベース接続を設定します。
8. interface ファイルからの単一接続またはクラスタ接続の作成
interface ファイルから Data Assurance (DA) リソースをインポートします。
9. オプションの設定手順
ユーザ認証、アラート、データ収集スケジューリング、バックアップ、レポートの設定除去オプションを含む詳細な設定を実行します。

参照：

- ユーザ承認 (54 ページ)
- ログイン、役割、グループ (106 ページ)
- セキュリティのセットアップ (78 ページ)
- ログインまたはグループへの役割の割り当て (100 ページ)

SAP Control Center の起動

scc コマンドを使用して SAP Control Center を起動します。

前提条件

SAP Control Center に使用するブラウザに Adobe Flash Player をインストールします。

手順

1. SAP Control Center を起動します。
 - Windows - <install_location>\\$SCC-3_3\bin に移動して **scc.bat** をダブルクリックします。
 - UNIX - **scc.sh** を実行します。

起動の進捗に関するメッセージがコマンドウィンドウに表示されます。SAP Control Center が実行されていると、コマンドウィンドウは SAP Control Center

使用開始にあたって

コンソールになります。コマンドを発行して、SCC とそのポート、プラグイン、サービスに関するステータス情報を取得できます。

2. Web ブラウザを起動し、`https://<hostname>:8283/scc` を入力します。

参照：

- SAP Control Center コンソール (165 ページ)

Windows での ODBC ドライバの登録

Windows で、管理者権限を使用して **scc.bat** を実行し、ODBC ドライバを登録します。

Windows マシンで SAP Control Center を初めて起動すると、ODBC ドライバが登録されます。ODBC ドライバの自動登録では、レジストリ設定が編集されるため、引き上げた管理者権限を使用して **scc.bat** を実行する必要があります。十分な権限なしで初回の起動を行うと、エラーが発生し起動に失敗します。

Windows 2008、Windows 7、および Windows 8 では、すでに管理者権限を持っている場合でも [管理者として実行] 設定を使用して SCC を起動する必要があります。このプロセスについて次に説明します。

Windows のその他のバージョンでは、初めて SCC を起動する場合、管理者としてログインしている必要があります。次の手順に従う必要はありません。

1. Windows 2008、Windows 7、または Windows 8 では、管理者権限を使用してコマンドプロンプトウィンドウを開きます。
 - [スタート]>[すべてのプログラム]>[アクセサリ] を選択します。[コマンドプロンプト] を右クリックし、[管理者として実行] を選択します。
 - または、[スタート] メニューの [検索] ボックスに **cmd** と入力し、文にカーソルを合わせ、[Shift+Ctrl+Enter] キーを押します。
2. **scc.bat** を実行します。

Windows での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントを起動および停止する方法は複数あります。SAP Control Center または SCC エージェントは手動で起動できます。これは、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

このトピックは、SAP Control Center (管理 UI を含むサーバ) および SCC で管理される各製品サーバで実行される SCC エージェントの両方に適用されます。インストーラで両方のオプションを選択して同じディレクトリに SCC と SCC エージェントをインストールした場合、単一のコマンドを実行するか、単一のサービスを制御することで、常にそれらを一緒に起動および停止します。このトピックは、シ

シングルトンインストール (共有ディスクを使用しない)、および共有ディスクから実行されている SCC エージェントとサーバのインスタンスの両方に適用されません。

SAP Control Center または SCC エージェントを手動で実行する場合、起動または停止のたびにコマンドを発行する必要があります。サービスとして実行する場合 (推奨)、それが自動的に起動および再起動されるように設定することができます。オプションは次のとおりです。

- **scc.bat** コマンドを使用して SCC または SCC エージェントを手動で起動します。このコマンドにより、SCC コンソールにアクセスできます。このコンソールを使用して、サービスを停止したり、サービス、ポート、システムプロパティ、および環境変数に関する情報を表示できます。さらに、**scc.bat** は、トラブルシューティングの目的でログレベルを変更するために使用することもできます。**scc.bat** を使用すると、サービスで使用可能な自動起動と再起動の機能を利用できません。
- SCC サーバまたはエージェントの SAP Control Center サービスを起動、停止、設定するには、Windows の [コントロールパネル] の [サービス] リストを使用します。
- **net start** コマンドと **net stop** コマンドを使用します。これは、サービスとして実行されるように SAP Control Center または SCC エージェントを設定するもう 1 つの方法です。

注意： SCC エージェントまたはサーバをサービスとして起動するには、次の手順を実行します。

- シングルトンインストールでサービスとしてエージェントまたはサーバをインストールするには、インストーラで [はい] を選択しておく必要があります。
 - 共有ディスクインストールの場合、エージェントやサーバは、**sccinstance** コマンドの **-service** オプションを使用して展開されている必要があります。
-

シングルトンインストールでは、SCC または SCC エージェントをサービスとして起動することができ、サービスが自動的に再起動されるように設定します。起動の前に、Windows の [サービス] リストに SAP Control Center サービスがあることを確認します。

次に、起動/停止オプションごとの手順を説明します。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) を起動します。**
 - a) (SCC エージェントの場合はこの手順を省略します。) Windows 2008、Windows 7、または Windows 8 で初めて SAP Control Center を起動する場合、SAP Control Center の ODBC ドライバを登録できるようにコマンドプロンプ

使用開始にあたって

トで [管理者として実行] オプションを設定します (これは、システム管理者としてログインしている場合にも必要です)。

- b) **scc** コマンドを入力します。

シングルトンインストールの場合:

```
%SYBASE%\¥SCC-3_3¥bin¥scc.bat
```

インスタンスの場合:

```
%SYBASE%\¥SCC-3_3¥bin¥scc.bat -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center** または **SCC エージェント** (一緒にインストールされている場合は両方) を停止します。

- a) **scc --stop** コマンドを入力します。

シングルトンインストールの場合:

```
%SYBASE%\¥SCC-3_3¥bin¥scc.bat --stop
```

インスタンスの場合:

```
%SYBASE%\¥SCC-3_3¥bin¥scc.bat --stop -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

注意: また、`scc-console>` プロンプトで、**shutdown** を入力することもできます。

- **Windows** の [コントロール パネル] から **起動または停止し、自動起動と再起動を設定** します。

- a) Windows の [コントロール パネル] を開きます。

- b) [Administrative Tools] > [Services] を選択します。

- c) [サービス] リストで “SAP Control Center” を見つけます。 インスタンス用のサービスの場合はリリース番号が付いている場合があります。 またインスタンス名が付いている場合もあります。 サービス名では、エージェントとサーバは区別されません。 サービスが実行されている場合、[状態] 列には [開始] と表示されます。

- d) サービスを起動または停止するには、[Services] リストで [SAP Control Center] エントリを右クリックし、[Start] または [Stop] を選択します。

- e) 自動起動を設定するには、サービスをダブルクリックします。
 - f) マシンの起動時にサービスが自動的に起動するように設定するには、[Startup type] を [Automatic] に変更します。
 - g) 障害が発生した場合にサービスを再起動するには、[Recovery] タブを選択し、[First]、[Second]、[Subsequent] のエラーを [Restart Service] に変更します。
 - h) [Apply] をクリックして変更を保存してから、ダイアログボックスを閉じます。
- **Windows のコマンドラインから SAP Control Center サービス (SAP Control Center と SCC エージェントのいずれか一方または両方を制御する) を起動または停止します。**

- a) サービスを起動するには、**net start** コマンドを入力します。

シングルトンインストールの場合:

```
net start "SAP control center 3.3"
```

```
The SAP Control Center 3.3 service is starting.....
The SAP Control Center 3.3 service was started
successfully.
```

インスタンスの場合、インスタンス名 (この例では Boston-1) をカッコに含めます。

```
net start "SAP control center 3.3 (Boston-1)"
```

```
The SAP Control Center 3.3 (Boston-1) service is
starting.....
The SAP Control Center 3.3 (Boston-1) service was started
successfully.
```

- b) サービスを停止するには、**net stop** コマンドを入力します。

シングルトンインストールの場合:

```
net stop "SAP control center 3.3"
```

```
The SAP Control Center 3.3 service is stopping.....
The SAP Control Center 3.3 service was stopped
successfully.
```

インスタンスの場合、インスタンス名 (この例では Boston-1) をカッコに含めます。

```
net stop "SAP control center 3.3 (Boston-1)"
```

```
The SAP Control Center 3.3 (Boston-1) service is
stopping.....
```

```
The SAP Control Center 3.3 (Boston-1) service was stopped successfully.
```

UNIX での SAP Control Center の起動と停止

SAP Control Center または SCC エージェントは手動で起動できます。これは、テストやトラブルシューティングに便利です。また、サービスが自動的に起動され、障害発生時には再起動されるように設定することもできます。

このトピックは、SAP Control Center (管理 UI を含むサーバ) および SCC で管理される各製品サーバで実行される SAP Control Center エージェントの両方に適用されます。インストーラで両方のオプションを選択して同じディレクトリに SCC と SCC エージェントをインストールした場合、単一のコマンドを実行するか、単一のサービスを制御することで、それらを一緒に起動および停止します。このトピックは、シングルインストール (共有ディスクを使用しない)、および共有ディスクから実行されている SCC エージェントとサーバのインスタンスの両方に適用されます。

SAP Control Center または SCC エージェントを手動で起動する場合、起動または停止のたびにコマンドを発行する必要があります。サービスとして実行する場合 (推奨)、それが自動的に起動および再起動されるように設定することができます。オプションは次のとおりです。

- **scc.sh** スクリプトを使用して SAP Control Center または SCC エージェントを手動で起動します。次のいずれかの方法を使用できます。
 - フォアグラウンドで **scc.sh** を実行し、SCC コンソールにアクセスします。このコンソールを使用して、サービスを停止したり、サービス、ポート、システムプロパティ、および環境変数に関する情報を表示できます。
 - バックグラウンドで **scc.sh** を実行し、SCC コンソールが表示されないようにします。

トラブルシューティングのためにデフォルト以外のログレベルで SAP Control Center を実行するには、**scc.sh** を使用します。**scc.sh** を使用して手動で起動すると、サービスで使用可能な自動起動と再起動の機能を利用できません。

- **sccd** スクリプトを使用して SCC または SCC エージェントが自動的に起動されるように設定します。

次に、起動/停止オプションごとの手順を説明します。

- **SAP Control Center または SCC エージェントを初めて起動する前に、環境変数を設定します。** これは、一度だけ行います。
 - a) SAP Control Center インストールディレクトリの親ディレクトリに変更します (通常、親ディレクトリは `/opt/sap` または `opt/sybase` です)。
 - b) 次のいずれかを実行して、環境変数を設定します。

Bourne シェル :

```
. SYBASE.sh
```

C シェル :

```
source SYBASE.csh
```

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) をフォアグラウンドで実行します。**

フォアグラウンドでの実行は、手動で起動する場合の方法です。SCC または SCC エージェントを停止して再起動するには、コマンドを発行する必要があります。

- a) SCC または SCC エージェントを起動し、起動シーケンスの終了時にコンソールにそれをドロップするには、**scc** コマンドを入力します。

シングルトンインストールの場合:

```
$SYBASE/SCC-3_3/bin/scc.sh
```

インスタンスの場合:

```
$SYBASE/SCC-3_3/bin/scc.sh -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) をバックグラウンドで実行します。**

nohup、**&**、および **>** を使用すると、SAP Control Center または SCC エージェントをバックグラウンドで実行し、出力とシステムエラーをファイルにリダイレクトし、SCC コンソールを非表示にすることができます。バックグラウンドでの実行は、手動で起動する場合の方法です。SCC または SCC エージェントを停止して再起動するには、コマンドを発行する必要があります。

- a) シェルに対応する次のサンプルと同様のコマンドを実行します。サンプルコマンドはどちらも `scc-console.out` ファイルに出力をダイレクトします。出力ファイルがすでに存在する場合は、その他のシェル演算子を使用してファイルに追加したり、ファイルをトランケートすることが必要になることがあります。

Bourne shell (sh) または Bash

シングルトンインストールの場合 :

```
nohup ./scc.sh 2>&1 > scc-console.out &
```

インスタンスの場合 :

```
nohup ./scc.sh -instance <instance-name> 2>&1 > scc-console-your-instance.out &
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

C シェル

使用開始にあたって

シングルトンインストールの場合：

```
nohup ./scc.sh >& scc-console.out &
```

インスタンスの場合：

```
nohup ./scc.sh -instance <instance-name> >& scc-console.out &
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **SAP Control Center または SCC エージェント (一緒にインストールされている場合は両方) を停止します。**

- a) `scc-console>` プロンプトから停止するには、次のように入力します。

```
shutdown
```

警告！ UNIX のプロンプトで **shutdown** と入力しないでください。入力すると、オペレーティングシステムがシャットダウンしてしまいます。

UNIX コマンドラインから停止するには、**scc --stop** コマンドを入力します。

シングルトンインストールの場合：

```
$(SYBASE)/SCC-3_3/bin/scc.sh --stop
```

インスタンスの場合：

```
$(SYBASE)/SCC-3_3/bin/scc.sh --stop -instance <instance-name>
```

インスタンスの名前がホスト名と同じ場合は (デフォルト)、**-instance** オプションを省略できます。

- **サービスとして実行されるように SAP Control Center または SCC エージェントを設定します。**

UNIX サービスは、マシンの起動後に自動的に開始され、バックグラウンドで実行されるデーモンプロセスです。SCC の UNIX インストールには、シェルスクリプト **sccd** が含まれています。このシェルスクリプトを使用して SCC サービスを設定できます (一部の UNIX プラットフォームでは、サービスの設定を容易にするツールが提供されています。Linux **chkconfig** はその例です)。

注意： SAP では、UNIX でのサービスの設定に慣れていないユーザは、この作業をシステム管理者に任せるか、UNIX プラットフォームのシステム管理のマニュアルを参照することをおすすめします。

- a) `$(SYBASE)/SCC-3_3/bin/sccd` を次のディレクトリにコピーします。

- AIX (SCC エージェントのみ)： `/etc/rc.d/init.d`
- HP-UX (SCC エージェントのみ)： `/sbin/init.d`
- その他のプラットフォーム： `/etc/init.d`

b) sccd を開き、次の変更を加えます。

- SYBASE 変数を設定する行を SAP Sybase インストールのロケーション (SAP Control Center インストールディレクトリ scc-3_3 の親) に変更します。Sybase 製品または環境変数がすでに存在するマシンに SCC がインストールされている場合、このディレクトリ名はデフォルトで /opt/sybase です。それ以外の場合、デフォルトの親ディレクトリは /opt/sap です。
- 共有ディスクモードを使用していない場合、または共有ディスクモードを使用してホスト名と同じ名前の単一インスタンスを実行している場合は、手順 5.c (67 ページ) または手順 5.d (67 ページ) にスキップします。
- 共有ディスクモードを使用してホスト名とは異なる名前の単一インスタンスを実行している場合、または同じホスト上で複数のインスタンスを実行している場合は、スクリプト名にインスタンス名を追加します。

```
SCRIPT_NAME=scc.sh
```

上記を次のように変更します。

```
SCRIPT_NAME="scc.sh -instance <instance-name>"
```

- 共有ディスクモードを使用して同じホスト上で複数のインスタンスを実行している場合は、出力ログファイルの名前にインスタンス名を追加します。

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service.out &
```

上記を次のように変更します。

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service_<instance-name>.out &
```

- 共有ディスクモードを使用して、同じホストで複数のインスタンスを実行する場合、インスタンスごとに sccd スクリプトのコピーを一意の名前で保存します。各コピーで、スクリプト名にインスタンス名を追加し、さらにインスタンス名を前述のように出力ログファイル名に追加します。sccd のコピーごとに残りの手順を実行します。

c) Linux の場合は、サービスがランレベル 2、3、4、5 で実行されるように設定します。

```
/usr/sbin/chkconfig --add sccd  
/usr/sbin/chkconfig --level 2345 sccd
```

sccd スクリプトは、/usr/sbin/service sccd status を使用してテストできます (**service** コマンドでは次のオプションが受け入れられます。

start | stop | status | restart)。

d) Linux 以外のプラットフォームでは、次のディレクトリを検索します。

- AIX (SCC エージェントのみ)： /etc/rc.d/rc<X>.d

使用開始にあたって

- HP-UX (SCC エージェントのみ) : /sbin/rc<X>.d
- Solaris の場合 : /etc/rc<X>.d

ここで、<X> はランレベル (たとえば 3) です。ご使用のプラットフォームのディレクトリに 2 つのソフトリンクを作成して、次を参照するようにリンクを設定します。

- AIX (SCC エージェントのみ) :
/etc/rc.d/init.d/sccd: S90sccd および
/etc/rc.d/init.d/sccd: K10sccd
- HP-UX (SCC エージェントのみ) :
/sbin/init.d/sccd: S90sccd および
/sbin/init.d/sccd: K10sccd
- Solaris の場合 :
/etc/init.d/sccd: S90sccd および
/etc/init.d/sccd: K10sccd

S90sccd リンクはサービスを起動し、K10sccd リンクはサービスを停止します。リンク内の 2 桁の数値は、サービスの起動と停止の優先度を示します。

- e) S90sccd リンクと K10sccd リンクを使用してサービスの起動と停止をテストします。リンクは、マシンの起動時または停止時に自動的に呼び出されます。

メモリ使用の設定

(オプション) SAP Control Center によって使用されるメモリサイズを設定する必要があるかどうか、および必要がある場合に使用する設定方法を決定します。

通常は、SAP Control Center のメモリの使用量を設定する必要はありません。この表では、設定できるメモリのオプションと、変更を考える必要がある状況を示します。

変更する値	状況	ガイドライン
<p>最大メモリ</p> <ul style="list-style-type: none"> • <code>jvmopt=-Xmx</code> - SAP Control Center を Windows サービスとして実行している場合 • <code>SCC_MEM_MAX</code> - SCC を UNIX サービスとして実行している場合 • <code>SCC_MEM_MAX</code> - コマンドラインから SCC を起動している場合 	<ul style="list-style-type: none"> • 指定したサイズよりも多くのメモリが SAP Control Center によって使用されるのを防ぐ必要がある場合 • SAP Control Center fails to start and may display an error: Could not create the Java virtual machine. • OutOfMemory エラーが、SAP Control Center のヒープスペースが不足していることを示している。 • 起動プロセス時にシステムメモリについての警告メッセージが表示される場合 • SAP Control Center がインストールされているマシンのメモリが 4GB 未満である (メモリが 4GB 未満のマシンで SAP Control Center を起動すると、システムメモリに関する起動警告メッセージがトリガされる)。 	<p>メモリが 4GB 未満のマシンでは、最大メモリを 256MB 以上に設定する。</p> <p>デフォルト値：なし (メモリが 4GB 以上のマシンでは、最大メモリは動的に設定され、システムメモリの量によってのみ効率的に制限される)。</p>

変更する値	状況	ガイドライン
永続メモリ <ul style="list-style-type: none"> • <code>jvmopt=-XX:MaxPermSize</code> - SAP Control Center を Windows サービスとして実行している場合 • <code>SCC_MEM_PERM</code> - SCC を UNIX サービスとして実行している場合 • <code>SCC_MEM_PERM</code> - コマンドラインから SCC を起動している場合 	OutOfMemory エラーが、SAP Control Center の永続的な生成領域が不足していることを示している。	32MB 単位でメモリを増やす。デフォルト値の 2 倍に設定しても OutOfMemory エラーが表示される場合、SAP テクニカルサポートに問い合わせる。 デフォルト値：128MB

メモリオプションは、次の 2 つの方法で変更できます。

- コマンドラインから起動された SAP Control Center の場合 - `scc` コマンドを実行して SAP Control Center を起動する前に、コマンドを実行して 1 つ以上の環境変数を設定します。この方法を使用する場合、メモリオプションの変更は現在のログインセッションの間だけ継続します。この方法は、新しいオプションの値をテストする場合に便利です。
- SAP Control Center サービスの場合 - SAP Control Center サービスに使用されるファイルを変更します。この方法を使用する場合、メモリオプションの変更は永続的です。SAP Control Center がサービスとして起動するたびに変更したオプションが使用されます。

コマンドラインでのメモリオプションの変更

コマンドラインから SAP Control Center を起動する前に、メモリオプションの値を一時的に変更するコマンドを発行できます。

この方法を使用して行った変更は、現在のログインセッションの間のみ継続します。この方法は、新しいオプションの値をテストする場合に便利です。

1. SAP Control Center が起動している場合は停止します。
2. 環境変数を設定します。サイズをメガバイトで指定しますが、コマンドでは単位を指定しません。

Windows の例:

```
> set SCC_MEM_MAX=512
```

UNIX の例:

```
bash$ export SCC_MEM_MAX=512
```

3. `scc` コマンドを使用して SAP Control Center を起動します。

参照：

- Windows での SAP Control Center の起動と停止 (60 ページ)
- UNIX での SAP Control Center の起動と停止 (64 ページ)
- scc コマンド (72 ページ)

SAP Control Center Windows サービスのメモリオプションの変更

`jvmopt` コマンドを `scc.properties` ファイルに追加して、SAP Control Center Windows サービスのメモリオプション (`-Xmx` または `-XX:MaxPermSize`) を変更します。

この方法を使用してメモリオプションを設定する場合、変更は永続的になります。つまり、これらのオプションは、SAP Control Center がサービスとして起動するごとに使用されます。

1. SAP Control Center が起動している場合は停止します。
2. SAP Control Center プロパティファイルを開きます。

```
<SAP Control Center-install-directory>%SCC-3_3%bin
%scs.properties
```

3. メモリサイズを Java フォーマットで指定する `jvmopt` 行を追加 (すでに存在する場合は変更) します。メガバイトの場合は `m` を、ギガバイトの場合は `g` を使用します。

例を示します。

```
jvmopt=-Xmx512m
```

4. ファイルを保存し、SAP Control Center Windows サービスを起動します。

参照：

- Windows での SAP Control Center の起動と停止 (60 ページ)

SCC UNIX サービスのメモリオプションの変更

SAP Control Center UNIX サービスのメモリ設定を変更するには、該当する環境変数 (`SCC_MEM_MAX` または `SCC_MEM_PERM`) を `sccd` スクリプトに追加します。

この方法を使用してメモリオプションを設定する場合、変更は永続的になります。つまり、これらのオプションは、SAP Control Center がサービスとして起動するごとに使用されます。

1. SAP Control Center が起動している場合は停止します。
2. `sccd` ファイルを開きます。 `/etc/init.d/sccd`
3. 環境変数をファイルの先頭 (コメントの後) に追加します。サイズをメガバイト単位で指定します。ただし、コマンドには単位を指定しません。
例を示します。

```
SCC_MEM_MAX=512
```

4. ファイルを保存し、SAP Control Center UNIX サービスを起動します。

参照：

- UNIX での SAP Control Center の起動と停止 (64 ページ)

scc コマンド

scc.bat (Windows) または **scc.sh** (UNIX) を使用して、SAP Control Center エージェントおよびサーバを起動および停止したり、ポートの設定やサービスの有効化/無効化などの管理タスクを実行します。

構文

```
scc[.bat | .sh] [-a | --address RMI-service-address]  
[-b | --bitwidth]  
[--dbpassword]  
[-disable | --disable service-name,service-name...]  
[-enable | --enable service-name,service-name...]  
[-h | --help]  
[-I | --info [information-category]]  
[-instance [instance-name]]  
[-m | --message message-level]  
[-password | --password password]  
  
[-p | --port {port-name=port-number |  
          service-name:property-name=port-number}]  
[{-start | --start} | {-stop | --stop}]  
[-status | --status]  
[-user | --user login-name]  
[-v | -version | --version]
```

パラメータ

- **-a | --address *RMI-service-address*** – RMI サービスが使用するアドレス。このマシンの IP アドレスまたは名前 (デフォルト)。
- **-b | --bitwidth** – 基盤のプラットフォームのビット幅 (32 または 64) を特定する文字列を返します。SAP Control Center は、このオプションを使用して、内部データベースで使用するライブラリを決定します。このオプションを使用すると、SAP Control Center は **scc** コマンドで起動しません。
- **--dbpassword** – リポジトリデータベース用に提供されているデフォルトの dba アカウントのパスワードを変更します。新しいパスワードを入力するようにプロンプトを表示し、パスワードを検証して、SAP Control Center サーバを起動します。このオプションは、SCC をバックグラウンドで起動した場合は動作しません。コンソールがない場合は、サーバを起動できません。
- **-disable | --disable *service-name,service-name...*** – 指定された SAP Control Center サービスを無効にします。このオプションは、SAP Control Center の実行中ま

たは SCC を起動するコマンドの一部である場合は動作しません。このオプションを使用するには、SCC を停止し、`scc --disable` を実行し、再起動します。サービス名については、`--port` を参照してください。各サービスはカンマで区切ります。

- **-enable | --enable *service-name,service-name...*** – 指定された SCC サービスを有効にします。サービス名については、`--port` を参照してください。各サービスはカンマで区切ります。このオプションを使用する場合、SAP Control Center は **scc** で起動しません。SCC を起動するには、別のコマンドを使用します。
- **-h | --help** – **scc** コマンドのヘルプと役に立つ情報を表示します。このオプションを使用すると、SAP Control Center は **scc** で起動しません。
- **-I | --info [*information-category*]** – SAP Control Center に関する指定されたカテゴリの情報を表示します。各カテゴリはカンマで分割します。次の情報カテゴリがあります。
 - `all` - `sys`、`ports`、および `services` カテゴリに提供されるすべての情報を返します。デフォルトのオプションです。
 - `sys` - SCC のこのインスタンスに関する全般的な情報を返します。バージョン、ホーム (インストール) ディレクトリ、ホストマシンの名前と IP アドレス、RMI ポート番号、メッセージレベル、プラットフォームと Java インストールに関する詳細が含まれます。
 - `ports` - SCC とそのサービスが受信するすべてのポートを一覧表示します。各ポートが使用されているかどうかを示し、各ポートで実行中のサービスを表示します。
 - `services` - SCC が認識しているすべてのサービスを一覧表示します。サービスが有効かどうかを示し、各サービスが依存するほかのサービスを一覧表示します。
 - `sysprop` - Java VM が認識する Java システムのすべてのプロパティとその値を一覧表示します。
 - `env` - Java VM プロセス環境すべてを一覧表示します。
- **-instance [*instance-name*]** – 他のオプション (`-start` や `-stop` など) と組み合わせて使用して、共有ディスク配備の SCC インスタンスを指定します。インスタンスの名前を入力しないと、デフォルトでホストの名前に設定されます。
- **-m | --message *message-level*** – システムログに記録される詳細レベル (ロギングレベル) を設定します。有効な値は OFF、FATAL、ERROR、WARN、INFO、DEBUG、および ALL です。デフォルトは WARN です。
- **-password | --password** – SCC がサーバの停止やステータスのクエリに使用するユーザアカウントのパスワードを指定します。このオプションは、`--user` と組み合わせて使用します。`--password` を指定せずに `--user` を使用してコマンドを入力すると、パスワードの入力を求めるコンソールのプロンプトが表示されません。

使用開始にあたって

- p | --port {port-name=port-number | service-name:property-name=port-number}** - 指定されたサービスを、指定されたポートで実行するように設定します。SAP Control Center と同じシステム上の他のソフトウェアとの間でポートの競合が検出された場合は、ポートを変更すると有効です。このオプションを使用する場合、SAP Control Center は **scc** で起動しません。SCC を起動するには、別のコマンドを使用します。

有効なポート名、サービス名、およびプロパティ名は次のとおりです。

ポート名	説明	サービス名	プロパティ名	デフォルトのポート
db	データベースポート SCC サーバ上に存在	ScsSADataserver メッセージング アラート スケジューラ	com.sybase.asa. server.port messaging.db. port alert.database. port org.quartz.data- Source.ASA. URL	3638
http	Web HTTP ポート SCC サーバ上に存在	EmbeddedWeb- Container	http.port	8282
https	Web HTTPS (セキュア HTTP) ポート SCC サーバ上に存在	EmbeddedWeb- Container	https.port	8283
jiniHttp	JINI HTTP サーバ SCC サーバと SCC エージェントに存在	Jini	httpPort	9092
jiniRmid	JINI リモートメソッド呼び出しデー モン SCC サーバと SCC エージェントに存在	Jini	rmidPort	9095
msg	メッセージングポート SCC サーバ上に存在	メッセージング	messaging.port	2000
rmi	RMI ポート SCC サーバと SCC エージェントに存在	RMI	port	9999

ポート名	説明	サービス名	プロパティ名	デフォルトのポート
tds	Tabular Data Stream™ ポート (他の SAP データベース製品との通信に使用される) SCC サーバと SCC エージェントに存在	Tds	tdsPort	9998

また、`scc --info ports` を実行して、サービス名と、関連付けられているプロパティ名を表示することもできます。出力の最初の 2 カラムに表示されます。

- **-start | --start** – SCC サーバを起動します。これはデフォルトのオプションです。オプションなしで **scc** を実行すると、SCC を起動します。このオプションは、ポートを設定したり、サービスを有効化/無効化するオプションを使用する同じコマンドと組み合わせることはできません。SCC を起動するには、別の **scc** コマンドを使用します。
- **-status | --status** – SCC が実行中であるかどうかを示すステータスメッセージが表示されます。
- **-stop | --stop** – 実行中の SCC を停止します。
- **-user | --user [login-name]** – SAP Control Center が管理対象サーバの停止やステータスのクエリに使用するユーザアカウントを指定します。このオプションは、**--password** と組み合わせて使用します。ログイン名を入力しないと、入力を求めるコンソールのプロンプトが表示されます。
- **-v | --version | --version** – このサーバで実行されている SAP Control Center ソフトウェアのバージョンを表示します。このオプションを使用すると、SAP Control Center は **scc** で起動しません。

例

- **RMI ポートの設定** – これらの各コマンドは、RMI ポートを 9999 (デフォルト) に設定します。最初のコマンドは、ポート名の構文の例を示します。次のコマンドは、サービス名: プロパティ名の構文の例を示します。

```
scc --port rmi=9999
scc --port RMI:port=9999
```

- **RMI ポートの設定と SCC の起動** – これらのコマンドは、RMI ポートを 9996 に設定し、次に SCC を起動します。コマンドにポート設定のオプションが含まれる場合、**scc** は起動されないので、2 つのコマンド (ここではカンマで区切られている) が必要です。

使用開始にあたって

```
scc -p rmi=9996; scc
```

- **すべてのデータベースポートの設定** – このコマンドは、4つの SQL Anywhere データベースポート (データサーバ、メッセージング、データベースアラート、スケジューラ) すべてを 3638 に設定します (SCC リポジトリは SQL Anywhere データベースです)。

```
scc --port db=3638
```

- **TDS ポートの設定** – このコマンドは、TDS ポートを 9998 (デフォルト) に設定します。

```
scc --port Tds:tdsPort=9998
```

- **サービスを有効にして、SCC を起動します。** – 最初の **scc** コマンドは、TDS サービスを有効にし、次のコマンドは SCC を起動します (2つのコマンドは、セミコロンで分割します)。2番目のコマンドが必要なのは、**scc** に **-enable** オプションが含まれる場合、SAP Control Center は起動されないためです。

```
scc -enable Tds; scc
```

- **SCC インスタンスの起動** – このコマンドは、kalamazoo という名前の SCC インスタンスを起動します。デフォルトなので、**-start** はオプションです。

```
scc -start -instance kalamazoo
```

パーミッション

scc パーミッションは、すべてのユーザにデフォルトで設定されています。これを使用するためのパーミッションは必要ありません。

参照：

- ポートの設定 (96 ページ)
- ログインレベルまたはメッセージレベル (163 ページ)

SAP Control Center へのログイン

SAP Control Center の Web コンソールにログインします。

前提条件

SCC 用に使用するブラウザに Adobe Flash Player をインストールします。『SCC-product-name インストールガイド』を参照してください。

手順

通常、SAP Control Center では、オペレーティングシステムまたは LDAP ディレクトリサービスからユーザを認証します。SCC で使用するログインアカウントが不明な場合は、SCC 管理者に問い合わせてください。

1つのアカウントに同時に許可されるログインセッションは1つのみです。同じアカウントで複数のユーザが同時にログインすることはできません。

注意：新たにインストールされた SAP Control Center にセキュアな認証がまだ設定されていないときは、sccadmin アカウントを使用します。パスワードはインストール時に設定されています。詳細については、『SCC-product-name インストールガイド』を参照してください。

1. SAP Control Center サーバに接続します。Web ブラウザで、`https://scc-hostname:8283/scc` と入力します。
2. ログイン名とパスワードを入力して、[Login] をクリックします。

ヒント：Windows アカウントを使用して SCC にログインする場合は、`username@domain` の形式でユーザ名を入力します。上位レベルのドメイン拡張子 (.com や .net など) は省略します (例: fred@sap.com ではなく、fred@sap と入力します)。

SAP Control Center のログアウト

SAP Control Center での作業が完了したら、ログインセッションを終了します。

メインメニューバーから、[Application] > [Log Out] を選択します。

または、ウィンドウの右上にある [Log Out] をクリックします。

注意：管理者が自動ログアウト機能を設定している場合は、管理者が設定したタイムアウト期間よりも長い間セッションがアイドル状態 (入力やマウス動作がない状態) になると、ログアウトされます。

自動ログアウト期間が設定されていない場合は、

- リフレッシュする画面 (モニタ画面やデータ収集ジョブ画面など) に開いているログインセッションは、無期限に開いたままになります。
 - 変更されない画面に開いているログインセッションは、30 分で期限が切れます。次にサーバに要求を行うと、ログアウトされます。
-

セキュリティのセットアップ

ログイン認証を設定し、役割をマップします。

SAP Control Center 製品モジュールを設定する前に、セキュリティに関するトピックを確認して以下の手順を実行します。

注意：以下のセキュリティに関するトピックは、実際の運用環境での使用を想定していません。SCC を評価またはテストしている場合は、「評価のクイックスタート (13 ページ)」を参照してください。

1. セキュリティ

SAP Control Center は LDAP サーバまたはオペレーティングシステム、あるいはその両方を使用してユーザログインを認証できます。

2. Windows 認証の設定

Windows オペレーティングシステムを利用する認証はデフォルトで有効化されています。古いバージョンの SAP Control Center からアップグレードし、古いバージョンの認証設定を使用せず、認証に Windows を使用せず、ログインアカウントを手動で作成する場合のみ設定が必要です。SAP では、SCC でアカウントを自動作成することをおすすめします。

3. UNIX 用のプラグ可能認証モジュール (PAM) の設定

UNIX オペレーティングシステムのアカウントを使用して、ユーザ名とパスワードのログインがサポートされるように SAP Control Center を設定します。

4. LDAP 認証モジュールの設定

SAP Control Center の LDAP 認証モジュールは、正しい LDAP サーバを指定するようにセキュリティ設定ファイルを編集して設定します。

5. LDAP または OS グループに対する SAP Control Center の役割のマッピング

LDAP またはオペレーティングシステムを介して認証されたユーザに SAP Control Center 権限を付与するには、SAP Control Center で使用される役割を LDAP またはオペレーティングシステムのグループに関連付けます。

6. パスワードの暗号化

テキストファイルに保存している間、安全に保つ必要があるパスワードなどの値を暗号化するには、`passencrypt` ユーティリティを使用します。

7. ポートの設定

(オプション)`scc --port` コマンドを使用して、SAP Control Center サービスを新しいポートに割り当てます。

セキュリティ

SAP Control Center は LDAP サーバまたはオペレーティングシステム、あるいはその両方を使用してユーザログインを認証できます。

- SAP Control Center は、inetOrgPerson (RFC 2798) スキーマをサポートする任意の LDAP サーバを使用して認証を行うよう設定できます。
- SAP Control Center は、オペレーティングシステムを使用して認証を行う場合、SAP Control Center サーバマシン (クライアントではない) のオペレーティングシステムを使用します。

SCC でネイティブユーザアカウントを作成することもできますが、この方法で認証を行うことは推奨されません。既存の LDAP、Windows、または UNIX ログインアカウントを使用して認証を行うよう SCC を設定した方が簡単かつ安全です。

SAP では、SCC および SCC によって管理される SAP データベース製品に共通の認証プロバイダを使用することを強くおすすめします。共通の認証プロバイダを使用することにより、シングルサインオンが SAP Control Center とそのマネージドサーバのユーザに対して機能します。

SCC は各認証ログインアカウントを要求し、事前に定義する役割を持ちます。ログインが認証されれば、ログインの役割がセキュリティモジュールによって取得され SCC の事前に定義される役割にマップされます。許可はセキュリティモジュールネイティブ役割と SCC 役割の間をマップすることで決定されます。マッピングは使用されている OS または LDAP サーバで「sybase」グループを作成し、すべての SCC ユーザに加えることにより可能です。または SCC role-mapping.xml ファイルを修正し SCC 役割にネイティブの役割のマッピングを設定することによって可能です。セキュリティモジュールはログインを認証し、管理リソースに対するアクセスを承認します。

SAP Control Center は認証に対する事前定義されたログインモジュールを提供します。すべてのログインモジュールは <install_location>/SCC-3_3/conf/csi_config.xml ファイルの中で定義されます。構文は SAP Common Security Infrastructure (CSI) フレームワークにより定義されます。別のログインモジュールを設定してセキュリティの強さをカスタマイズすることができます。ログインモジュールは、次のとおりです。

- 事前設定ユーザログイン - ユーザ名、パスワード、役割のリストを定義します。デフォルトのユーザ名は sccadmin であり、このパスワードはインストール時に設定されます。ネイティブの役割は SCC 管理者で、sccAdminRole にマップされています。事前設定ユーザログインモジュールを csi_config.xml に追加することによって、追加のアカウントを作成できま

す。ただし SAP では、運用環境での認証では事前ユーザログインモジュールの使用をおすすめしていません。

- NT プロキシログイン - 基本となる Windows オペレーティングシステムに認証を委任します。NT プロキシログインモジュールから SCC へログインする場合は、フォーマット `username@nt-domain-name` でユーザ名を入力してください。たとえば、`user@sap` を入力します。Windows 認証はデフォルトで有効化されていますが、SCC 3.2.5 以前からのアップグレード後は、若干の設定作業が必要です。
- UNIX プロキシログイン - Pluggable Authentication Modules (PAM) を使用して基本となる UNIX または Linux オペレーティングシステムに認証を委任します。UNIX PAM を通して SCC にログインするときは、UNIX のユーザ名とパスワードを入力してください。UNIX 認証はデフォルトで有効化されていますが、若干の設定が必要となります。
- LDAP ログイン - 指定の LDAP サーバに認証を委任します。LDAP サーバを通して SCC にログインするときは、LDAP のユーザ名とパスワードを入力してください。LDAP 認証はデフォルトでは有効化されていません。ログインモジュールを設定する必要があります。

Windows 認証の設定

Windows オペレーティングシステムを利用する認証はデフォルトで有効化されています。古いバージョンの SAP Control Center からアップグレードし、古いバージョンの認証設定を使用せず、認証に Windows を使用せず、ログインアカウントを手動で作成する場合のみ設定が必要です。SAP では、SCC でアカウントを自動作成することをおすすめします。

このタスクは任意です。ただし、SAP Control Center アカウントの自動作成を選択しない場合は、手動で入力する必要があります。LDAP やローカルオペレーティングシステムを使用して SCC ユーザの認証を行う場合も、SCC で権限 (ユーザの権利) を設定するには、アカウントが必要です。

1. SCC の管理者権限を持つアカウントを使用して、SCC にログインします。(ログインアカウントまたはそのグループに `sccAdminRole` が設定されている必要があります)。
2. [Application] > [Administration] > [Security] を選択します。
3. [Automatically add SCC login records for authenticated logins] のラベルが表示されたボックスをクリックして選択または選択解除します。
4. [Automatically grant sccUserRole to newly created logins] のラベルが表示されたボックスをクリックして選択または選択解除します。
5. [OK] をクリックして [Security] ダイアログを閉じます。

次のステップ

この後は2とおりの手順があります。

- SCC ログインアカウントの自動作成を選択しなかった場合は、それぞれのアカウントを SCC に手動で入力します。
- 基本的なユーザアクセス以上の権限が必要な場合は、ログインアカウントに権限を付与します。権限を付与するには、SCC の役割をログインアカウントに直接割り当てるか、ログインアカウントをグループに割り当て、SCC の役割をそのグループにマッピングします。一般に、グループを使用する方法のほうが効率的です。

参照：

- LDAP または OS グループに対する SAP Control Center の役割のマッピング (93 ページ)
- システムへのログインアカウントの追加 (104 ページ)

UNIX 用のプラグ可能認証モジュール (PAM) の設定

UNIX オペレーティングシステムのアカウントを使用して、ユーザ名とパスワードのログインがサポートされるように SAP Control Center を設定します。

1. root 権限を持つログインアカウントを使用して、プラットフォームの PAM を設定します。

プラットフォーム	アクション
Solaris	<SCC-install-dir>/utility/<sunos>/pam.conf ファイル (SAP Control Center に付属) の内容を Solaris プラットフォーム上の /etc/pam.conf ファイルに追加する。
Linux	<SCC-install-dir>/utility/<linux>/sybase-csi ファイル (SAP Control Center に付属) を Linux プラットフォーム上の /etc/pam.d ディレクトリにコピーする。 注意： SAP Control Center に付属の sybase-csi ファイルは、最新の SUSE バージョンおよび Red Hat Linux バージョンとの互換性がない。詳細については、このトピックの最後にある例を参照のこと。

注意： 上記の表で、オペレーティングシステムを示すパスの箇所は、実際に表示される内容と多少異なる場合があります。

2. ホストの UNIX システムがディレクトリルックアップ認証 (yp、NIS など) を使用しておらず、認証がローカルの /etc/passwd ファイルに照らして実行され

使用開始にあたって

る場合は、`/etc/shadow` のパーミッションを変更して、SCC を実行するログインアカウントに読み込みアクセスを付与します。

3. (SAP Control Center の起動前に PAM を設定した場合は省略) SAP Control Center を再起動します。
4. (オプション) アカウント作成オプションを変更します。
 - a) 管理者権限 (`sccAdminRole`) を持つアカウントを使用して、SAP Control Center にログインします。
 - b) [Application] > [Administration] > [Security] を選択します。
 - c) [Automatically add SCC login records for authenticated logins] のラベルが表示されたボックスをクリックして選択または選択解除します。(SCC 3.2.6 以降はこのオプションがデフォルトで有効化されています。)
 - d) [Automatically grant sccUserRole to newly created logins] のラベルが表示されたボックスをクリックして選択または選択解除します。(SCC 3.2.6 以降はこのオプションがデフォルトで有効化されています。)
 - e) [OK] をクリックして [Security] ダイアログを閉じます。

例: SUSE Linux 11、Red Hat Enterprise Linux 6.0 用の PAM

SUSE 11 以降は、SAP Control Center に付属している `sybase-csi` ファイルを使用しないでください。代わりに、`/etc/pam.d` ディレクトリで、次の記載がある `sybase-csi` ファイルを作成します。

```
# sybase-csi PAM Configuration (SUSE style)
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

Red Hat 6.0 以降は、SAP Control Center に付属している `sybase-csi` ファイルを使用しないでください。代わりに、`/etc/pam.d` ディレクトリで、次の記載がある `sybase-csi` ファイルを作成します。

```
# sybase-csi PAM Configuration (Red Hat style)
auth      include      system-auth
account   include      system-auth
password  include      system-auth
session   include      system-auth
```

次のステップ

この後は 2 とおりの手順があります。

- SAP Control Center ログインアカウントの自動作成を選択しなかった場合は、それぞれのアカウントを SAP Control Center に手動で入力します。SAP Control Center で権限(ユーザの権利)を設定するには、アカウントが必要です。
- 基本的なユーザアクセス以上の権限が必要な場合は、ログインアカウントに権限を付与します。権限を付与するには、SAP Control Center の役割をログインアカウントに直接割り当てるか、ログインアカウントをグループに割り当て、SAP Control Center の役割をそのグループにマッピングします。一般に、グループを使用する方法のほうが効率的です。

参照：

- LDAP または OS グループに対する SAP Control Center の役割のマッピング (93 ページ)
- システムへのログインアカウントの追加 (104 ページ)

LDAP 認証モジュールの設定

SAP Control Center の LDAP 認証モジュールは、正しい LDAP サーバを指定するようにセキュリティ設定ファイルを編集して設定します。

1. <SCC-install-dir>\%conf%\csi_config.xml ファイルを開きます。
2. 囲んでいる <!-- と --> 文字を削除して設定ファイル内の LDAP モジュールのコメント化を解除します (または必要に応じて LDAP モジュールをファイルに追加します)。次のサンプルモジュールでは、ユーザ認証を提供する LDAP サーバを指定します。

サンプルモジュールには、OpenDS LDAP サーバに使用されるプロパティが示されます。ActiveDirectory で機能する値については、このタスクの最後に示されている例を参照してください。LDAP モジュールで使用可能な設定プロパティは、サブトピックで説明されています。

```
<authenticationProvider controlFlag="sufficient"
name="com.sybase.security.ldap.LDAPLoginModule">
  <options name="BindDN" value="cn=Directory Manager"/>
  <options name="BindPassword" value="secret"/>
  <options name="DefaultSearchBase" value="dc=example,dc=com"/>
  <options name="ProviderURL" value="ldap://localhost:10389"/>
  <options name="ServerType" value="openldap"/>
</authenticationProvider>
<provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer"/>
```

注意：太字で示された値のみを変更します。BindPassword が暗号化されている場合 (SAP の推奨)、それを定義する行に encrypted="true" を含める必要があります。この行は次のようになります。

使用開始にあたって

```
<options name="BindPassword" encrypted="true"
value="1snjikfwregfqr43hu5io..."/>
```

3. ファイルを保存します。
4. 使用する LDAP サーバの SSL 証明書に、標準以外の認証局による署名がある場合(自己署名証明書である場合など)は、**keytool** ユーティリティを使用して、JVM または JDK がその証明書を信頼するように設定します。次のコマンドを実行します。

Windows の場合：

```
keytool -import -keystore %SAP_JRE7%\lib\security\cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

UNIX の場合：

```
keytool -import -keystore $SAP_JRE7/lib/security/cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

ActiveDirectory に使用される LDAP 設定値

ActiveDirectory server については、LDAP ログインモジュールの設定プロパティに次の値を使用します。

```
ServerType: msad2K
DefaultSearchBase: dc=<domainname>,dc=<tld> or o=<company
name>,c=<country code>
    E.g. dc=sybase,dc=com or o=Sybase,c=us
ProviderUrl: ldaps://<hostname>:<port>
    E.g.: ldaps://myserver:636
AuthenticationFilter: (& (userPrincipalName={uid})
(objectclass=user))
BindDN: <User with read capability for all users>
BindPassword: <Password for BindDN user>
RoleFilter: (|(objectclass=groupofnames) (objectclass=group))
controlFlag: sufficient
```

次のステップ

SCC の役割を LDAP グループにマッピングします。

参照：

- LDAP または OS グループに対する SAP Control Center の役割のマッピング (93 ページ)

LDAP Configuration Properties (LDAP 設定プロパティ)

SAP Control Center LDAP サービスを制御するには、csi_config.xml ファイルで次のプロパティを使用します。

注意： 次の文字が LDAP 内の名前で使用された場合は特別な意味を持ちます。、(カンマ)、=(等号)、+(プラス記号)、<(小なり)、>(大なし)、#(番号またはハッシュマーク)、;(セミコロン)、¥(バックスラッシュ/円マーク)、/(スラッシュ)、LF(改行)、CR(復帰改行)、"(二重引用符)、'(一重引用符)、*(アスタリスク)、?(疑問符)、&(アンパサンド)、および文字列の先頭または末尾のスペース。LDAP プロバイダは、これらの特殊文字が設定プロパティの名前または DN に含まれていると処理することができません。また、以下に示す一部のプロパティではこれらの特殊文字を共通名に使用することができません。

プロパティ	デフォルト値	説明
ServerType	なし	<p>(省略可能) 接続先の LDAP サーバのタイプ。</p> <ul style="list-style-type: none"> • sunone5 - SunOne 5.x または iPlanet 5.x • msad2k - Microsoft Active Directory、Windows 2000 • nsds4 - Netscape Directory Server 4.x • openldap - OpenLDAP Directory Server 2.x <p>選択する値によって、以下の認証プロパティのデフォルト値が設定される。</p> <ul style="list-style-type: none"> • RoleFilter • UserRoleMembership • RoleMemberAttributes • AuthenticationFilter • DigestMD5Authentication • UseUserAccountControl
ProviderURL	ldap://localhost:389	<p>LDAP サーバへの接続に使用される URL。サーバが次に該当する場合は、デフォルト値を使用する。</p> <ul style="list-style-type: none"> • 共通のセキュリティインフラストラクチャで有効になっている製品と同じマシンに置かれている。 • デフォルトポート (389) を使用するよう設定されている。 <p>それ以外の場合、値を設定する次の構文を使用する。</p> <pre>ldap://<hostname>:<port></pre>

プロパティ	デフォルト値	説明
Default-SearchBase	なし	<p>認証、役割、属性、自己登録に他の検索ベースが指定されていない場合に使用される LDAP 検索ベース。</p> <ol style="list-style-type: none"> dc=<domainname>,dc=<tld> たとえば、mycompany.com ドメインにあるマシンには dc=mycompany,dc=com の検索ベースがある。 o=<company name>,c=<country code> たとえば、Mycompany 組織内のマシンの場合、o=mycompany,c=us となる。 <hr/> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
SecurityProtocol	なし	<p>LDAP サーバへの接続に使用されるプロトコル。暗号化されたプロトコルを使用するには、URL で ldaps の代わりに ssl を使用する。</p>
AuthenticationMethod	Simple	<p>LDAP に対するすべての認証要求で使用される認証方法。一般に有効値は java.naming.security.authentication JNDI プロパティと同じ。次のいずれかを選択します。</p> <ul style="list-style-type: none"> simple - クリアテキストのパスワード認証を指定する。 DIGEST-MD5 - よりセキュアなハッシュパスワード認証。この方法では、サーバでプレーンテキストのパスワード記憶領域が使用される。また、JRE 1.4 以降でのみ機能する。

プロパティ	デフォルト値	説明
<p>AuthenticationFilter</p>	<p>ほとんどの LDAP サーバの場合: (&uid={uid})(objectclass=person)</p> <p>または</p> <p>Active Directory 電子メールのルックアップの場合: (&userPrincipalName={uid})(objectclass=user) [ActiveDirectory]</p> <p>Active Directory Windows ユーザ名のルックアップの場合: (&sAMAccountName={uid})(objectclass=user)</p>	<p>ユーザのルックアップ時に使用するフィルタ。</p> <p>ユーザ名に基づいた検索を実行するときに、このフィルタを使用して、指定されたユーザ名と一致する LDAP エントリが判別される。</p> <p>フィルタの文字列 "{uid}" は、指定されたユーザ名に置き換えられる。</p> <hr/> <p>注意: このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
<p>AuthenticationScope</p>	<p>onelevel</p>	<p>認証の検索スコープ。サポートされる値は、次のとおり。</p> <ul style="list-style-type: none"> onelevel subtree <p>値が指定されていない場合、または無効な値が指定された場合、デフォルト値が使用される。</p>

プロパティ	デフォルト値	説明
AuthenticationSearchBase	なし	<p>ユーザの認証に使用される検索ベース。このプロパティを設定しない場合は、DefaultSearchBase の値が使用される。</p> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> • このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 • このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
BindDN	なし	<p>初期 LDAP 接続を構築するときにバインドするユーザ DN。</p> <p>多くの場合、このユーザはすべてのユーザレコードでの読み込みパーミッションを必要とする。値を設定しない場合、匿名バインドが使用される。匿名バインドは、ほとんどのサーバで追加の設定なしで機能する。</p> <p>ただし、LDAP アトリビュータは、この DN を LDAP サーバのユーザの作成にも使用する可能性がある。自己登録機能が使用される場合、そのユーザにユーザレコードの作成に必須のパーミッションが必要な場合もある。このような動作は、useUserCredentialsToBind を true に設定していない場合に発生する可能性がある。この場合、LDAP アトリビュータは、この DN を使用して、ユーザ属性を更新する。</p>

プロパティ	デフォルト値	説明
BindPassword	なし	<p>任意のユーザの認証に使用される、BindDN のパスワード。 BindDN と BindPassword によって、LDAP 接続がユニットに分離される。</p> <p>AuthenticationMethod プロパティは、この初期接続に使用されるバインドメソッドの決定に使用される。</p> <p>SAP はパスワードの暗号化を推奨し、パスワード暗号化ユーティリティを提供している。 BindPassword を暗号化する場合は、オプションを設定する行に encrypted=true を含める。次に例を示します。</p> <pre data-bbox="606 569 1174 638"><options name="BindPassword" encrypted="true" value="1snjikfwregfqr43hu5io..."/></pre> <p>BindPassword を暗号化しない場合、このオプションは次のようになる。</p> <pre data-bbox="606 743 1112 795"><options name="BindPassword" value="s3cr3T"/></pre>
RoleSearch-Base	なし	<p>役割のリストの取得に使用される検索ベース。このプロパティを設定しない場合は、DefaultSearchBase の値が LDAP に使用される。</p> <hr/> <p>注意： このプロパティを使用して SCC を認証するときの注意点:</p> <ul data-bbox="606 1043 1174 1164" style="list-style-type: none"> • このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 • このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。

プロパティ	デフォルト値	説明
RoleFilter	<p>SunONE/iPlanet の場合: (<code>&object-class=ldapsubentry</code>) (<code>object-class=nsrolededefinition</code>)</p> <p>Netscape Directory Server の場合: (<code> objectclass=groupofnames</code>) (<code>objectclass=groupofunique-names</code>)</p> <p>ActiveDirectory の場合: (<code> objectclass=groupofnames</code>) (<code>objectclass=group</code>)</p>	<p>役割検索フィルタ。このフィルタは役割検索ベースと役割スコープと組み合わせて使用すると、LDAP サーバ内の全役割のリストを返す。選択されたサーバタイプによってはいくつかのデフォルト値が存在する。サーバタイプを選択せず、このプロパティが初期化されていない場合は、役割を利用できない。</p> <hr/> <p>注意: このプロパティを使用して SCC を認証するときの注意点:</p> <ul style="list-style-type: none"> このプロパティの値の共通名または識別名に上記の特殊文字を使用しないこと。 このプロパティのユーザ名またはパスワードに中国語や日本語の文字を使用しないこと。
RoleMember-Attributes	<p>Netscape Directory Server と OpenLDAP サーバの場合: <code>member,uniquemember</code></p>	<p>この役割を付与されたユーザの DN を導出する際に LDAP で使用される役割属性のカンマ区切りリスト。これらの値は、ユーザの役割リストを決定するため、アクティブなユーザと相互参照される。このプロパティの使用例として、LDAP グループを役割のプレースホルダとして使用する場合がある。このプロパティには、Netscape サーバタイプが選択されたときのみデフォルト値がある。</p>
RoleNameAttribute	<code>cn</code>	<p>役割名として使用される役割エントリの属性。これは、役割リストに表示されるか、認証されたユーザに付与される役割名である。</p>
RoleScope	<code>onelevel</code>	<p>役割の検索スコープ。サポートされている値は次のとおり。</p> <ul style="list-style-type: none"> <code>onelevel</code> <code>subtree</code> <p>値が指定されていない場合、または無効な値が指定された場合、デフォルト値が使用される。</p>

プロパティ	デフォルト値	説明
SkipRole- Lookup	false	<p>RoleSearchBase および RoleFilter を使用してルックアップされた役割と相互参照しないで、プロパティ UserRoleMembershipAttributes によって指定された属性を使用してルックアップされた役割を付与するには、このプロパティを true に設定する。</p> <p>LDAP 設定の検証は、利用可能なすべての役割の一覧表示でエラーが発生しても、正常に完了する。エラーは検証時にサーバログに記録されるが、SCC にはレポートされず、設定の保存が可能になる。これは、役割マッピング用の物理的な役割を一覧表示するとき、および SCC に影響する。ユーザの認証を正常に行うには、SkipRoleLookup プロパティを true に設定する。</p>
UserRole- Membershi- pAttributes	<p>iPlanet/SunONE の場合: nsRoleDN</p> <p>Active Directory の場合: memberOf</p> <p>その他すべての場合: none</p>	<p>ユーザがメンバとして属するすべての役割の DN が含まれるユーザ属性を定義する。</p> <p>これらのカンマ区切り値は、役割検索ベースと検索フィルタで取得された役割と相互参照され、ユーザの役割のリストが生成される。</p> <p>SkipRoleSearch プロパティが true に設定されている場合、これらのカンマ区切り値は、役割検索ベースおよび役割検索フィルタで取得された役割と相互参照されない。「SkipRoleLookup」を参照。</p> <p>注意： ActiveDirectory でネストされたグループを使用する場合は、このプロパティを tokenGroups に設定する必要がある。</p>
UserFreeform- RoleMember- shipAttributes	なし	<p>自由形式の役割メンバシップ属性リスト。このカンマ区切りリストにある属性を持つユーザは、属性値と等しい名前を持つ役割へのアクセスが自動的に許可される。たとえば、このプロパティの値が department で、ユーザの LDAP レコードにおける department 属性の値が {sales, consulting} である場合、ユーザには sales と consulting という役割が付与される。</p>
Referral	ignore	<p>referral が発生したときの動作。有効な値は、LdapContext によって決定される値。ただし、follow、ignore、throw が含まれる場合がある。</p>

使用開始にあたって

プロパティ	デフォルト値	説明
DigestMD5AuthenticationFormat	DN OpenLDAP の場合: Username	DIGEST-MD5 バインド認証 ID 形式。
UseUserAccountControlAttribute	Active Directory の場合: true	このプロパティを true に設定すると、UserAccountControl 属性で、無効化されたユーザアカウント、アカウントの期限切れ、パスワードの期限切れなどが検出される。ActiveDirectory ではこの属性を、上記情報の格納にも使用する。
EnableLDAPConnectionTrace	False	LDAP 接続トレースを有効化する。出力は、temp ディレクトリのファイルに記録される。このファイルのロケーションはサーバログに記録される。
ConnectTimeout	0	LDAP サーバへの接続を確立しようとするときのタイムアウトをミリ秒単位で指定する。このプロパティ値により、設定された LDAP サーバへの接続を確立しようとするときに JNDI com.sun.jndi.ldap.connect.timeout プロパティが設定される。LDAP プロバイダが設定された期間内に接続を確立できない場合は、接続の試行がアボートされる。0 以下の整数値を使用すると、ネットワークプロトコルのタイムアウト値が使用される。
ReadTimeout	0	サーバへの初期接続の確立後、読み込み操作に対するサーバの応答をクライアントが待機する期間をミリ秒単位で制御する。このプロパティ値により、設定された LDAP サーバへの接続を確立しようとするときに JNDI com.sun.jndi.ldap.read.timeout プロパティが設定される。LDAP プロバイダが設定された期間内に LDAP 応答を取得できない場合は、読み込みの試行がアボートされる。読み込みタイムアウトは、サーバとの初期接続が確立された後のサーバからの LDAP 応答に適用される。0 以下の整数値は、読み込みタイムアウトが指定されないことを意味する。

プロパティ	デフォルト値	説明
LDAPPool- MaxActive	8	LDAP サーバへの同時 LDAP 接続の数を制限する。正の数値以外の数値は、制限がないことを示す。このオプションが複数の LDAP プロバイダに設定されていると、最初の LDAP プロバイダによって設定された値がロードされ、他のすべての値よりも優先される。LDAPPoolMaxActive に達すると、その後で LDAP プロバイダクラスがプールから LDAP 接続を借用しようとしても、新しいオブジェクトまたはアイドル状態のオブジェクトがプールで利用可能になるまで、無期限にブロックされる。接続プールによって、設定された LDAP サーバに確立される TCP 接続の数が管理されるため、LDAP プロバイダのパフォーマンスとリソース使用率が向上する。
controlFlag	オプション	複数の認証プロバイダを設定する場合は、各プロバイダに controlFlag を使用して、ログインシーケンスでの認証プロバイダの使用方法を制御する。 controlFlag は、LDAP 設定プロパティよりも一般的なログインモジュールである。

LDAP または OS グループに対する SAP Control Center の役割のマッピング

LDAP またはオペレーティングシステムを介して認証されたユーザに SAP Control Center 権限を付与するには、SAP Control Center で使用される役割を LDAP またはオペレーティングシステムのグループに関連付けます。

前提条件

- LDAP と UNIX に必要: 認証モジュールの設定。
- オプション: SCC 認証を提供するシステム (LDAP または OS) に以下のグループを作成して SAP Control Center ユーザに割り当てます。
 - sybase - sccUserRole を付与します。すべての SCC ユーザを sybase グループに割り当てます。
 - SCC Administrator - sccAdminRole を付与します。SCC 管理者ユーザのみをこのグループに割り当てます。

手順

SAP Control Center は、ローカルオペレーティングシステムまたは LDAP サーバを介してユーザを認証できるように設定できます。このタイプの認証作業を実行す

使用開始にあたって

るには、認証を提供するシステム (LDAP またはオペレーティングシステム) に存在するグループに SCC の役割をマッピングする必要があります。

sybase および SCC 管理者グループは、role-mapping.xml で事前定義されているため、便利に使用できます。sybase および SCC 管理者グループを LDAP システムに追加して、SCC ユーザおよび管理者にその値を入力すると、次のタスクを省略できます。つまり、下記の手順を実行する必要がなくなります。

次の表は、SCC の役割に対する LDAP と OS グループのデフォルトのマッピングのリストです。ログインモジュールは、csi_config.xml で定義されています。

ログインモジュール	OS グループ	SAP Control Center の役割
UNIX プロキシ	root	uaAnonymous、uaAgentAdmin、uaOSAdmin
	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	user	uaAnonymous
	guest	uaAnonymous
NT プロキシ	Administrators	uaAnonymous、uaAgentAdmin、uaOSAdmin
	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	Users	uaAnonymous
	Guests	uaAnonymous
LDAP	sybase	uaAnonymous、uaPluginAdmin、sccUserRole
	SCC Administrator	uaAnonymous、sccAdminRole

マッピングの実行には次の 2 つの方法があります。

- (推奨) SAP Control Center がユーザの認証に使用するオペレーティングシステムまたは LDAP サーバに "sybase" グループと "SCC Administrator" グループを追加し、SAP Control Center にアクセスする必要があるすべてのユーザをこれらのグループの一方または両方に追加します。
- role-mapping.xml ファイルを編集して、LDAP またはオペレーティングシステムの既存グループを使用するように SAP Control Center を設定します。このオプションについて次に説明します。

1. SAP Control Center が起動している場合は停止します。
2. テキストエディタで次のファイルを開きます。

```
<SCC-install-directory>/conf/role-mapping.xml
```

3. ファイルで `sccUserRole` セクションを探します。

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
</Mapping>
```

4. SCC ユーザの認証に使用している LDAP または OS グループの `MappedName` 行を追加します。 `sccUserRole` セクションは次のようになります。

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
  <MappedName>my_SCC_group</MappedName>
</Mapping>
```

5. ファイルで `sccAdminRole` セクションを探します。

```
<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
</Mapping>
```

6. SCC 管理者の認証に使用している LDAP または OS グループの `MappedName` 行を追加します。 `sccAdminRole` セクションは次のようになります。

```
<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>my_SCC_admin_group</MappedName>
</Mapping>
```

7. ファイルを保存して終了します。

8. (LDAP のみ) LDAP レポジトリで定義された役割が `role-mapping.xml` で定義された役割と一致していることを確認します。

9. `<SCC-install-dir>%conf%csi_config.xml` ファイルで、`BindPassword` プロパティと `ProviderURL` プロパティを配備内で使用される値に設定します。
Sybase では、機密情報に関連する値を暗号化してから `csi_config.xml` に保存することをおすすめします。

10. SAP Control Center を起動します。

参照：

- LDAP 認証モジュールの設定 (83 ページ)

パスワードの暗号化

テキストファイルに保存している間、安全に保つ必要があるパスワードなどの値を暗号化するには、`passencrypt` ユーティリティを使用します。

使用開始にあたって

暗号化パスワードは設定ファイルに安全に保存できます。**passencrypt** の実行時、およびログイン時に、パスワードをクリアテキスト (暗号化されていない) で入力します。

SAP Control Center の bin ディレクトリにある **passencrypt** は、csi_config.xml の PreConfiguredLoginModule で使用されるパスワードに SHA-256 ハッシュアルゴリズムを使用します。

1. コマンドウィンドウを開き、bin ディレクトリに移動します。

Windows の場合： `cd <SCC-install-directory>\bin`

UNIX の場合： `cd <SCC-install-directory>/bin`

2. パスワードを暗号化するには、**passencrypt -csi** と入力します。その結果表示されたプロンプトで、新しいパスワードを入力します。
passencrypt は、入力したパスワード (画面には表示されません) を暗号化し、暗号化した形式でパスワードを表示します。
3. 暗号化されたパスワードをコピーします。
4. 暗号化されたパスワードを必要な場所に貼り付けます。

ポートの設定

(オプション) **scc --port** コマンドを使用して、SAP Control Center サービスを新しいポートに割り当てます。

前提条件

SAP Control Center と、同じホストで実行されているその他のソフトウェアとの間のポートの競合を確認します。

手順

SAP Control Center は、他のサービスがポートを使用していると適切に動作できません。右カラムの下に一覧表示されているポートで競合を発見したら、他のサービスのポートを再設定するか、ここで説明するように SAP Control Center を再設定します。

ポート名	説明	サービス名	プロパティ名	デフォルトのポート
db	データベースポート SCC サーバ上に存在	SccSADataserver メッセージング アラート スケジューラ	com.sybase.asa. server.port messaging.db. port alert.database. port org.quartz.data- Source.ASA. URL	3638
http	Web HTTP ポート SCC サーバ上に存在	EmbeddedWeb- Container	http.port	8282
https	Web HTTPS (セキュア HTTP) ポート SCC サーバ上に存在	EmbeddedWeb- Container	https.port	8283
jiniHttp	JINI HTTP サーバ SCC サーバと SCC エージェントに存在	Jini	httpPort	9092
jiniRmid	JINI リモートメソッド呼び出しデー モン SCC サーバと SCC エージェントに存在	Jini	rmidPort	9095
msg	メッセージングポート SCC サーバ上に存在	メッセージング	messaging.port	2000
rmi	RMI ポート SCC サーバと SCC エージェントに存在	RMI	port	9999
tds	Tabular Data Stream™ ポート (他の SAP データベース製品との通信に使用さ れる) SCC サーバと SCC エージェントに存在	Tds	tdsPort	9998

使用開始にあたって

1. SAP Control Center を停止します。
2. **scc --info ports** を実行して、SAP Control Center サービスのリストとそのプロパティおよび割り当てられているポートを表示します。
3. ポートを再割り当てするには、コマンドを次の形式のいずれかで入力します。

```
scc --port port-name=port-number
```

```
scc --port service-name:property-name=port-number
```

データベースサービスが別のポートを使用するように設定する場合を除き、最初の簡潔な形式を使用します(デフォルトでは、すべてが同じポートを使用します)。
4. SAP Control Center を起動します。
5. **scc --info ports** を再度実行して、ポートが再割り当てされたことを確認します。

例

4つのデータベースサービス(データサーバ、メッセージング、データベースアラート、およびスケジューラ)のすべてを同じポート 3639 に設定します(データベースは、SAP Control Center 内部レポジトリに使用される SAP® SQL Anywhere®)。

```
scc --port db=3639
```

データベースメッセージングサービスだけをポート 3639 に設定します。

```
scc --port Messaging:messaging.db.port=3639
```

HTTP ポートを 9292 に設定します。

```
scc --port http=9292
```

Jini RMI デーモンをポート 9696 に設定します。

```
scc --port jiniRmid=9696
```

メインの SAP Control Center メッセージングサービスをポート 2001 に設定します。

```
scc --port msg=2001
```

RMI ポートを 9991 に設定します。

```
scc --port rmi=9991
```

Tabular Data Stream ポートを 9997 に設定します。

```
scc --port tds=9997
```

注意： **scc** コマンドでポート設定オプション (**-p** または **--port**) を使用すると、SAP Control Center は起動しません。SCC を起動するには、別の **scc** コマンドを実行します。

参照：

- scc コマンド (72 ページ)

自動ログアウトタイマの設定

(オプション) ユーザが長時間にわたって非アクティブな場合にログインセッションを停止するように、SAP Control Center を設定します。

前提条件

SAP Control Center を起動して、管理者権限を持つアカウントでログインします。(ログインアカウントまたはそのグループに `sccAdminRole` が設定されている必要があります)。

手順

1. アプリケーションのメニューバーから、[Application] > [Administration] を選択します。
2. [General Settings] を選択します。
3. [Auto-Logout] タブをクリックします。
4. アイドルユーザが自動的にログアウトされるまでの経過時間を分単位で入力します。
自動ログアウトを無効にするには、0 を入力するか、ボックスを空のままにします。
5. [OK] をクリック (変更内容を適用して、プロパティダイアログを閉じる) するか、[Apply] をクリック (変更内容を適用して、ダイアログは閉じない) します。

参照：

- SAP Control Center の起動 (59 ページ)
- SAP Control Center へのログイン (76 ページ)

ユーザ承認

SAP Control Center での権限メカニズムには、ログインアカウントとタスクベースの役割が使用されます。

SAP Control Center へのアクセスはログインアカウントによって制御されます。パーミッションでは、特定のタイプのサーバの管理とモニタリングなど、ユーザが SCC で実行できるタスクを制御する、定義済みの役割が割り当てられます。これらの役割は、ログインアカウントまたはグループに直接割り当てることができます。ログインアカウントの役割は、そのログインアカウントが属するグループ

使用開始にあたって

の役割を継承します。コンポーネント製品モジュールで、一部の役割は自動的に割り当てられます。

SAP Control Center では役割が次のように分類されます。

- システム標準の役割 - ユーザがどのように SCC と対話できるようにするかを定義します。
- 製品ごとの役割 - SCC で管理されている特定のリソース (たとえば、RepBoston01 という名前の Replication Server) とユーザがどのように対話できるようにするかを定義します。

注意: ここで説明されているツールは、SCC 対応のログインアカウントを管理するためのツールです。管理対象リソースで作成されたアカウントとグループは、これらのツールで管理できません。

参照:

- 管理対象リソースのログインアカウントの認証 (113 ページ)

ログインまたはグループへの役割の割り当て

セキュリティ設定オプションを使用して、1つ以上の役割を SAP Control Center のログインアカウントまたはグループに追加します。これらの役割は、ユーザがサーバのモニタや SAP Control Center の管理などのタスクを実行できるようにします。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。サーバのモニタリング役割を割り当てるには、まずサーバを登録します。

手順

SAP Control Center で管理タスクを実行する任意のログインアカウントに sccAdminRole を割り当てます。

1. アプリケーションのメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Logins] または [Groups] をクリックします。
4. 表から、役割を割り当てるログインアカウントまたはグループを選択します。
5. [役割] タブをクリックします。
6. [Available roles for resource] リストで、ロールを選択してから [Add] をクリックします。たとえば、管理者権限を付与するには、SCC サービス sccAdminRole

を追加します。モニタ権限を付与するには、該当するサーバとサーバタイプの MonitorRole を追加します。

注意： SAP Control Center 製品モジュールでは特定の役割が自動的に割り当てられるため、MonitorRole の追加が不要な場合もあります。

[Has following roles] リストに役割が表示される場合、このアカウントまたはグループがその役割にすでに設定されています。

7. [OK] をクリックします。

参照：

- ログインまたはグループからの役割の削除 (101 ページ)

ログインまたはグループからの役割の削除

セキュリティ設定オプションを使用して、1つ以上の役割を SAP Control Center のログインアカウントまたはグループから削除します。

前提条件

このタスクを実行するには、管理権限が必要です。

手順

1. メニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Logins] または [Groups] をクリックします。
4. 役割を削除するログインアカウントまたはグループを選択します。
5. [役割] タブをクリックします。
6. 役割を選択して [Remove] をクリックします。
7. [OK] をクリックします。

参照：

- ログインまたはグループへの役割の割り当て (100 ページ)

グループの追加

新しいグループを作成するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

グループを使用すると、役割が管理しやすくなります。役割を個々のユーザに割り当てるのではなく、役割をグループに割り当て、必要に応じて、そのグループにユーザを追加するか、またはグループからユーザを削除します。

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Groups] を選択します。
4. [Create Group] をクリックします。
5. グループ名と説明を入力します。
6. [Finish] をクリックします。

参照：

- グループの削除 (102 ページ)
- グループへのログインアカウントの追加 (103 ページ)
- グループからのログインアカウントの削除 (103 ページ)

グループの削除

グループを削除するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Groups] を選択します。
4. 削除するグループを選択します。
5. [Delete] をクリックします。
6. [OK] をクリックして削除を確定します。

参照：

- グループの追加 (101 ページ)
- グループへのログインアカウントの追加 (103 ページ)
- グループからのログインアカウントの削除 (103 ページ)

グループへのログインアカウントの追加

1つ以上のログインアカウントをグループに追加するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Groups] をクリックします。
4. アカウントを割り当てるグループを選択します。
5. [Membership] タブをクリックします。
6. アカウントを選択し、[Add] をクリックします。
7. [OK] をクリックします。

参照：

- グループの追加 (101 ページ)
- グループの削除 (102 ページ)
- グループからのログインアカウントの削除 (103 ページ)

グループからのログインアカウントの削除

グループから 1つ以上のログインアカウントを削除するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. SAP Control Center Properties で、[Security] フォルダを展開します。
3. [Groups] を選択します。
4. メンバを削除するグループを選択します。

使用開始にあたって

5. [Membership] タブをクリックします。
6. ログインを選択し、[Remove] をクリックします。
7. [OK] をクリックします。

参照：

- グループの追加 (101 ページ)
- グループの削除 (102 ページ)
- グループへのログインアカウントの追加 (103 ページ)

システムへのログインアカウントの追加

SAP Control Center のネイティブログインアカウントを作成するには、セキュリティ設定オプションを使用します。

前提条件

- このタスクを実行するには、SCC 管理者権限 (sccAdminRole) を持っている必要があります。
- LDAP またはオペレーティングシステムを使用してユーザを認証する場合は、適切な認証モジュールを設定する必要があります。

手順

注意：すべての SAP Control Center ユーザに対して、ネイティブのログインアカウントを手動で作成することはおすすめていません。LDAP またはオペレーティングシステムのユーザアカウントを使用してユーザを認証するように SAP Control Center を設定するほうが効率的です。このようにすると、SCC によって認証されたすべてのユーザにネイティブアカウントが自動的に作成されます。

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Login] を選択します。
4. [Create Login] をクリックします。
5. 新しいアカウントのログイン名と有効期限を入力します。有効期限の入力は、オプションです。
6. [Next] をクリックします。
7. [Specify new user information] を選択します。
8. ユーザについての詳細情報を入力します。

- Title
- First name*
- M.I. (ミドルネームのイニシャル)
- Last name*
- Suffix
- E-mail address*
- Phone
- Ext.
- Fax
- Mobile
- Supports text messaging (チェックボックス)

*[First Name]、[Last Name]、および [E-mail Address] のフィールドを入力する必要があります。

9. [Finish] をクリックします。

次のステップ

新しいログインアカウントに権限を付与します。権限を付与するには、SAP Control Center の役割をログインアカウントに直接割り当てるか、ログインアカウントをグループに割り当て、SAP Control Center の役割をそのグループにマッピングします。一般に、グループを使用する方法のほうが効率的です。

システムからのログインアカウントの削除

SAP Control Center のログインアカウントを削除するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Logins] を選択します。
4. 削除するログインを選択します。
5. [Delete] をクリックします。
6. [OK] をクリックして削除を確定します。

ユーザプロフィールの変更

ログインアカウントのサスペンド、有効期限の終了日の設定、アカウントのユーザ情報の変更を実行するには、セキュリティ設定オプションを使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Security] フォルダを展開します。
3. [Logins] を選択します。
4. 変更するログインアカウントを選択します。
5. [General] タブをクリックします。
6. このアカウントをサスペンドするには、[Login disabled] をクリックします。
7. このアカウントの有効期限の終了日を設定するには、[Expiration] フィールドの隣のカレンダーアイコンをクリックし、日付を選択します
8. [Apply] をクリックします。
9. [User Info] タブをクリックします。
10. ユーザ情報を編集します。
このユーザが電子メールのアラートサブスクリプションを設定している場合、ここに入力した電子メールアドレスが、SAP Control Center によってサブスクリプションダイアログに自動的に設定されます。
11. [Apply] をクリックします。

ログイン、役割、グループ

SAP Control Center には、事前に定義されたログインアカウントと役割があります。

ログインアカウントは、SAP Control Center に接続可能なユーザを特定します。アカウントには、そのユーザが実行できるタスクを制御する役割があります。ネイティブの SCC アカウントを使用してユーザを認証できますが、オペレーティングシステムまたは LDAP ディレクトリサービスに認証を委任する方法のほうが安全です。

SCC には事前定義されたログインアカウントが付属しています。事前定義されたアカウントは、SAP Control Center のインストール、設定、およびテストのみに使用することをおすすめします。このアカウントは、実際の運用環境での使用を想定していません。

表 10 : 事前定義されたログインアカウント

ログイン名	説明
sccadmin	SAP Control Center の管理機能のすべてを使用できる。設定およびテストに使用する。

役割は、ログインアカウントまたはグループに割り当てることができる、事前定義されたプロファイルです。役割は、ログインアカウントのアクセス権を制御します。SCC には、実際の運用環境での使用を想定した事前定義された役割が付属しています。

表 11 : 事前定義された役割

役割	説明
sccUserRole	SAP Control Center の管理作業以外のアクセスを提供する。すべてのユーザに必須で、認証されたすべてのユーザに自動的に割り当てられる。
sccAdminRole	SAP Control Center を管理するための管理権限を提供する。

SCC 製品モジュールのモニタ権限は、自動的に割り当てられます。

グループは、1つ以上のログインアカウントで構成されます。1つのグループ内のすべてのアカウントに、そのグループに付与された役割が割り当てられます。SCC では、ビジネス要件に応じてグループを作成できます。

使用開始にあたって

設定

SAP Sybase Control Center for Data Assurance を設定します。

注意： SAP Control Center を運用環境用に設定する前に、ヘルプの「使用開始にあたって」セクションのタスクを完了しておきます。セキュリティの設定は、特に重要です。

1. Data Assurance サーバのモニタリング設定

SAP Control Center を使用して監視する Data Assurance (DA) サーバを認証します。リソースが認証されると、SAP Control Center によって DA サーバ監視オプションが有効になります。

2. Data Assurance サーバの登録

リソース (モニタ対象として使用可能なサーバなど) を登録して、SAP Control Center がそのリソースと接続情報を認識できるようにします。

3. 一括登録のためのリソースのインポート

(オプション) 複数のサーバを interfaces または sql.ini ファイルからインポートして登録します。

4. 管理対象リソースのログインアカウントの認証

SAP Control Center がサーバまたはエージェントに接続して監視データを収集したりリソースを管理したりする場合に使用するログインアカウントとパスワードを指定します。

5. 統計収集のセットアップ

データ収集ジョブを作成し、スケジュールをジョブに追加するには、管理対象リソースの [Properties] ビューを使用します。

6. エージェント接続の作成

compareset およびスキーマジョブの作成に必要な Data Assurance (DA) エージェント接続を作成します。

7. データベース接続の作成

Data Assurance (DA) サーバにプライマリデータベース接続および複製データベース接続を設定します。

8. interface ファイルからの単一接続またはクラスタ接続の作成

interface ファイルから Data Assurance (DA) リソースをインポートします。

9. オプションの設定手順

ユーザ認証、アラート、データ収集スケジューリング、バックアップ、リポトリの設定除去オプションを含む詳細な設定を実行します。

参照：

- ユーザ承認 (54 ページ)
- ログイン、役割、グループ (106 ページ)
- セキュリティのセットアップ (78 ページ)
- ログインまたはグループへの役割の割り当て (100 ページ)

Data Assurance サーバのモニタリング設定

SAP Control Center を使用して監視する Data Assurance (DA) サーバを認証します。リソースが認証されると、SAP Control Center によって DA サーバ監視オプションが有効になります。

Data Assurance サーバの登録

リソース (モニタ対象として使用可能なサーバなど) を登録して、SAP Control Center がそのリソースと接続情報を認識できるようにします。

1. [Resource Explorer] で、[Resources] > [Register] を選択します。
2. 以下を指定します。

フィールド	説明
Resource Name	(必須) 登録するリソースの名前。大文字と小文字を使用して管理対象サーバの実際の名前を入力する。SAP Control Center に登録された名前が、サーバ名と完全一致しないと、トポロジビューなどの一部のモニタ機能が機能しない。
Resource Type	リソースタイプを選択する。 • Data Assurance Server - Data Assurance サーバをモニタする。
Description	リソースの識別に役立つ簡単な説明。

3. [Next] をクリックします。
4. リソースの接続情報を指定します。

フィールド	説明
Host Name	ローカルのホスト名。
Port Number	ローカルのポート番号。

5. (オプション) SCC で当該リソースの認証に使用可能なユーザ名とパスワードを入力して、そのソフトウェアバージョンを検索します。クレデンシャルはこの目的のみに使用され、使用後は破棄されます。

ここで認証を行いたくない場合は、[I do not want to supply authentication information] をクリックします。

この手順により、サーバが公式に認証を受ける (後の設定プロセス) 前に SCC でそのサーバの正しいバージョン情報を表示できるようになります。

6. [Next] をクリックします。
7. (オプション) [Add this resource to the current perspective] をクリックします。リソースの管理やモニタを可能にするには、リソースをパースペクティブ (現在のパースペクティブである必要はない) に追加する必要があります。
8. (オプション) [Open the resource explorer to view this new resource] をクリックします (このオプションは、Resource Explorer が開いているときは存在しません)。
9. [Finish] をクリックします。

参照：

- 共通の表示オプション (5 ページ)
- リソース (149 ページ)
- リソースの登録解除 (149 ページ)

一括登録のためのリソースのインポート

(オプション) 複数のサーバを `interfaces` または `sql.ini` ファイルからインポートして登録します。

前提条件

`interfaces` または `sql.ini` ファイルを、Web ブラウザをホストするマシン上のロケーション、またはそのマシンからアクセス可能なロケーションにコピーします。

手順

`interfaces` (UNIX) ファイルまたは `sql.ini` ファイル (Windows) には、SAP データベースサーバとそのポートがリストされています。他の接続情報もある場合があります。このファイルは、サーバのインストール時に作成されます。

- Windows の場合: `%SYBASE%\%ini%sql.ini`
- Unix の場合: `$SYBASE/interfaces`

`interfaces` ファイルの詳細については、『設定ガイド Open Client/Open Server 15.0 UNIX 版』で、設定ファイルに関する付録を参照してください。

sql.ini ファイルの詳細については、『設定ガイド SAP Sybase ASE 15.0 Windows 版』で、sql.ini を使用するネットワーク通信に関する章を参照してください。

注意： Import Resources ウィザードは、1つのタイプ (SAP ASE、SAP® Sybase IQ®、Replication Server など) のサーバを一括でインポートします。interfaces ファイルまたは sql.ini ファイルに複数のタイプが構成されている場合、各リソースタイプに対してこの手順を実行する必要があります。

1. アプリケーションのメニューで、[View] > [Open] > [Resource Explorer] を選択します。
2. [Resource Explorer] で、[Resources] > [Import] を選択します。
Import Resources ウィザードが開きます。[Interfaces file] が既に選択されています。
3. [Next] をクリックします。
[Directory Service Connection] ページが表示されます。
4. [Browse] をクリックし、インポート元のインタフェースファイルに移動します。
[File name] フィールドには入力できません。
5. [Next] をクリックします。
6. [Import Resource Type] ページで、インポートするサーバのタイプを選択します。
7. [Resource Selection] ページで、インポートするサーバをクリックして選択します。
[Import Resource Type] ページで選択したタイプのサーバのみを選択します。正しくないタイプのサーバをインポートすると、それらは SAP Control Center によって適切にモニタまたは管理されません。
8. リソースのタイプによっては、ファイルに構成されている接続パラメータ以外に、たとえば、Replication Server の RSSD ホスト名とポート、SAP ASE の文字セットと言語など、その他の設定が必要になります。必要な接続パラメータをすべて入力します。
9. [Next] をクリックします。
10. (オプション) [Add these resources to the current perspective] をクリックします。リソースの管理やモニタを可能にするには、リソースを観点 (現在の観点である必要はない) に追加する必要があります。
11. [Next] をクリックします。
[Confirmation] ページに、選択したリソースのリストが表示されます。
12. インポートする準備が整ったら、[Finish] をクリックします。選択を変更するために以前の画面に戻るには、[Back] をクリックします。

[Finish] をクリックすると、SCC によってリソースがインポートされて登録され、概要ページに表示されます。

13. [Close] をクリックして、ウィザードを終了します。

新しくインポートされたリソースが [Resource Explorer] に表示されます。現在のパースペクティブに追加することを選択している場合、リソースは [Perspective Resources] ビューにも表示されます。

参照：

- リソース (149 ページ)
- リソースの登録解除 (149 ページ)

管理対象リソースのログインアカウントの認証

SAP Control Center がサーバまたはエージェントに接続して監視データを収集したりリソースを管理したりする場合に使用するログインアカウントとパスワードを指定します。

SAP Control Center に登録されている各リソースごとにこのタスクを実行します。

注意： アラートまたは収集ジョブの作成などの管理タスクの間にサーバを認証することもできます。

1. ブラウザを SAP Control Center に接続し、ログインします。
2. [Perspective Resources] ビューが開いていない場合は、ツールバーの [Show/Hide Perspective Resources View] アイコンをクリックします。
3. [Perspective Resources] ビューでリソースを選択し、ビューメニューから [Resource] > [Authenticate] を選択します。
4. [Use my current SCC login] または [Specify different credentials] を選択します。

注意： [Use my current SCC login] オプションは SCC for Replication では使用できません。

5. [Specify different credentials] を選択した場合は、リソースへの接続に使用する SAP Control Center のログインとパスワードを入力します。
6. 選択したリソースが Replication Server の場合は、RSSD ユーザ名とパスワードを入力します。
7. [OK] をクリックして、保存してダイアログを終了します。

参照：

- ユーザ承認 (99 ページ)

統計収集のセットアップ

データ収集ジョブを作成し、スケジュールをジョブに追加するには、管理対象リソースの [Properties] ビューを使用します。

統計の収集は、システムリソースを大量に消費します。多数の収集ジョブを実行すると、サーバの負荷が大きくなります。最適のパフォーマンスを実現するために、Sybase では、データ収集ジョブのスケジューリングについて、次のようなガイドラインをおすすめします。

- 各収集に対して1つのみの収集ジョブをスケジュールします。
- 収集の間隔を5分以上に設定します(デフォルトは5秒です)。

管理対象リソースのデータ収集は、リソースから認証されるまで実行されません。

1. [Perspective Resources] ビューで、リソースを選択して、ドロップダウン矢印をクリックし、[Resource] > [Properties]を選択します。
2. [Collection Jobs] を選択します。
3. [Create Job] をクリックします。
4. このリソースがまだ認証されていない場合は、[Authentication] ページが表示されます。SAP Control Center がリソースにログインするために使用するユーザー名とパスワードを入力します。[Authenticate] をクリックしてクレデンシャルを検証します。データ収集は、認証されたリソースでのみ実行されます。
5. [Collection Information] ページで、このジョブを実行するデータ収集を選択します。
6. (オプション) このジョブをレポジトリに保存しない場合は、[Save data collected from this job] を選択解除します。

収集データを保存しないことを選択すると、ジョブが実行される時に開いているすべてのビュー(ヒートチャートやリソースモニタなど)が更新されます。開いているビューがない場合は、ジョブを実行してもデータは取得されません。

このオプションは、ジョブの作成後は変更できません。変更する必要がある場合は、データ収集を削除して、再度追加します。

7. [Next] をクリックします。
8. (オプション) スケジュールを作成しない場合は、[Create a schedule for this job] を選択解除します。
9. 新しいスケジュールの詳細を指定します。

フィールド	説明
Name	このスケジュールの名前
Description	このスケジュールの説明

10. ジョブの開始を [Now] または [Later] から選択します。[Later] を選択する場合は、開始する日時を指定します。

11. このスケジュールの期間を指定します。ジョブを実行します。

- [Once]
- [Repetitively] (指定した間隔で)

フィールド	説明
Repeat interval	ジョブ実行の間の期間 (秒、分、時間、または日)

- [Until] (指定する間隔で指定した停止日まで)

フィールド	説明
Repeat interval	ジョブ実行の間の期間 (秒、分、時間、または日)
Stop date	ジョブが実行を停止する日時

注意： 日時は、現時時間を使用して入力します。SAP Control Center が必要に応じて入力された時間をリモートのタイムゾーンに変更します。

スケジュールを作成した後にその期間 (once/repetitively/until 設定) を変更することはできません。スケジュールの期間を変更するには、削除してからスケジュールを作成しなおします。

12. [Finish] をクリックします。

参照：

- エージェント接続の作成 (117 ページ)
- ジョブスケジューリング (144 ページ)
- スケジュールの表示または削除 (147 ページ)

統計について

SAP Control Center の可用性統計とパフォーマンス統計について説明します。

SAP Control Center で扱う統計には、次の 2 つのタイプがあります。

- 可用性統計は、現在の状態に重点を置いており、モニタリングしているリソース (たとえばサーバまたはエージェント) が適切に実行し、機能しているかどうかを判断するのに役立ちます。

設定

- パフォーマンス統計は、同一リソースの時間経過に伴う動作に重点を置いています。お使いの環境におけるデータの流れを表します。パフォーマンス統計を使用することによって、傾向の把握、リソースボトルネックなどの問題の識別、リソース計画の作成を実行できます。

SAP Control Center には、事前定義された主要パフォーマンス指標 (KPI) が製品モジュールごとに用意されており、これらの KPI はコレクションにグループ化されます。サーバステータスなどの KPI は、フレッシュなときは可用性統計に使用されますが、履歴パフォーマンス統計として長期間の値も保持します。

可用性統計は、各製品モジュールのヒートチャート画面とリソースモニタリング画面に表示されます。

パフォーマンス統計は、各製品モジュールの統計チャート画面とリソースモニタリング画面に表示されます。

一部の KPI は、製品モジュールごとに、デフォルトで収集されます。他の KPI をヒートチャート、統計チャート、リソースモニタリングのビューで表示するには、スケジューラで収集ジョブをセットアップする必要があります。データ収集と、それらで収集される KPI の詳細については、データ収集のヘルプトピックを参照してください。

いくつかの設定オプションが、SAP Control Center のデータの収集と表示に影響を及ぼします。

- 収集実行間隔 データ収集の頻度。これをスケジューラで収集ジョブに設定します。
- 画面再表示間隔 画面の再表示間隔。画面の再表示によって、最新の利用可能なデータが表示されます。画面再表示間隔は製品モジュールで設定します (モジュールによっては、設定できません)。
- チャート傾向期間 履歴チャートで表示対象となるデータの期間。チャート傾向期間は製品モジュールで指定します (設定できないモジュールもあります)。

Data Collections for SAP Replication Server Data Assurance のオプション

SAP Control Center for Data Assurance (DA) のデータ収集では、サーバとエージェントの高度な情報を収集します。

デフォルトのまたは定義済みのデータ収集のいずれかから DA データの収集をスケジューリングできます。DA サーバが認証されると、`collection_da_overview` というデフォルトのデータ収集が設定されます。

参照:

- ジョブスケジューリング (144 ページ)

Data Assurance の主要パフォーマンス指標

主要パフォーマンス指標 (KPI) は、SAP Control Center で Data Assurance (DA) サーバのダッシュボードやチャートに表示される統計を提供します。

Data Assurance のデフォルトのデータ収集 [collection_da_overview] で使用される KPI は次のとおりです。

KPI	説明
Server CPU Utilization	サーバ全体の CPU 使用率 (パーセンテージ表記)。
Server Memory Utilization	サーバ全体のメモリ使用率 (パーセンテージ表記)。
Agent CPU Utilization	エージェント全体の CPU 使用率 (パーセンテージ表記)。
Resource State	リソースの状態 (Running、Stopped、Unknown など)。
Agent Memory Utilization	エージェント全体のメモリ使用率 (パーセンテージ表記)。

Data Assurance サーバ、エージェント、データベース接続のステータス

ステータスは、ダッシュボード、ヒートチャート、トポロジアイコンで使用されます。

状態	説明
Running	DA オブジェクトは、アクティブ状態である。
Stopped	DA オブジェクトは、停止されている。
Unknown	DA オブジェクトの状態を判断できない。

エージェント接続の作成

compareset およびスキーマジョブの作成に必要な Data Assurance (DA) エージェント接続を作成します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Agent Connections] を選択します。
4. 次のいずれかを行います。

設定

- [Folder] > [Create Agent Connection] を選択します。
- [Data Assurance Agent Connections] を選択した際に表示されるボタンをクリックし、[Create Agent Connection] を選択します。

5. エージェント接続情報を指定します。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択。
Name	(必須) エージェント接続の名前。スペースは使用できない。
Host	(必須) DA エージェントがインストールされているサーバの名前。
Port	(必須) DA エージェントのポート番号。
Username	(必須) DA エージェントのユーザ名。
Password	(必須) DA エージェントのパスワード。
Description	エージェント接続の識別に役立つ簡単な説明。

6. (オプション) [Test] をクリックして、指定したエージェント接続情報が正しいことを確認します。
7. [OK] をクリックします。

新しいエージェント接続プロファイルが [Data Assurance Agent Connections] テーブルに表示されます。

参照：

- 統計収集のセットアップ (114 ページ)
- Data Assurance エージェント (169 ページ)
- エージェント接続の編集 (169 ページ)
- エージェント接続の削除 (170 ページ)
- すべてのエージェント接続の表示 (170 ページ)
- エージェント接続のテスト (171 ページ)

データベース接続の作成

Data Assurance (DA) サーバにプライマリデータベース接続および複製データベース接続を設定します。

1. [Perspective Resources] ビューで DA サーバを選択します。

2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Create Database Connection] を選択します。
 - [Database Connections] を選択した際に表示されるボタンをクリックし、[Create Database Connection] を選択します。
5. データベース接続情報を指定します。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択する。
Name	(必須) データベース接続の名前。スペースは使用できない。
Description	データベース接続の識別に役立つ簡単な説明。
Type	(必須) データベースタイプ。SAP Adaptive Server Enterprise (SAP ASE)、SAP ASE Cluster、Replication Server System Database (RSSD)、Oracle、IQ、SAP HANA データベース、Microsoft SQL Server、および IBM DB2 がある。
Agent	(必須) データベースへの接続に使用する DA エージェント。DA サーバのインストールで定義されるローカルエージェント、[Data Assurance Agent Connections] に定義されているリモートエージェント、またはまだ定義されていない新しいリモートエージェントのいずれかである。
Database	(必須) 接続先のデータベース名。
Host	(必須) データベースが置かれているサーバの名前。
Port	(必須) データベースのポート番号。
Username	(必須) データベースのユーザ名。
Password	データベースのパスワード。
Property	JDBC 接続のプロパティ。 注意： SAP ASE への SSL 接続をサポートする追加の JDBC プロパティを入力します。

6. (オプション) [Test] をクリックして、正しいデータベース情報を指定したことを確認します。
7. [OK] をクリックします。

新しいデータベース接続が [Database Connections] テーブルに表示されます。

参照：

- データベース接続 (171 ページ)
- データベース接続の編集 (171 ページ)
- データベース接続の削除 (172 ページ)
- すべてのデータベース接続プロファイルの表示 (173 ページ)
- データベース接続のテスト (173 ページ)

interface ファイルからの単一接続またはクラスタ接続の作成

interface ファイルから Data Assurance (DA) リソースをインポートします。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Import Connection] を選択します。
 - [Database Connections] を選択した際に表示されるボタンをクリックし、[Import Connection] を選択します。
5. ローカルドライブをブラウズして、interface ファイルまたは `sql.ini` ファイルを選択し、[Next] または [Import Resource Type] をクリックします。
6. 使用する DA サーバおよびリソースタイプを選択して、[Next] または [Resource Selection] をクリックします。
7. インポートするリソースおよびこの接続で使用するエージェントを選択して、選択したエージェントに接続するためのユーザ名とパスワードを指定し、[Next] または [Confirm] をクリックします。

注意： パスワードフィールドは必須ではありません。

8. [Finish] をクリックします。

参照：

- データベース接続 (171 ページ)
- データベース接続の編集 (171 ページ)
- データベース接続の削除 (172 ページ)
- すべてのデータベース接続プロファイルの表示 (173 ページ)
- データベース接続のテスト (173 ページ)

オプションの設定手順

ユーザ認証、アラート、データ収集スケジューリング、バックアップ、リポジットの設定除去オプションを含む詳細な設定を実行します。

表 12 : 設定領域

設定領域	説明	トピック
ユーザ認証	ユーザのグループを設定したり、役割を割り当てる。管理者権限 (sccAdminRole) を持つユーザが必要。	ユーザ認証 (99 ページ)
認証	Windows、UNIX、および LDAP ユーザが SAP Control Center にログインできるように認証モジュールを追加する。	セキュリティの設定 (78 ページ)
データ収集	収集間隔とスケジュールの変更、スケジュールの中断および再開、収集ジョブの削除を行う。	ジョブスケジューリング (144 ページ)
リソース	リソースの登録解除、パースペクティブへの追加、削除を行う。	リソース (149 ページ)
パースペクティブ	パースペクティブの作成、削除、名前の変更を行う。	パースペクティブ (152 ページ)
リポジット	除去オプションの設定、リポジットリデータベースのバックアップのスケジューリングを行う。	リポジット (155 ページ)

設定

データローとスキーマの比較

複数の SAP ASE データベース間でデータローとスキーマを比較し、不一致を表示します。

comparesets

comparesets は、テーブルとカラムのセットで構成され、特定のジョブで比較されるデータを定義します。

compareset には、次の内容が含まれます。

- 比較するテーブル
- ローをユニークに定義するキーカラム
- 比較するカラム
- 比較するローを定義する **WHERE** 句

compareset では、ソースとターゲットのテーブルとカラムが同じ名前である必要はありません。各 compareset には、1つのソースと1つ以上のターゲットが必要です。任意の数のジョブで使用できます。

Compareset の作成

データベース接続プロファイルおよび比較するソーステーブルおよびターゲットテーブルを含む compareset を作成します。

前提条件

エージェント接続を作成したことを確認します。

手順

1. [Perspective Resources] ビューで Data Assurance サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Comparesets] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Create Compareset] を選択します。
 - [Data Assurance Comparesets] を選択した際に表示されるボタンをクリックし、[Create Compareset] をクリックします。

5. compareset の基本情報を指定し、[Next] または [Source Table] をクリックします。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択する。
Name	(必須) compareset の名前。
Description	compareset の識別に役立つ簡単な説明。

6. 既存のデータベース接続を選択するか、[New] をクリックして新しい接続を作成します。
7. スキーマおよびデータベーステーブルを選択します。
8. 比較する列を選択します。
9. (オプション) 比較ジョブを制御する制約を指定します。
10. [Next] または [Target Table(s)] をクリックします。
11. ソーステーブルに対して実行したのと同じ手順を繰り返します。
12. (オプション) [Add Target] をクリックしてソーステーブルと比較する新しいターゲットテーブルを定義します。

注意： ソーステーブルは、1つ以上のターゲットテーブルと比較できます。

13. [Finish] をクリックします。

参照：

- Data Assurance エージェント (169 ページ)
- エージェント接続の作成 (117 ページ)
- データベース接続の作成 (118 ページ)
- ロー比較ジョブの作成 (127 ページ)

compareset の編集

既存の compareset の詳細を変更します。

前提条件

変更する compareset が、実行中のジョブで使用されていないことを確認します。

手順

1. [Perspective Resources] ビューで Data Assurance サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Comparesets] を選択します。

4. compareset を選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。
 - compareset を選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. 必要に応じて、ソーステーブルとターゲットテーブルの詳細を変更します。
ソーステーブルを別のターゲットテーブルにマップすることもできます。
6. [Apply] をクリックして、[OK] をクリックします。

参照：

- データベース接続の作成 (118 ページ)
- ロー比較ジョブの作成 (127 ページ)
- Data Assurance のジョブのステータスおよびレポートの表示 (138 ページ)

Compareset の削除

リストから compareset を削除します。

前提条件

削除する compareset が実行中のジョブで使用されていないことを確認します。

手順

1. [Perspective Resources] ビューで Data Assurance サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Comparesets] を選択します。
4. compareset を選択し、次のいずれかを実行します。
 - [Resource] > [Delete] を選択します。
 - compareset を選択した際に表示されるボタンをクリックし、[Delete] を選択します。
5. [OK] をクリックします。

参照：

- Data Assurance のジョブのステータスおよびレポートの表示 (138 ページ)

すべての compareset の表示

Data Assurance (DA) サーバの compareset をすべて表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Comparesets] を選択します。

データパーティション境界値の表示

各 comparesets に対して保存されるデータパーティション境界値を表示します。

1. [Perspective Resources] ビューで、DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Comparesets] を選択します。
4. compareset を選択します。
5. compareset を選択した際に表示されるボタンをクリックし、[Boundaries...] を選択します。

Data Assurance のジョブ

Data Assurance (DA) のジョブは、ロー比較またはスキーマ比較のいずれかです。

ロー比較ジョブを作成する際、使用する compareset を指定し、ジョブを実行するスケジュールを設定します。ロー比較ジョブは、日、週、または月単位で実行できます。あるいは、手動で実行することもできます。スキーマ比較ジョブは手動で実行できますが、スケジュールすることはできません。

また、ロー比較ジョブは Replication Server System Database (RSSD) に基づいて作成できます。このためには、テーブルレベルの複写定義およびサブスクリプションを SAP Replication Server の RSSD からインポートします。

『Replication Server Data Assurance オプションユーザーズガイド』>「Replication Server Data Assurance オプション」>「ジョブと比較」を参照してください。

ロー比較ジョブ

ロー比較では、対象のデータベーステーブルすべてのローをプライマリキーまたはユニークキーでソートし、1 つずつ比較します。比較の概要は、Data Assurance システムデータベース (DASD) に保存されます。ローの相違を示す詳細なテキストまたは XML レポートは、データディレクトリに保存されます。

ロージョブでは、比較オブジェクトを作成し、compareset を特定の比較に追加し、さまざまな比較パラメータを設定し、比較を実行する必要がある時間を設定します。

ロー比較ジョブの作成

ロー比較ジョブを設定します。

前提条件

compareset を作成したことを確認します。

手順

1. [Perspective Resources] ビューで Data Assurance サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Create Job] を選択します。
 - [Database Assurance Jobs] を選択した際に表示されるボタンをクリックし、[Create Job] を選択します。
5. 次のようなロー比較ジョブの基本情報を指定します。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択する。
Name	(必須) ロー比較ジョブの名前。
Active	選択するとロージョブを実行できることを示す。
Description	ロー比較ジョブの識別に役立つ簡単な説明。

6. [Next] または [Option] をクリックします。
7. 同時ジョブの最大数の値を入力します。
同時に実行するジョブの最大数です。
8. [Next] または [Comparison] をクリックします。
9. 設定している現在の比較の一般的な情報を指定します。

フィールド	説明
Name	(必須) ロー比較ジョブの比較の名前。
Active	選択された場合に比較ジョブを実行できることを示す。

フィールド	説明
Description	比較の識別に役立つ簡単な説明。
Priority	比較の優先レベル。
Compareset	事前定義された compareset の名前。compareset には、比較するソーステーブルとターゲットテーブルが含まれている。

注意： 1つのロー比較ジョブに対して複数の比較を作成できますが、パフォーマンスが低下することがあります。複数の比較を作成するには、[Add Comparison] をクリックします。

10. (オプション) [Comparison Options] タブで、比較オプションのデフォルト値を変更するか、受け入れます。
11. (オプション) [Column Options] タブで、compareset に含まれている各列の列オプションのデフォルト値を変更するか、受け入れます。
12. (オプション) [Next] または [Schedule] をクリックします。
13. (オプション) [With Schedule (s)] をクリックして、このロー比較ジョブのスケジュールを設定します。または、後からスケジュールを設定したり、手動でジョブを実行することもできます。
14. [Finish] をクリックします。

参照：

- comparesets (123 ページ)

比較とカラムのオプション

ロージョブを作成するための比較とカラムのオプションを把握しておいてください。

表 13 : 比較オプション

フィールド	説明
Abort condition (rows):	差異のカウン트가指定値を超えた場合、ロー比較をアボートする。 有効な値: 1 ~ 9223372036854775807 デフォルト値: 1000

フィールド	説明
Abort row count mismatch:	<p>テーブルのローカウントが一致しない場合にロー比較を中止するかどうかを決定する。</p> <p>有効な値: true または false</p> <p>デフォルト値: false</p>
Auto reconciliation:	<p>調整スクリプトを自動的に適用するかどうかを示す。</p> <p>有効な値: true または false</p> <p>デフォルト値: false</p> <hr/> <p>注意: AUTO_RECONCILE を有効にするには、CREATE_COL_LOG を true に設定します。</p>
Compare mode:	<p>ロー比較モードを指定する。</p> <ul style="list-style-type: none"> row_compare - すべてのテーブルローを比較する。 key_compare - プライマリキーカラムを比較する。 row_count - ローカウントを比較する。 <p>デフォルト値: row_compare</p>
Compress row data:	<p>ローデータをエージェントとサーバの間で比較する。</p> <p>有効な値: true または false</p> <p>デフォルト値: false</p>
Create column log:	<p>すべての消失ロー、孤立したロー、および一貫性のないローの値 (キーおよびカラム) をリストしたカラムの差異についてのログを生成する。以下を実行する場合は、カラムログを作成する。</p> <ul style="list-style-type: none"> 調整スクリプトを生成 自動調整を実行 詳細なレポートを生成 <p>有効な値: true または false</p> <p>デフォルト値: false</p>
Create reconciliation script:	<p>調整スクリプトを生成する。このパラメータを使用するには、CREATE_COL_LOG も true に設定する必要がある。</p> <p>有効な値: true または false</p> <p>デフォルト値: false</p>

データローとスキーマの比較

フィールド	説明
Enable row count:	<p>送信元テーブルおよびターゲットテーブルのローを比較前にカウントするかどうかを指定する。DA サーバは、比較の進行状況と終了時刻を見積もるためにローカウントを使用する。</p> <hr/> <p>注意： <code>COMPARE_MODE</code> が <code>row_count</code> の場合に、DA サーバはローをカウントします。<code>ENABLE_ROW_COUNT</code> は、<code>COMPARE_MODE</code> の値が <code>row_count</code> 以外の場合にのみ使用してください。</p> <hr/> <p>有効な値: true または false デフォルト値: true</p>
External sort:	<p>エージェント上のローをソートすることで、データベースで ORDER BY 句の処理の影響を低減する。</p> <p>有効な値: true または false デフォルト値: false</p>
Hash type:	<p>比較のハッシュタイプを指定する。</p> <ul style="list-style-type: none"> • <code>database_hash</code> - データベースによって指定されたハッシュ関数を使用する。 • <code>agent_hash</code> - Replication Server Data Assurance オプションによって指定されたハッシュ関数を使用する。 <hr/> <p>注意： 異機種間での比較の場合は、ハッシュタイプ比較オプションを <code>agent_hash</code> に設定します。<code>database_hash</code> 比較オプションは、SAP ASE 同士の比較にのみ使用します。</p>
Maximum retry:	<p>前の比較と異なる結果があるローの再比較を行う合計回数を指定する。</p> <p>有効な値: 0 ~ 100 デフォルト値: 3</p>
Partitions:	<p>テーブルのパーティションの数を指定する。</p> <hr/> <p>注意： このパーティションの数は 0 より大きくする必要があり、最大値 1024 より大きい値は指定できません。</p> <hr/> <p>デフォルト値: 1</p>

フィールド	説明
Retry option:	リトライオプションを指定する。 <ul style="list-style-type: none"> never -再比較を実行しない。 wait_and_retry -RETRY_MAX および RETRY_DELAY_SEC の設定に基づいて再比較を実行する。 デフォルト値: never
Retry delay (seconds):	再比較と再比較の遅延の秒数を指定する。 有効な値: 0 ~ 86400 デフォルト値: 10

表 14 : カラム比較オプション

カラムオプション	値
Compare mode:	各カラムの比較方法を指定する。 <ul style="list-style-type: none"> column_hash - カラムのハッシュ値を使用して比較を実行する。 row_hash - 合計ハッシュ値を使用して、このオプションが指定されたすべてのカラムを一緒に比較する。 literal - カラムのリテラル値を使用して比較を実行する。

ロー比較ジョブの編集

Data Assurance (DA) ロー比較ジョブの詳細を変更します。

- [Perspective Resources] ビューで DA サーバを選択します。
- [Resource] > [Administration Console] を選択します。
- [Data Assurance Server] を展開し、[Data Assurance Job] を選択します。
- ロー比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。
 - ロー比較ジョブを選択した際に表示されるボタンをクリックし、[Properties] を選択します。
- 必要に応じて、[General]、[Comparisons]、[Options]、および [Schedules] タブでジョブの情報を変更します。
 [Comparison] タブで詳細を変更するには、次の手順に従います。

データローとスキーマの比較

- a) 比較を選択して、表示されるボタンをクリックし、[Properties] を選択します。
- b) 必要に応じて、[General]、[CompareSet]、および [Options] タブで比較の情報を変更します。
[Comparisons] タブでタブごとに変更を行って [Apply] をクリックしたら、[OK] をクリックします。

6. [Apply] をクリックして、[OK] をクリックします。

ロー比較ジョブのスケジューリング

Data Assurance (DA) ロー比較ジョブをスケジューリングします。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. ロー比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。
 - ロー比較ジョブを選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. [Schedules] を選択し、表示されるボタンをクリックし、[Create Schedule] をクリックします。
6. ジョブを実行する日時を設定します。
7. [Apply] をクリックして、[OK] をクリックします。

Replication Server System Database に基づくジョブの作成

Replication Server の既存のテーブルレベルの複写定義およびサブスクリプションに基づいて、Data Assurance (DA) ジョブを作成します。

前提条件

Replication Server system database (RSSD) 接続を作成したことを確認します。

手順

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Import Job from RSSD] を選択します。

- [Database Assurance Jobs] を選択した際に表示されるボタンをクリックし、[Import Job from RSSD] を選択します。

5. ジョブの基本情報を指定します。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択する。
Name	(必須) RSSD ジョブの名前。
RSSD connection	(必須) [Database Connection] で作成した、使用する RSSD 接続。 Replication Server system database (RSSD) 接続を選択するには、[Select] を選択する。
Description	RSSD に基づくジョブの識別に役立つ簡単な説明。
Maximum concurrent jobs	同時に実行する RSSD ジョブの最大数。
Priority for comparison(s)	優先レベル。

6. [Next] または [Source DB Mapping] をクリックします。
7. RSSD のソースデータベース情報および DA サーバのデータベース接続を選択します。

注意： [Selected] チェックボックスで、比較の生成をフィルタリングできます。選択したデータベースセットにプライマリデータベース引数が含まれている複写定義のみを使用して比較が生成されます。

8. [Next] または [Target DB Mapping] をクリックします。
9. RSSD のターゲットデータベース情報および DA サーバのデータベース接続を選択します。

注意： [Selected] チェックボックスで、比較の生成をフィルタリングできます。選択したデータベースセットに複写データベース引数が含まれているサブスクリプションのみを使用して、自動生成された比較のターゲット引数が生成されます。

10. [Next] または [Comparisons Options] をクリックします。
11. 比較オプションを指定します。
12. (オプション) [Next] または [Schedule] をクリックします。
13. [Finish] をクリックします。

参照：

- 比較とカラムのオプション (128 ページ)

データローとスキーマの比較

- データベース接続の作成 (118 ページ)

スキーマ比較ジョブ

スキーマ比較では、1つのプライマリデータベースのスキーマを1つまたは複数のレプリケートデータベースと比較できます。自動テーブル名マッピングを使用してデータベーススキーマ全体を比較したり、テーブル名マッピングを使用して特定のテーブルを比較したりすることができます。

スキーマ比較ジョブの作成

Data Assurance (DA) サーバのデータベースレベルオブジェクトとテーブルレベルオブジェクトを比較するスキーマ比較ジョブを設定します。

前提条件

エージェント接続を作成したことを確認します。

手順

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. 次のいずれかを行います。
 - [Folder] > [Create Schema Job] を選択します。
 - [Data Assurance Jobs] を選択した際に表示されるボタンをクリックし、[Create Schema Job] を選択します。
5. スキーマジョブの基本情報およびオプション情報を指定します。

フィールド	説明
Data Assurance server	(必須) DA サーバの名前。ドロップダウンリストから選択する。
Name	(必須) スキーマ比較ジョブの名前。
Description	スキーマ比較ジョブの識別に役立つ簡単な説明。
Maximum concurrent jobs	(必須) 同時に実行するスキーマ比較ジョブの最大数。

6. [Next] または [Comparisons] をクリックします。
7. [Create] をクリックしてスキーマジョブの比較を指定します。
8. 比較の基本情報を指定します。
9. [Next] または [Data Sources] をクリックします。

10. [Select Source] をクリックします。
11. ソースデータのデータベース接続プロファイルを選択し、[OK] をクリックします。
12. [Add Target] をクリックします。

注意： 複数のターゲットデータベースを追加できます。

13. ターゲットデータのデータベース接続プロファイルを選択し、[OK] をクリックします。
14. [Next] または [Include All Tables] をクリックします。
15. [Include all tables] を選択します。
16. (オプション) スキーマ比較から除外する [Add Table] をクリックします。
17. [Next] または [Map Tables] をクリックします。
18. (オプション) [Add Mapping] をクリックして、スキーマを比較するソーステーブルとターゲットテーブルのマッピングを指定します。

注意： 1つのスキーマ比較に対して少なくとも1つの属性 (include-all または テーブルマッピング) を設定します。テーブルマッピングを選択すると、異なる名前を持つテーブルのスキーマを比較できます。

19. [Finish] を2回クリックします。

参照：

- Data Assurance エージェント (169 ページ)
- 比較とカラムのオプション (128 ページ)
- Data Assurance ジョブの削除 (137 ページ)
- Data Assurance のジョブの実行 (136 ページ)
- Data Assurance のすべてのジョブの表示 (137 ページ)
- Data Assurance のジョブのステータスおよびレポートの表示 (138 ページ)
- エージェント接続の作成 (117 ページ)

スキーマ比較ジョブの編集

Data Assurance (DA) スキーマ比較ジョブの詳細を変更します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. スキーマ比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。

データローとスキーマの比較

- スキーマ比較ジョブを選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. 必要に応じて、[General]、[Comparisons]、および [Options] タブでスキーマジョブの情報を変更します。
[Comparison] タブで詳細を変更するには、次の手順に従います。
 - a) スキーマ比較を選択して、表示されるボタンをクリックし、[Properties] を選択します。
 - b) 必要に応じて、[General]、[Data Source]、[Include All Tables]、および [Map Tables] タブでスキーマ比較の情報を変更します。
タブごとに変更を行って [Apply] をクリックしたら、[OK] をクリックします。
 6. [OK] をクリックします。

参照：

- 比較とカラムのオプション (128 ページ)
- Data Assurance ジョブの削除 (137 ページ)
- Data Assurance のジョブの実行 (136 ページ)
- Data Assurance のすべてのジョブの表示 (137 ページ)
- Data Assurance のジョブのステータスおよびレポートの表示 (138 ページ)

Data Assurance のジョブの管理と実行

Data Assurance のジョブを実行してレポート、ジョブステータス、ジョブ履歴を表示します。

Data Assurance のジョブの実行

Data Assurance (DA) のロー比較ジョブまたはスキーマ比較ジョブを実行します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。
4. ロー比較ジョブまたはスキーマ比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Run] を選択します。
 - ロー比較ジョブまたはスキーマ比較ジョブを選択した際に表示されるボタンをクリックし、[Run] を選択します。

Data Assurance ジョブの削除

Data Assurance (DA) ロー比較ジョブまたはスキーマ比較ジョブを削除します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Assurance Jobs] を選択します。
4. ロー比較ジョブまたはスキーマ比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Delete] を選択します。
 - ロー比較ジョブまたはスキーマ比較ジョブを選択した際に表示されるボタンをクリックし、[Delete] を選択します。
5. [OK] をクリックします。

Data Assurance のジョブの比較を削除する

ローまたはスキーマ比較ジョブの比較を削除します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Assurance Jobs] を選択します。
4. ローまたはスキーマ比較ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。
 - ロー比較ジョブまたはスキーマ比較ジョブを選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. [Comparisons] を選択します。
6. 比較を選択して、表示されるボタンをクリックし、[Delete Comparison] を選択します。

Data Assurance のすべてのジョブの表示

Data Assurance (DA) のすべてのロー比較ジョブとスキーマ比較ジョブのリストを表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Jobs] を選択します。

Data Assurance のジョブのステータスおよびレポートの表示

Data Assurance (DA) のジョブの状態が実行中、保留中、完了、またはアポートであるかどうかを確認し、欠落したデータ、孤立したデータ、矛盾するデータのレポートを表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Monitor] を選択します。
3. Data Assurance Monitor で, [Job Status] を選択します。
4. (オプション) [Abort] をクリックし、実行中のジョブを停止します。

Data Assurance ジョブ履歴

Data Assurance (DA) ジョブ履歴には、実行されたジョブとそのジョブの送信時間および完了時間のリストが含まれます。

これらのジョブのレポートを表示して、テキスト形式または XML 形式で保存することもできます。

ジョブ履歴レポートの表示

完了した Data Assurance (DA) ジョブのリストを表示し、それらのジョブのレポートを表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Job Histories] を選択します。
4. DA ジョブを選択して、表示されるボタンをクリックし、[Report] を選択します。

ジョブ履歴の削除

ジョブ履歴を削除して、サーバの領域をクリアします。

1. [Perspective Resources] ビューで Data Assurance (DA) サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Job Histories] を選択します。
4. DA ジョブを選択し、次のいずれかを実行します。
 - [Resource] > [Delete] を選択します。
 - DA ジョブを選択した際に表示されるボタンをクリックし、[Delete] を選択します。
5. [OK] をクリックします。

管理とモニタ

SAP Control Center では、使用できるリソースの管理とモニタおよび統計情報の表示ができます。

リソースの可用性の表示: ヒートチャート

ヒートチャートを使用して、現在のパースペクティブのサーバのステータスと可用性を表示します。

ヒートチャートには、パースペクティブ内のリソースの状態 (リソースが実行中、中断中、停止中) が表示されます。これに加え、ヒートチャートには、各リソースのタイプが一覧表示され、最後のデータ収集の開始時間などの統計データが表示されます。

表示するリソースをフィルタリングしたり、検索したり、結果をカラムでソートすることができます。また、リソースを選択して、コンテキストメニューでプルダウンし、リソースタイプに基づいて異なる監視および管理オプションを表示できます。

ヒートチャートのデータは、管理対象サーバから直接収集され、収集されたときの日時でタグ付けされ、SAP Control Center リポジトリに保存されます。

1. アプリケーションのメニューバーで、[View] > [Open] > [Heat Chart] を選択します。
2. (オプション) チャートのアイコンが示すステータスの情報を表示するには、マウスをアイコンに合わせます。
 - [Status] カラム - アイコンのツールチップでリソースのステータスを説明します (実行中や停止など)。
 - [Status] の右側のすべてのカラム - アイコンのツールチップで、カラム上部に一覧表示された KPI の値を示します。
3. (オプション) フィルタリング (ヒートチャートのリソースのリストを絞り込む) やカラムを変更するためのツールを表示するには、[Perspective Heat Chart] メニューバーから [View] > [Filter] を選択します。
[Filter and Column tools] が左側のペインに表示されます。
4. (オプション) フィルタリングを使用するには、ビューのメニューバーから [View] > [Filter] を選択し、[Filter string] フィールドに検索ワードを入力します。

検索単語には、サーバまたはリソースのタイプの名前または名前の一部など、ヒートチャートのテーブル部分に表示される任意の文字列を入力できます。たとえば、「ASE Server」と入力できます。

5. (オプション) フィルタリング設定として以下のいずれかを選択します。
 - [Match case]- 表示されるデータに、大文字と小文字を含む検索ワードが含まれているリソースを検索します。または
 - [Exact match] - 表示されるデータに、検索ワードと完全に一致する項目を含むリソースを検索します。
6. (オプション) [Filter on] リストからカラムを選択すると、カラムの検索を制限できます。
7. (オプション) [Columns] をクリックして、ヒートチャートのオプションをカスタマイズします。
8. (オプション) ヒートチャートに表示しないすべてのカラムを選択解除します。
9. (オプション) カラムヘッダのソート矢印をクリックして、カラム値を昇順または降順にソートします。
10. (オプション) リソースのローをクリックし、リソース名の右側のメニューをプルダウンして、選択したリソースで利用できるオプションを表示します。
11. (オプション) [Filter and Columns tools] ペインの大きさを調整するには、ツールのペインとリソーステーブルとの間の枠線の上でカーソルを移動します。カーソルの形がサイズ変更アイコンに変化したら、クリックして、枠線を左方向または右方向に移動します。
12. (オプション) [Filter and Columns] ツールを非表示にするには、[View] > [Filter] を選択解除します。

パフォーマンスカウンタのグラフ表示: 統計チャート

パフォーマンスの傾向を表示するには、指定された期間のパフォーマンスカウンタのセットのグラフを生成します。

前提条件

グラフ表示する統計データが収集されていることを確認します。データが収集されていることを確認するには、[Resource Properties] ビューの [Collection Jobs] ページに移動し、収集ジョブの [History] タブを確認します。リソースモニタでも確認できます。リソースモニタにデータが表示されたら、データが収集されています。

手順

ヒント： データ収集は、リソースによって認証されると開始されます。認証されてからの時間が短いリソースでは、有効なグラフを作成するのに十分なデータが蓄積されていないことがあります。

1. [Perspective Resources] ビューで、リソースをクリックして、ビューのメニューバーで [Resource] > [Statistics Chart] を選択します。
2. [Statistics] タブのフォルダを展開し、グラフ表示する主要パフォーマンス指標 (KPI: Key Performance Indicator) を選択します。
3. [Graph Statistic] をクリックするか、KPI を [Chart] タブにドラッグします。
[Chart] タブにはデータがグラフ表示され、KPI と対応する値、それが収集された日時が [Data] タブに表示されます。
4. (オプション) グラフ表示する KPI を追加する手順を繰り返します。
5. (オプション) [Chart] タブの下のスライダを使用して、グラフに表示する時間量を、分から年の範囲で制御します。
6. (オプション) 表示されるグラフを前または後に移動するには、[<<]、[<]、[>]、および [>>] を使用します。移動する量は、スライダの設定によって異なります。

ヒント： 統計チャートは固定期間のデータを表示し、この期間は自動的に変更されません。直近の統計を表示し、グラフを最新の状態に維持するには、新しい統計が収集されるごとに、表示される期間を調整します。

7. (オプション) スライダの上に [date] と [time] のラベルがあります。これらをクリックすることによって、グラフの開始時刻、終了時刻、表示期間を変更できます。
8. (オプション) [Clear Graph] をクリックして、すべてのグラフ表示されている統計を削除し、新たに開始します。

注意： 最大 2 つの異なる測定単位を使用して、最大 5 つの統計をグラフ表示できます。デフォルトでは、24 時間の統計のみが利用できます。これより長く統計を保存するには、レポートリ消去オプションを変更します。

参照：

- レポートリ消去の設定 (160 ページ)

SAP Control Center の管理

統計情報およびアクティビティログを使用して SAP Control Center for Data Assurance の管理とモニタを行います。

管理コンソール

パースペクティブで選択したリソースを参照し、管理するには、管理コンソールを使用します。

リソースの参照と管理

新しいリソースを作成するか、既存のリソースの参照と管理を実行します。

前提条件

既存のリソースを表示または管理するには、少なくとも 1 つのリソースを登録し、パースペクティブに追加します。

手順

管理コンソールを使用すると、サーバと、サーバレベルより下のプロセス、データベース、デバイスなどのリソースの両方を表示し、管理できます。

1. 管理コンソールを起動します。

- Administration Console に 1 つまたは複数のリソースの情報を表示するには、[Perspective Resources] ビューでリソースを選択し、[Resource] > [Administration Console] を選択します。この方法は、選択したリソースのみを表示するため、最も効率的な方法です。
- Administration Console にすべてのリソースの情報を現在のパースペクティブで表示するには、メインメニューバーで、[View] > [Open] > [Administration Console] を選択します。多数のリソースを監視している場合は、Administration Console にロードするのに数分かかります。

2. オブジェクトタイプの階層を展開するには、左ウィンドウ枠の[Navigation] > [Browse]を展開します。矢印アイコンをクリックして、オブジェクトタイプを展開します。

3. 階層のオブジェクトタイプ (サーバタイプなど) を選択します。

管理コンソールの右ウィンドウ枠に、そのタイプのリソースのリストが表示されます。

注意： 右ウィンドウ枠のメッセージローは、次のもののプレースホルダです。

- 失敗した要求 - 再試行するには、メッセージローを選択し、右側に表示されるドロップダウン矢印をクリックします。[Retry] を選択します。
- 応答の遅い要求 - これらのローは、real データが到着するとすぐに置き換えられます。
- 大量の結果セット - 表示するには、メッセージローを選択し、右側に表示されるドロップダウン矢印をクリックします。[Expand] を選択します。結果が表示されるまでに 1 分位かかる場合があります。

詳細情報を示すツールチップを表示するには、メッセージローにマウスを合わせます。

4. (オプション) 現在選択しているタイプのオブジェクトを作成するには、[Folder] > [Create] または [Folder] > [New] を選択します。
5. (オプション) ビューをリフレッシュするには、[Folder] > [Refresh] を選択します。
6. 左右いずれかのペインで、オブジェクトを選択します。ドロップダウン矢印が名前の右側に表示されます。右ウインドウ枠でオブジェクトが選択されている場合は、[Resource] メニューがアクティブになります。
7. ドロップダウン矢印をクリックして、オブジェクトで実行できるアクションのメニューを表示します。右ウインドウ枠でオブジェクトが選択されている場合は、[Resource] メニューを使用して同じアクションを表示します。

注意：一部の管理対象オブジェクトでは、実行できる操作はありません。

リソースの検索とフィルタリング

関心のあるリソースまたはリソース内のオブジェクトを迅速に検索するには、管理コンソールの検索およびフィルタツールを使用します。

1. 管理コンソールを起動します。
 - Administration Console に 1 つまたは複数のリソースの情報を表示するには、[Perspective Resources] ビューでリソースを選択し、[Resource] > [Administration Console] を選択します。この方法は、選択したリソースのみを表示するため、最も効率的な方法です。
 - Administration Console にすべてのリソースの情報を現在のパースペクティブで表示するには、メインメニューバーで、[View] > [Open] > [Administration Console] を選択します。多数のリソースを監視している場合は、Administration Console にロードするのに数分かかります。
2. (オプション) 管理コンソールのツールを使用して、表示されるリソースを制御できます。
 - a) 左ウインドウ枠で [Resource Selection] をクリックします。
 - b) 右ウインドウ枠にあるリソースのリストがリフレッシュされ、このウインドウ枠で行った選択が反映されます。複数選択による変更を行っている場

合は、[Automatically refresh details] を選択解除してリフレッシュ機能をオフにします。

- c) 管理コンソールの表示に含めるリソースを選択するか、表示から除外するリソースを選択解除します。

3. 階層をナビゲートせずにリソースを検索するには、次の手順を実行します。

- a) 左ウィンドウ枠で、[Navigation] > [Search] を選択します。
- b) (必須) [Search] タブで、検索するリソースのリソースタイプとオブジェクトタイプを選択します。
- c) 検索文字列を入力します。
検索文字列には、リソースの完全名または部分名を指定できます。
- d) (オプション) 名前が検索文字列と一致するリソースのみを検索するには、[Exact match] を選択します。
- e) [Search] をクリックします。
結果が右ウィンドウ枠に表示されます。

注意： 右ウィンドウ枠のメッセージローは、次のもののプレースホルダです。

- 失敗した要求 - 再試行するには、メッセージローを選択し、右側に表示されるドロップダウン矢印をクリックします。[Retry] を選択します。
- 応答の遅い要求 - これらのローは、real データが到着するとすぐに置き換えられます。
- 大量の結果セット - 表示するには、メッセージローを選択し、右側に表示されるドロップダウン矢印をクリックします。[Expand] を選択します。結果が表示されるまでに 1 分位かかる場合があります。

詳細情報を示すツールチップを表示するには、メッセージローにマウスを合わせます。

- f) 検索をさらに絞り込むには、検索結果のカラムの上部にあるフィールドにフィルタ文字列を入力します。たとえば、データベースの検索で、Device カラムの上に wilma と入力すると、デバイス wilma に関連する結果のみが表示されます。

ジョブスケジューリング

スケジュールとは、データ収集ジョブと、このジョブをシステムで実行する頻度を定義したものです。

SAP Control Center では、収集ジョブによって、モニタリング画面とチャートに表示されるデータが得られます。コレクションは、主要パフォーマンス指標 (KPI) のセットです。スケジューラで収集ジョブが実行されると、コレクションの各 KPI の値が収集され、収集された日時でデータがタグ付けされます。データは、リポジトリに保管されて表示されます。各製品モジュールには、スケジュール可能な、事前定義された収集ジョブがあります。

スケジュールは、1 回かぎり、または繰り返しとして定義できます。ジョブのスケジュールは、次のようないくつかの属性に基づいて変更できます。

- Repeat interval
- Date
- Time

ジョブ履歴には、それぞれの日に実行されたジョブのステータスが表示されます。

参照：

- 統計収集のセットアップ (114 ページ)
- Data Collections for SAP Replication Server Data Assurance のオプション (116 ページ)

データ収集ジョブの実行と停止

データ収集ジョブの実行または停止を行うには、[Properties] ビューを使用します。

ほとんどの場合、データ収集ジョブはスケジュールに従って実行する必要があります。ジョブを手動で開始または停止する必要があることはほとんどありません。

1. [Perspective Resources] ビューで、ジョブに関連付けられているリソースを選択し、[Resource] > [Properties] を選択します。
2. [Collection Jobs] を選択します。
3. ジョブを選択して、以下を実行します。
 - ジョブを即時実行するには、[Execute] をクリックします。
 - ジョブを停止するには、[Stop] をクリックします。次に、[Yes] をクリックして確定します。

データ収集ジョブの削除

1 つ以上のデータ収集ジョブを削除するには、リソースの [Properties] ビューを使用します。

1. [Perspective Resources] ビューで、ジョブに関連付けられているリソースを選択し、[Resource] > [Properties] を選択します。
2. [Collection Jobs] を選択します。
3. ジョブを選択し、[Delete] を選択します。
4. [OK] をクリックして、削除を確認します。

データ収集ジョブの再開と中断

リソースの [Properties] ビューを使用して、データ収集ジョブを再開または中断します。

1. [Perspective Resources] ビューからジョブに関連付けられたリソースを選択し、[Resource] > [Properties]を選択します。
2. [Collection Jobs] を選択します。
3. ジョブ ([Collection Jobs] テーブルの上位の項目) を選択します。 [General] タブで次の手順を実行します。
 - ジョブを再開するには、[Resume] をクリックします。
 - ジョブを停止するには、[Suspend] をクリックし、[Yes] をクリックして停止を確定します。

ヒント： [General] タブが灰色表示されている場合は、 [Collection Jobs] テーブルでジョブ (親) ではなくスケジュール (子) を選択しています。 [General] タブを表示するには、親のジョブを選択してください。

新規スケジュールのジョブへの追加

リソースの [Properties] ビューを使用して、データ収集ジョブにスケジュールを追加します。

1. [Perspective Resources] ビューからジョブに関連付けられたリソースを選択し、[Resource] > [Properties] を選択します。
2. [Collection Jobs] を選択します。
3. ジョブを選択します。
4. [Add Schedule] をクリックします。
5. 新しいスケジュールの詳細を指定します。

フィールド	説明
Name	このスケジュールの名前
Description	このスケジュールの説明

6. ジョブの開始を [Now] または [Later] から選択します。 [Later] を選択する場合は、開始する日時を指定します。
7. このスケジュールの期間を指定します。ジョブを実行します。
 - [Once]
 - [Repetitively] (指定した間隔で)

フィールド	説明
Repeat interval	ジョブ実行の間の期間 (秒、分、時間、または日)

- [Until] (指定する間隔で指定した停止日まで)

フィールド	説明
Repeat interval	ジョブ実行の間の期間 (秒、分、時間、または日)
Stop date	ジョブが実行を停止する日時

注意： 日時は、現時時間を使用して入力します。SAP Control Center が必要に応じて入力された時間をリモートのタイムゾーンに変更します。

スケジュールを作成した後にその期間 (once/repetitively/until 設定) を変更することはできません。スケジュールの期間を変更するには、削除してからスケジュールを作成しなおします。

8. [Finish] をクリックして、スケジュールを保存します。
9. [OK] をクリックします。

スケジュールの表示または削除

スケジュールの詳細を表示するか、データ収集ジョブからスケジュールを削除します。

1. [Perspective Resources] ビューからジョブに関連付けられたリソースを選択し、[Resource] > [Properties]を選択します。
2. [Collection Jobs] を選択します。
3. 収集ジョブのスケジュールを表示するには、ジョブ名の左にある矢印をクリックしてジョブを展開します。
ジョブ名の横に矢印がない場合、そのジョブにはスケジュールがありません。
4. スケジュールを選択します。
[Schedule] タブに名前、説明、開始/終了日付、繰り返し間隔が表示されます。
5. (オプション) 選択したスケジュールを削除するには、[Delete] をクリックします。
6. [OK] をクリックします。

参照：

- 統計収集のセットアップ (114 ページ)

ジョブのデータ収集間隔の変更

管理対象リソースの [Properties] ビューを使用して、データ収集スケジュールを変更します。

1. [Perspective Resources] ビューで、サーバ(またはその他のリソース)を選択します。
2. ビューのメニューバーで、[Resource] > [Properties]を選択します。
3. [Collection Jobs] を選択します。
4. ジョブフォルダを展開し、スケジュールを選択します。
5. [Schedule] タブで、[Repeat interval] フィールドを変更します。
6. [Apply] をクリックします。

スケジューラのレジュームとサスペンド

すべてのスケジュールされたジョブをレジュームまたはサスペンドするには、スケジューラ設定を使用します。

前提条件

このタスクを実行するには、管理権限 (sccAdminRole) が必要です。

手順

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [SAP Control Center Properties] ダイアログで、[Scheduler] を選択します。
3. 次のいずれかを実行します。
 - スケジューラをレジュームするには、[Resume] をクリックします。
 - スケジューラをサスペンドするには、[Suspend] をクリックします。
4. [OK] をクリックします。

ジョブ実行履歴の表示

データ収集ジョブの実行履歴を表示するには、[Properties] ビューを使用します。

1. [Perspective Resources] ビューで、ジョブに関連付けられているリソースを選択し、[Resource] > [Properties] を選択します。
2. [Collection Jobs] を選択します。
3. ジョブを選択します。
4. [History] タブをクリックします。

リソース

SAP Control Center では、リソースは、SCC によるモニタリングと管理がサポートされる、一意の製品コンポーネントまたはサブコンポーネントです。サーバは、もっとも一般的な管理対象リソースです。

SCC で管理できるリソースには、サーバ、エージェント、データベース、デバイス、プロセスが含まれます。管理対象リソースは、SCC でモニタおよび管理できる製品コンポーネントまたはサブコンポーネントです。リソース管理の2つの重要なツールは、Resource Explorer と [Perspective Resources] ビューです。

- Resource Explorer には、SCC に登録されているリソースがリストに示されます。このリストには、まだ観点に追加していないリソースが含まれていることがあります。登録することで、SCC でリソースへの接続、ログイン、モニタリングデータの取得、およびコマンドの発行が可能になります。リソースはサーバレベルまたはエージェントレベルで登録されます。また、サーバまたはエージェントを登録することで、データベースやプロセスなど、SCC で管理可能なサブコンポーネントが認識されます。リソースは、個別に登録できます。また、一括でインポートすることによって一度に複数登録することもできます。
- [Perspective Resources] ビューには、現在のパースペクティブに追加した登録済みのリソースが表示されます。リソースの可用性とパフォーマンスを管理またはモニタするには、リソースをパースペクティブに追加する必要があります。

参照：

- Data Assurance サーバの登録 (110 ページ)
- 一括登録のためのリソースのインポート (111 ページ)

リソースの登録解除

1つ以上のサーバまたは他のリソースを SAP Control Center から削除します。

1. SAP Control Center ツールバーで、[Launch Resource Explorer] アイコンをクリックします。
2. Resource Explorer で、登録を解除するリソースを選択します。複数のリソースを選択するには、[Shift] キーを押しながら、または [Ctrl] キーを押しながらクリックします。
3. [Resources] > [Unregister] を選択します。
4. [Yes] をクリックして削除を確定します。

参照：

- Data Assurance サーバの登録 (110 ページ)

- 一括登録のためのリソースのインポート (111 ページ)

パースペクティブへのリソースの追加

1つ以上のリソースを現在のパースペクティブに追加します。

前提条件

リソースを登録します。

手順

同じパースペクティブの他のリソースと一緒に監視および管理できるように、サーバまたはその他のリソースをパースペクティブに追加します。

1. SAP Control Center ツールバーで、[Launch Resource Explorer] アイコンをクリックします。
2. 観点に追加するリソースを選択します。複数のリソースを選択するには、[Shift クリック]または[Control クリック]を使用します。
3. 次のいずれかを実行します。
 - [Resources] > [Add Resources to Perspective] を選択します。
 - Resource Explorer から、[Perspective Resources] ビューにリソースをドラッグアンドドロップします。複数のリソースを選択できます。

参照：

- パースペクティブからのリソースの削除 (150 ページ)
- リソース (149 ページ)
- Data Assurance サーバの登録 (110 ページ)
- 一括登録のためのリソースのインポート (111 ページ)

パースペクティブからのリソースの削除

1つ以上のリソースを現在のパースペクティブから削除します。

パースペクティブからリソースを削除しても、リソースの登録は解除されません。追加された他のパースペクティブには残り、引き続き Resource Explorer からアクセスできます。

1. リソースを移動する前に、リソースが開いているビューで使用されていないことを確認してください。
 - リソースを表示しているビューをすべて閉じます。
 - 管理コンソールを閉じたくない場合は、次の手順でリソースの選択を解除します。
 - a) 管理コンソールの左ウィンドウ枠で [Resource Selection] をクリックします。

- b) リストのリソースを探し、ボックスをクリックして選択を解除します。
2. [Perspective Resources] ビューが開いていない場合は、パースペクティブツールバーの[Show/Hide Perspective Resources View] アイコンをクリックします。
3. [Perspective Resources] ビューで、削除するリソースを選択します。複数のリソースを選択するには、[Shift クリック]または[Control クリック]を使用します。
4. [Resource] > [Remove]を選択します。
5. [Yes] をクリックして削除を確定します。

参照：

- パースペクティブへのリソースの追加 (150 ページ)

リソースの名前と接続プロパティの変更

SAP Control Center に登録したリソースのプロパティを変更します。

1. [Perspective Resources] ビューで、リソースを選択して、[Resource] > [Properties] を選択します。
2. (オプション) [General Properties] ページで、リソースの名前または説明を変更します。
大文字と小文字を使用して管理対象サーバの実際の名前を入力する。SAP Control Center に登録された名前が、サーバ名と完全一致しないと、トポロジビューなどの一部のモニタ機能が機能しない。
3. (オプション) [Connection Information] ページで、次の変更を行います。
 - ホスト名
 - ポート番号
 - 管理対象リソースのその他のオプション
4. [OK] をクリック (変更内容を適用して、プロパティダイアログを閉じる) するか、[Apply] をクリック (変更内容を適用して、ダイアログは閉じない) します。

Resource Explorer でのリソースの検索

すべての管理対象リソースを検索するか、特定のリソースに検索を絞り込みます。

1. [Launch Resource Explorer] アイコンをクリックします。
2. [Filter] ペインが [Resource Explorer] ウィンドウに表示されない場合、ビューのメニューバーから [View] > [Filter] を選択します。
3. [Filter string] フィールドに検索単語を入力します。

検索単語には、サーバまたはリソースのタイプの名前または名前の一部など、Resource Explorer の表部分に表示される任意の文字列を入力できます。たとえば、「ASE Server」と入力できます。

4. (オプション) フィルタリング設定として以下のいずれかを選択します。
 - [Match case]- 表示データに、大文字小文字の違いも考慮して、検索単語があるリソースを検索します。または、
 - [Exact match] - 表示データに検索単語と同一の項目があるリソースを検索します。
5. (オプション) [Filter on] リストからカラムを選択し、検索対象をそのカラムに限定します。

パースペクティブ

パースペクティブは、1つ以上の管理対象リソースのセット用のコンテナの名前です。パースペクティブをカスタマイズして、環境に必要な情報を提供できます。

観点は SAP Control Center ウィンドウの主な作業領域であり、管理対象リソースを整理できます。リソースの場所 (大陸、州、タイムゾーンなど)、用途、リソースを所有するグループ、管理者に基づいて、リソースを観点に割り当てることができます。観点は、メインウィンドウにタブとして表示されます。

パースペクティブごとに、[Perspective Resources] ビューがあります。このビューには、パースペクティブ内のリソースが一覧表示され、高レベルのステータスと説明的な情報が表示されます。詳細ビューから切り替えてアイコンビューに戻すには、[View] メニューを使用します。

必要に応じて、ヒートチャート、統計チャート、Alert Monitor などの別のビューを開き、観点のリソースを管理することもできます。観点のビューには、観点内のリソースに関する情報のみが表されます。

1つのリソースが複数のパースペクティブに表示されることもあります。

パースペクティブの作成

リソースを追加して管理できるパースペクティブを作成します。

1. アプリケーションのメニューバーから、[Perspective] > [Create] を選択します。
2. パースペクティブの名前を入力します。名前は 255 文字まで入力できます。
3. [OK] をクリックします。

パースペクティブの削除

パースペクティブウィンドウを削除します。

1. 削除するパースペクティブを選択します。

2. メインメニューバーから、[Perspective] > [Delete] を選択します。
選択した観点が削除されます。他の観点がある場合は、SAP Control Center に表示されます。

パースペクティブの名前変更

パースペクティブの名前を変更します。

1. 名前を変更するパースペクティブを選択します。
2. メインメニューバーから、[Perspective] > [Rename] を選択します。
3. パースペクティブの名前を入力します。
4. [OK] をクリックします。

ビュー

パースペクティブ内の1つ以上のリソースを管理するには、ビューを使用します。

SAP Control Center では、ビューは観点のリソースを監視して管理するために使用するウィンドウです。観点内のビューを再配置、並べて表示、カスケード表示、最小化、最大化し、全体的に表示を制御できます。

パースペクティブごとに次のビューがあります。

- Perspective Resources
- Administration Console
- Heat chart
- Alert Monitor
- Component log viewer
- 管理対象リソースのビュー。リソースタイプによって異なりますが、通常は統計チャート、プロパティビュー、モニタリングビューがあります。

注意： SAP Control Center ビューは、データベースビューには関連付けられていません。両者の目的は完全に異なります。

ビューの管理

現在のパースペクティブでビューを開き、閉じ、最小化し、最大化し、または元のサイズに戻します。




次の操作を実行できます。




タスク	操作
ビューを開く	次のいずれかを実行する。 <ul style="list-style-type: none"> • [Perspective Resources] ビューで、リソースを選択し、リソース名の右側のドロップダウン矢印をクリックし、ビューを選択して開く。 • アプリケーションのメニューバーで、[View] > [Open] を選択してビューを選択する。
ビューを閉じる	閉じるビューを選択する。アプリケーションのメニューバーで、[View] > [Close] を選択する。ビューの右上の [X] をクリックすることもできる。
ビューを最大化する	ビューの右上隅にあるボックスをクリックします。ビューがパースペクティブウィンドウ全体に拡大されます。このボックスを再度クリックすると、ビューが元のサイズに戻ります。
ビューを最小化する	ビューの右上隅にある [] をクリックする。ビューはパースペクティブウィンドウの下部の小さなタブに縮小される。
すべてのビューを最小化する	アプリケーションのメニューバーで、[View] > [Minimize All Views] を選択する。
ビューを元のサイズに戻す	ビューを最大化するには、最小化されたタブのボックスをクリックします。このボックスを再度クリックすると、ビューが元の (小さい方の) サイズに戻り、他のビューを同時に表示できます。
ビューを前面に移動	アプリケーションのメニューバーで、[View] > [Select] を選択して、サブメニューから必要なビューを選択する。

パースペクティブでのビューレイアウトの並べ替え

ビューレイアウトオプションを使用して、パースペクティブ領域を管理します。

SAP Control Center ツールバーの次のいずれかのアイコンをクリックします。

アイコン	アクション
	[Close All Open Views]
	[Minimize All Open Views]
	[Restore All Minimized Views]

アイコン	アクション
	[Cascade All Open Views]
	[Tile All Open Views Vertically]
	[Tile All Open Views Horizontally]

[Cascade all open views] では、ビューが重なります。[Tile all open views vertically] または [Tile all open views horizontally] では、ビューは重なりません。

また、SAP Control Center メニューバーからもビューのレイアウトを整理できます。メニューバーから、[Perspective]>[Arrange] を選択し、ビューレイアウトを選択します。

レポジトリ

SAP Control Center の埋め込みレポジトリには、管理対象リソースに関連する情報に加え、ユーザ設定データ、運用データ、統計情報が保存されます。

必要に応じてレポジトリデータベースをバックアップし、自動バックアップをスケジュールリングし、レポジトリをバックアップからリストアし、レポジトリの消去オプションを設定できます。フルバックアップとインクリメンタルバックアップを使用できます。フルバックアップは、レポジトリ全体をコピーします。インクリメンタルバックアップは、トランザクションログをコピーし、最後のフルバックアップまたはインクリメンタルバックアップ以降のすべての変更を取得します。

SAP Control Center では、デフォルトでバックアップが次のように保存されます。

- 各フルバックアップは、 の各サブディレクトリに保存されます。
- 各インクリメンタルバックアップは、 /backup/incremental のファイルに保存されます。

SAP では、インストールディレクトリが大きくなり過ぎないように、バックアップファイルを定期的にセカンダリ記憶ロケーションに移動することをおすすめします。

レポジトリのバックアップのスケジュールリング

レポジトリのフルバックアップおよびインクリメンタルバックアップが自動的に行われるように設定します。

前提条件

フルバックアップとインクリメンタルバックアップをいつ実行するかなど、バックアップの方針を決定します。たとえば、インクリメンタルバックアップを毎日

実行し、フルバックアップを毎週日曜日に実行するようにスケジュール設定します。

このタスクを実行するには、管理者権限 (sccAdminRole) を持っている必要があります。

手順

フルバックアップは、レポジトリ全体をコピーします。インクリメンタルバックアップは、トランザクションログをコピーし、最後のフルバックアップまたはインクリメンタルバックアップ以降のすべての変更を取得します。

1. メインメニューから、[Application] > [Administration] を選択します。
2. 左ウィンドウ枠で [Repository] を選択します。
3. [Full Backup] タブをクリックします。
4. (オプション) バックアップを保存するディレクトリを変更するには、[Browse] をクリックして目的のディレクトリに移動します。
5. [Schedule a Regular Backup] を選択します。
6. スケジュールしたバックアップを開始する日を指定します。[Start date] を入力するか、カレンダーをクリックして日付を選択します。
7. (オプション) [Time] および [AM/PM] コントロールを使用して、バックアップを実行する時刻を指定します。
8. [Repeat interval] を設定して、時刻、日、週を選択して、バックアップの頻度を指定します。
9. (オプション) バックアップのたびにレポジトリを消去するには、[Run a repository purge after the backup completes] を選択します。
10. バックアップスケジュールに消去を加える場合は、[Size Management] タブに移動し、[Automatically purge the repository periodically] を選択解除して自動消去を無効にします。
11. [Apply] をクリックして、スケジュールを保存します。
12. [Incremental Backup] タブをクリックして、上記の手順を繰り返して、インクリメンタルバックアップをスケジュールリングし、フルバックアップの間に実行します。

次のステップ

[Size Management] タブで消去オプションを設定します。

バックアップスケジュールの変更

レポジトリバックアップを中断または再開したり、バックアップスケジュールを変更します。

前提条件

このタスクを実行するには、管理者権限 (sccAdminRole) を持っている必要があります。

手順

1. メインメニューから、[Application] > [Administration] を選択します。
2. 左ウィンドウ枠で [Repository] を選択します。
3. 次のようにして、変更するバックアップのタイプを選択します。
 - [Full Backup] タブをクリックします。または
 - [Incremental Backup] タブをクリックします。
4. (オプション) バックアップスケジュールを中断または再開するには、[Schedule a Regular Backup] を選択または選択解除します。
このオプションを選択解除 (チェックを解除) すると、スケジューリングされた領域が灰色表示され、スケジューリングされたバックアップは実行されません。ただし、スケジュールは引き続き保存され、いつでも復活できます。
5. バックアップスケジュールを変更するには、[Start date]、[Time]、[Repeat interval] または単位を編集します。また、[Run a repository purge after the backup completes] を選択または選択解除することもできます。
6. [Apply] をクリックして、スケジュールを保存します。

即時バックアップの強制実行

スケジューリングされていないレポジトリのフルバックアップまたはインクリメンタルバックアップを実行します。

前提条件

このタスクを実行するには、管理者権限 (sccAdminRole) を持っている必要があります。

手順

1. メインメニューから、[Application] > [Administration] を選択します。
2. 左ウィンドウ枠で [Repository] を選択します。
3. 次のようにして、実行するバックアップのタイプを選択します。

- [Full Backup] タブをクリックします。または
 - [Incremental Backup] タブをクリックします。
4. [Back up Now] をクリックします。

バックアップは、[Location] フィールドに表示されているディレクトリに保存されます。

レポジトリのバックアップからのリストア

不要な変更を元に戻すか、重大な障害からリカバリするには、バックアップファイルをレポジトリデータベースにロードします。

バックアップをデフォルトのロケーション以外に格納するように SAP Control Center を設定している場合、この手順の copy コマンドのソースディレクトリを変更します。

1. SAP Control Center を停止します。
2. 最新のフルバックアップを /backup/<generated_directory_name> から /services/Repository にコピーします。次に例を示します。

Windows の場合：

```
copy C:\$sap\ SCC-3_3\backup\repository.  
270110161105\scs_repository.db  
C:\$sap\ SCC-3_3\services\Repository
```

UNIX の場合：

```
cp /opt/sap/ SCC-3_3/backup/repository.270110161105/  
scs_repository.db  
/opt/sap/ SCC-3_3/services/Repository
```

3. ロードするインクリメンタルバックアップがない場合、次の手順を実行します。
 - a) また、ログファイルを /backup/<generated_directory_name> から /services/Repository にコピーします。次に例を示します。

Windows の場合：

```
copy C:\$sap\ SCC-3_3\backup\repository.  
270110161105\scs_repository.log  
C:\$sap\ SCC-3_3\services\Repository
```

UNIX の場合：

```
cp /opt/sap/ SCC-3_3/backup/repository.270110161105/  
scs_repository.log  
/opt/sap/ SCC-3_3/services/Repository
```

- b) 手順 5 (159 ページ) にスキップします。

4. (オプション) インクリメンタルバックアップをロードするには、**-ad** オプションを使用してリポジトリデータベースを起動します。これにより、トランザクションログ (インクリメンタルバック) が `incremental` ディレクトリからロードされます (データベースは、フルバックアップを自動的にロードします)。次に例を示します。

Windows の場合：

```
cd sap¥ SCC-3_3¥services¥Repository
..¥..¥bin¥sa¥bin_<platform>¥dbsrv11.exe scc_repository -ad
sap¥ SCC-3_3¥backup¥incremental
```

UNIX の場合：

```
cd /opt/sap/ SCC-3_3/services/Repository
../../../../bin/sa/bin_<platform>/dbsrv11 scc_repository -ad
/opt/sap/ SCC-3_3/backup/incremental
```

レポジトリデータベースは、`incremental` ディレクトリにあるフルバックアップとインクリメンタルバックアップをロードします。インクリメンタルバックアップは日付が古い順にロードされます。ロードして保存した後に、データベースは停止します。

5. SAP Control Center を起動します。
インクリメンタルバックアップをロードすると、SAP Control Center は通常どおり起動します (リカバリは発生しません)。フルバックアップを Repository ディレクトリにコピーすると、データベースはフルバックアップからリポジトリをリカバリします。

例：インクリメンタルバックアップをレポジトリデータベースにロード

次のコマンドは、32 ビットの Windows マシンで SQL Anywhere を起動します。

```
% cd C:¥sap¥ SCC-3_3¥services¥Repository
% ..¥..¥bin¥sa¥bin_windows32¥dbsrv11.exe scc_repository -ad
C:¥sap¥ SCC-3_3¥backup¥incremental
```

次のコマンドは、Solaris を実行中の 64 ビットのマシンで SQL Anywhere® を起動します。

```
$ cd /opt/sap/ SCC-3_3/services/Repository
$ ../../bin/sa/bin_sunsparc64/dbsrv11 scc_repository -ad
/opt/sap/ SCC-3_3/backup/incremental
```

リポジトリ消去の設定

リポジトリ消去オプションを変更します。

前提条件

このタスクを実行するには、管理者権限 (sccAdminRole) を持っている必要があります。

手順

リポジトリをどのように消去するかを決定するには、次のことを考慮します。

- 消去すると、リポジトリが非常に大きなディスク領域を占めることを防ぐことができます。
- デフォルトでは、消去は有効です。1日1回行われ、1日よりも古いデータが消去されます。
- 統計とアラート履歴は、サーバパフォーマンスとユーザの動作の傾向を突き止めるために役立ちます。SAP Control Center の統計チャートでは、データがあれば、1年以上前の期間のパフォーマンスデータをグラフで表示できます。ディスク領域が十分にある場合は、長い期間のデータを保存したり、統計またはアラートの履歴の削除を無効にすることを検討します。
- 消去の頻度やその他のオプションを変更すると、SAP Control Center のパフォーマンスに影響を与える場合があります。

注意：スケジューリングされたポジトリのバックアップの一部で消去を設定する場合は、[Size Management] タブで自動消去を無効にします。

1. メインメニューバーから、[Application] > [Administration] を選択します。
2. [Repository] を選択します。
3. [Size Management] タブをクリックします。
4. 自動消去をオンまたはオフにするには、[Automatically purge the repository periodically] をクリックします。
スケジューリングされたフルバックアップまたはインクリメンタルバックアップの一部で消去を設定する場合は、このオプションをオフにします。
5. 次の消去オプションをクリックしてオンまたはオフにします。
 - [Purge statistics]
 - [Purge alert history]
6. [Purge data older than] に、リポジトリデータを消去するまでの日数を入力します。
7. [適用] をクリックし、次に [OK] をクリックします。

ロギング

ロギングは、ログファイルのイベントに関するメッセージを記録することで、SAP Control Center 管理者がエラーやその他のシステムイベントを特定して追跡するために役立ちます。

SAP Control Center では、次のログが管理されます。

- クライアントログ - ブラウザベースのクライアントコンポーネントでのアクティビティに関するメッセージを取得します。これらのメッセージは、コンポーネント製品モジュールによって生成され、ユーザに関連する情報で、ポップアップを表示するほど重大ではない情報を示します。クライアントログは、クライアントブラウザの操作を追跡するためにも使用されます。
- サーバログ - サービスの起動などの初期化手順中のアクティビティに関するメッセージ、ログインおよびログアウトを記録する監査メッセージ、スケジューリングされたイベントの失敗などのエラー、サーバ上のその他のイベントを取得します。サーバログには、次のものがあります。
 - コンポーネントログ。個々の製品モジュールに関するイベントのみを記録します。
 - SCC エージェントログ。複合ログです。SCC サーバでは、エージェントログはすべての製品モジュールおよび SAP Control Center フレームワーク内のイベントを記録します。SCC エージェントでは、エージェントログは、エージェント内のイベントを記録します。
- リポジトリログ - SAP Control Center リポジトリの SQL Anywhere データベースで発生した、挿入や更新に関する情報を取得します。このログは SCC-3_3¥log¥repository.log に置かれます。
- アラートサービスログ - アラートでトリガされたスクリプトの実行 (起動時間、終了時間、ステータス、終了コード) など、アラートサービスステータスとイベントに関する情報を取得します。このログは、SCC-3_3¥log¥alert-server.log に置かれます。

Data Assurance コンポーネントログの表示

SAP Control Center for Data Assurance のイベントログを表示します。

ログファイルは以下の場所にあります。

- Windows の場合 - %SYBASE%¥SCC-3_3¥plugins¥DAMAP¥log¥damap.log
 - UNIX の場合 - \$SYBASE/SCC-3_3/plugins/DAMAP/log/damap.log
1. ログビューアまたはテキストエディタを使用してログファイルを表示します。
 2. ログイン試行回数、サービスの起動の失敗など、対象のエントリを探します。

Data Assurance ログ設定の編集

Data Assurance (DA) のログレベルまたはロギング設定を変更します。

1. %SYBASE%\\$SCC-3_2¥plugins¥DAMAP に移動します。
2. logging.properties ファイルを開いて、必要に応じて設定を変更します。
3. logging.properties ファイルを保存して閉じます。
4. SCC サーバを再起動します。

SCC for Data Assurance のメッセージは、コンソールと damap.log ファイルに記録されます。damap.log ファイルは %SYBASE%\\$SCC-3_2¥plugins¥DAMAP¥log にあります。

SAP Control Center サーバログの表示

SAP Control Center サーバのイベントログを表示します。

SAP Control Center イベントログは、次の場所に格納されます。

- SAP Control Center が起動するコンソール。
 - SAP Control Center エージェントログ: <SCC-install-directory>/log/agent.log
 - リポジトリログ: <SCC-install-directory>/log/repository.log
 - インストールされている各 SAP Control Center 製品モジュールのコンポーネントログ。コンポーネントログのパスは、次のような形式になります。 <SCC-install-directory>/plugins/<component>/log/<component>.log
1. ログビューアまたは選択した方法を使用してログファイルのいずれかを表示します。
 2. ログイン試行回数やサービス起動失敗など、該当するエントリを検索します。
コンソールおよび SAP Control Center エージェントログファイルでは、一部のコンポーネントで、コンポーネント名がログエントリの前に追加されます。

SAP Control Center クライアントログの表示

SAP Control Center ブラウザクライアントの現在のセッションのイベントログを表示します。

観点タブウィンドウ(メインウィンドウ)で、クライアントログを表示するには以下のいずれかを実行します。

- [Ctrl+Alt+L] キーを押します。
- [View] > [Open] > [Log Window] を選択します。

注意： クライアントログリーダーには、現在のログインセッションに対する最新の 100 個のログメッセージが表示されます。

ロギングレベルの変更

SAP Control Center によってサーバログに記録されるイベントを決定するロギングレベルを調整します。このタスクでは、SAP Control Center の再起動が必要です。

SAP Control Center で問題が発生している場合、さらに多くのイベントが記録されるようにサーバのロギングレベルを変更することによって、問題の原因を発見できる可能性があります。

1. SAP Control Center を停止します。
2. ロギングレベルを変更する `-m` オプションを使用して SAP Control Center を再起動します。 <SCC-installation-dir>/bin で、次のように入力します。

```
scc -m <logging-level>
```

ロギングレベルは、OFF (何もログ記録しません)、FATAL (最も重大なイベントのみをログ記録します)、ERROR、WARN、INFO、DEBUG、ALL (すべてをログ記録します) です。

3. サーバログを調べて、問題を発生させる可能性のある手がかりを探します。
4. 問題を解決したら、ロギングレベルをデフォルトの WARN に設定します。ロギングレベルを DEBUG または ALL のレベルのままにすると、ログが制御できないほど大きくなる場合があります。

例

以下のコマンドは、インストールディレクトリで実行する必要があります。実行すると、ロギングレベルが debug に設定されて SAP Control Center が起動します。

```
Windows: bin\scc -m DEBUG  
UNIX: bin/scc -m DEBUG
```

参照：

- Windows での SAP Control Center の起動と停止 (60 ページ)
- UNIX での SAP Control Center の起動と停止 (64 ページ)

ロギングレベルまたはメッセージレベル

SAP Control Center によってログ記録されるイベントのタイプを制御するために使用できる値について説明します。

次の表は、ロギングレベルをレベルの高い方から低い方の順にリストしています。レベルが高いほど、重要度の高いイベントがログ記録されます。レベルを設定すると、それより上のレベルのすべてのイベントがログ記録されます。たとえば、

ロギングレベルを WARN に設定すると、WARN、ERROR、FATAL のレベルのイベントがログ記録されます。

OFF	何もログ記録されません。これが最も高いレベルです。
FATAL	サーバのアボートを発生させるような非常に重大なエラーイベントのみがログ記録されます。これは、イベントがログ記録される最も高いレベルです。
ERROR	サーバが動作を継続できるエラーイベントがログ記録されます。
WARN	潜在的に問題のある状況がログ記録されます。WARN が、通常の運用時 (つまり、システム初期化後) のデフォルトのロギングレベルです。
INFO	サーバ処理の進捗を大まかに追跡する情報メッセージがログ記録されます。システム初期化プロセス時には、INFO がデフォルトのロギングレベルです。
DEBUG	サーバがどのように動作しているかを細かく示す大量のイベントがログ記録されます。このレベルは、トラブルシューティング時に設定することをおすすめします。
ALL	ログ可能なすべてのイベントがログ記録されます。これが最も低いレベルです。

参照：

- scc コマンド (72 ページ)

ロギング設定の変更

SAP Control Center ロギングを変更するには、ロギング設定ファイル `log4j.properties` を編集します。

ログファイルの名前、ロケーション、最大サイズ、バックアップされるログファイルの数を変更できます。

コマンドのオプションを使用することによって、**scc** の起動時に SAP Control Center ログメッセージの全体的なレベルを変更できますが、DEBUG レベルを選択すると、大量のログメッセージが生成されて支障が起きることがあります。ログプロパティファイルを編集すると、SCC の各コンポーネントのロギングレベルを個別に設定できるなど、より細かく制御できます。このような変更は、log4j に精通しており、SAP のテクニカルサポートと一緒に作業する場合のみ行うことをおすすめします。DEBUG レベルのログメッセージは、一般的な運用では必要ありません (log4j を以前に使用したことがない場合は、まず、<http://logging.apache.org/log4j/1.2/manual.html> を参照してください)。

1. SCC を停止します。

2. <SCC-installation-directory>/conf にある log4j.properties ファイルのバックアップコピーを作成します。
3. 編集するために log4j.properties ファイルを開きます。
4. ニーズを満たすように、ファイルの値を変更します。次に例を示します。

目的	変更
ログファイルの名前またはロケーションを変更します。	<ul style="list-style-type: none"> • エージェントログ - log4j.appender.agent.File • レポジトリログ - log4j.appender.repository.File • 収集統計ログ - log4j.appender.collection-stats.File • アラートサーバログ - log4j.appender.alert.File • ゲートウェイログ - log4j.appender.gateway.File
1つのログファイルの最大サイズを変更する。このサイズに到達すると、SCC によって新しいファイルが作成される。	<ul style="list-style-type: none"> • エージェントログ - log4j.appender.agent.MaxFileSize • レポジトリログ - log4j.appender.repository.MaxFileSize • 収集統計ログ - log4j.appender.collection-stats.MaxFileSize • アラートサーバログ - log4j.appender.alert.MaxFileSize • ゲートウェイログ - log4j.appender.gateway.MaxFileSize
SCC がバックアップするログファイルの数を変更する。この数を超えると、最も古いファイルが削除される。	<ul style="list-style-type: none"> • エージェントログ - log4j.appender.agent.MaxBackupIndex • レポジトリログ - log4j.appender.repository.MaxBackupIndex • 収集統計ログ - log4j.appender.collection-stats.MaxBackupIndex • アラートサーバログ - log4j.appender.alert.MaxBackupIndex • ゲートウェイログ - log4j.appender.gateway.MaxBackupIndex

5. ファイルを保存して終了します。
6. SCC を起動して、ロギングの変更を有効にします。

参照：

- Windows での SAP Control Center の起動と停止 (60 ページ)
- UNIX での SAP Control Center の起動と停止 (64 ページ)

SAP Control Center コンソール

コンソールは、SAP Control Center サーバとそのサブシステムのステータスに関する詳細を表示するためのコマンドラインインタフェースです。

scc コマンドを使用して SAP Control Center を起動する場合は、起動メッセージが表示され、コンソールプロンプトが表示されます。

注意： SAP Control Center をサービスとして起動したり、**scc** の出力をファイルに送信したり、SAP Control Center をバックグラウンドで起動すると、コンソールプロンプトは表示されません。

参照：

- SAP Control Center の起動 (59 ページ)

コンソールコマンド

SAP Control Center コンソールを使用して、SAP Control Center のステータス情報とポート、プラグイン、サービスを取得します。

help コマンド

1つまたは複数の SAP Control Center コンソールコマンドの構文情報を表示します。

構文

```
help [command_name]
```

パラメータ

- **command_name** – オプション。status、info、または shutdown。 *command_name* を省略すると、**help** はすべてのコンソールコマンドの情報を返します。

例

- **例 1** – **status** コマンドの情報を返します。

```
help status
```

パーミッション

help パーミッションは、すべてのユーザに対してデフォルトで設定されています。これを使用するためのパーミッションは必要ありません。

info コマンド

SAP Control Center サーバの指定された部分の情報を表示します。

パラメータなしで **info** を入力すると、各パラメータの情報が返されます。

構文

```
info [-a | --sys]
[-D | --sysprop [system-property]]
[-e | --env [environment-variable]]
[-h | --help]
[-m | --mem]
[-p | --ports]
[-s | --services]
```

パラメータ

- **-a | --sys** – オプション。SAP Control Center が認識するすべてのサービスを一覧表示します。各サービスが有効であるかどうかを示し、各サービスが依存する他のサービスを一覧表示します。
- **-D | --sysprop [system-property]** – オプション。指定された Java システムプロパティに関する情報を表示します。すべての Java システムプロパティのリストとその値を返すには、system-property 引数を省略します。
- **-e | --env [environment-variable]** – オプション。SAP Control Center Java VM プロセス環境のすべての環境変数を一覧表示します。環境変数のリストとその値を返すには、environment-variable 引数を省略します。
- **-h | --help** – オプション。**info** コマンドに関する情報を表示します。
- **-m | --mem** – オプション。サーバのメモリリソースに関する情報を表示します。
- **-p | --ports** – オプション。SAP Control Center エージェントとサービスが受信するすべてのポートを一覧表示します。各ポートが使用されているかどうかを示し、各ポートで実行中のサービスを表示します。
- **-s | --services** – オプション。すべての SAP Control Center サービスを一覧表示します。各サービスが有効であるかどうかを示し、各サービスが依存するほかのサービスを一覧表示します。

例

- **例 1** – この SAP Control Center サーバ上のポートに関する情報を表示します。

```
info -p
```

パーミッション

info パーミッションは、すべてのユーザに対してデフォルトで設定されています。これを使用するためのパーミッションは必要ありません。

shutdown コマンド

SAP Control Center が起動している場合は停止します。

構文

```
shutdown
```

例

- **例 1** – SAP Control Center を停止します。

```
shutdown
```

パーミッション

shutdown パーミッションは、すべてのユーザに対してデフォルトで設定されています。これを使用するためのパーミッションは必要ありません。

status コマンド

SAP Control Center エージェント、プラグイン、SAP Control Center のサービスコンポーネントのステータスを表示します。

構文

```
status [-a | --agent]
[-h | --help]
[-p | --plugin [plugin-name]]
[-s | --service [service-name]]
```

パラメータ

- **-a | --agent** – SAP Control Center エージェントコンポーネントのステータスを表示します。
- **-h | --help** – **info** コマンドに関する情報を表示します。
- **-p | --plugin [*plugin-name*]** – 指定された SAP Control Center プラグイン (ASEMap、Adaptive Server® 管理モジュールなど) のステータスを表示します。プラグインのリストを返すには、*plugin-name* 引数を省略します。
- **-s | --service [*service-name*]** – 指定された SAP Control Center サービス (アラートサービスやメッセージングサービスなど) のステータスを表示します。サービスのリストを返すには、*service-name* 引数を省略します。

例

- **例 1** – レポジトリサービスのステータス情報を表示します。

```
status --service Repository
```

パーミッション

status パーミッションは、すべてのユーザに対してデフォルトで設定されています。これを使用するためのパーミッションは必要ありません。

Data Assurance 環境の管理とモニタ

Data Assurance サーバおよびエージェントの管理とモニタを行います。

Data Assurance エージェント

Data Assurance (DA) エージェントは、データをデータベースからフェッチし、DA サーバに圧縮します。

エージェントには、2つのタイプがあります。DA サーバ組み込みのローカルエージェントと、DA サーバが使用してジョブのパフォーマンスを向上させることができるスタンドアロン (リモート) エージェントです。

DA エージェントは、1つ以上のデータベースへの Java Database Connectivity (JDBC) コネクションを開き、比較のために使用するローデータを読み込みます。スタンドアロン DA エージェントがない場合、組み込み済みのローカルエージェントを使用する必要があります。

DA サーバの要求に基づいて、DA エージェントは次の処理を実行します。

- 設定に応じて事前比較用にローを圧縮する
- 比較用にローをフェッチする
- 設定に応じて事前比較用にローをハッシュ処理する
- 設定に応じて事前比較用にローをソートする
- 設定に応じてデータベースで **insert/delete/update** ステートメントを実行する

エージェント接続の編集

Data Assurance (DA) エージェント接続プロファイルの詳細を変更します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Agent Connections] を選択します。
4. DA エージェント接続を選択します。
5. 次のいずれかを行います。
 - [Resource] > [Properties] を選択します。
 - DA エージェント接続を選択した際に表示されるボタンをクリックし、[Properties] を選択します。
6. 必要に応じてエージェント接続情報を変更し、[Apply] をクリックします。

フィールド	説明
Host	(必須) DA エージェントがインストールされているサーバの名前。
Port	(必須) DA エージェントのポート番号。

フィールド	説明
Username	(必須) DA エージェントのユーザ名。
Password	(必須) DA エージェントのパスワード。
Description	エージェント接続の識別に役立つ簡単な説明。

7. (オプション) [Test] をクリックして、変更したエージェント接続情報が正しいことを確認します。
8. [OK] をクリックします。

参照：

- エージェント接続の作成 (117 ページ)

エージェント接続の削除

Data Assurance (DA) エージェント接続プロファイルを削除します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Agent Connections] を選択します。
4. DA エージェント接続を選択します。
5. 次のいずれかを行います。
 - [Resource] > [Delete] を選択します。
 - DA エージェント接続を選択した際に表示されるボタンをクリックし、[Delete] を選択します。
6. [OK] をクリックします。

参照：

- エージェント接続の作成 (117 ページ)

すべてのエージェント接続の表示

すべての Data Assurance (DA) エージェントの接続プロファイルを表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Agent Connections] を選択します。

参照：

- エージェント接続の作成 (117 ページ)

エージェント接続のテスト

Data Assurance (DA) エージェント接続が正しく設定されていることを検証します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Data Assurance Agent Connections] を選択します。
4. DA エージェント接続を選択します。
5. 次のいずれかを行います。
 - [Resource] > [Properties] を選択します。
 - DA エージェント接続を選択した際に表示されるボタンをクリックし、[Properties] を選択します。
6. [Test] をクリックします。

参照：

- エージェント接続の作成 (117 ページ)

データベース接続

SAP Control Center for Data Assurance では、プライマリデータベースと複製データベースのデータを比較するために、データベース接続の確立に必要な情報を含むデータベース接続プロファイルを作成する必要があります。

参照：

- データベース接続の作成 (118 ページ)
- interface ファイルからの単一接続またはクラスタ接続の作成 (120 ページ)

データベース接続の編集

Data Assurance (DA) サーバのデータベース接続の詳細を変更します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。
4. データベース接続を選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。

- データベース接続を選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. 必要に応じてデータベース接続情報を変更し、[Apply] をクリックします。

フィールド	説明
Description	データベース接続の識別に役立つ簡単な説明。
Agent	(必須) データベースへの接続に使用する DA エージェント。DA サーバのインストールで定義されるローカルエージェント、[Data Assurance Agent Connections] に定義されているリモートエージェント、またはまだ定義されていない新しいリモートエージェントのいずれかです。
Database	(必須) 接続先のデータベース名。
Host	(必須) データベースが置かれているサーバの名前。
Port	(必須) データベースのポート番号。
Username	(必須) データベースのユーザ名。
Password	データベースのパスワード。
Properties	JDBC 接続のプロパティ。

6. (オプション) [Test] をクリックして、変更したデータベース接続情報が正しいことを確認します。
7. [OK] をクリックします。

参照：

- データベース接続の作成 (118 ページ)
- interface ファイルからの単一接続またはクラスタ接続の作成 (120 ページ)

データベース接続の削除

Data Assurance (DA) サーバからデータベース接続を削除します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。
4. データベース接続を選択し、次のいずれかを実行します。
 - [Resource] > [Delete] を選択します。
 - データベース接続を選択した際に表示されるボタンをクリックし、[Delete] を選択します。
5. [OK] をクリックします。

参照：

- データベース接続の作成 (118 ページ)
- interface ファイルからの単一接続またはクラスタ接続の作成 (120 ページ)

すべてのデータベース接続プロファイルの表示

Data Assurance (DA) サーバ内にあるすべてのデータベース接続プロファイルを表示します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。

参照：

- データベース接続の作成 (118 ページ)
- interface ファイルからの単一接続またはクラスタ接続の作成 (120 ページ)

データベース接続のテスト

データベース接続が正しく設定されているかどうかを検証します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を展開し、[Database Connections] を選択します。
4. データベース接続を選択し、次のいずれかを実行します。
 - [Resource] > [Properties] を選択します。
 - データベース接続を選択した際に表示されるボタンをクリックし、[Properties] を選択します。
5. [Test] をクリックします。

参照：

- データベース接続の作成 (118 ページ)
- interface ファイルからの単一接続またはクラスタ接続の作成 (120 ページ)

Data Assurance サーバ

CPU、メモリ、キャッシュメモリの使用状況の統計を収集し、Data Assurance (DA) サーバとエージェントの可用性と状態を監視します。

トポロジと DA モニタを使用して、オブジェクトの可用性と状態を監視できます。トポロジは、DA システムオブジェクトをグラフィックで表現したもので、DA サーバ、エージェント、およびデータベースが含まれます。

モニタには、次のビューがあります。

- **Overview** – サーバ名、サーバのバージョン番号、最後にサーバがリフレッシュされた時間、サーバのステータス、チャートに表示されるメモリと CPU の利用状況などの高度な情報を表示します。このビューを使用して、DA サーバまたは DA エージェントを監視または停止できます。
- **Job Current Status** – ジョブをステータスとその他の関連情報とともに一覧表示し、比較を一覧表示します。どちらもテーブル形式で表示されます。このビューを使用して、アポートする既存のジョブを選択できます。
- **Settings** – 画面のリフレッシュ間隔の値を変更できます。

参照：

- 管理対象リソースのログインアカウントの認証 (113 ページ)

システムトポロジの表示

Data Assurance (DA) システムトポロジを使用して、DA サーバやエージェントの可用性をグラフィカルにモニタします。

前提条件

- モニタするサーバを [Perspective Resources] ビューに追加します。
- サーバを認証します。

手順

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Topology] を選択します。
トポロジビューが開き、選択した DA サーバおよび関連付けられたエージェントやデータベースが表示されます。
3. (オプション)[View Controls] タブおよび [Details] タブを使用すると、トポロジの表示にさらに役立ちます。

Data Assurance サーバおよびエージェントのステータスの表示

Data Assurance (DA) モニタには、サーバやエージェントに関する高レベルの情報が表示されます。

前提条件

- モニタするサーバを登録し、[Perspective Resources] ビューに追加します。
- サーバを認証します。

手順

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Monitor] を選択します。

注意： [Perspective Resources] ビュー、[Heat Chart] ビュー、[Resource Explorer] ビュー、およびトポロジビューにあるサーバアイコンのステータスバッジを使用してサーバステータスを表示することもできます。

Data Assurance サーバパラメータの設定

サーバのシステム設定を編集することにより、Data Assurance (DA) サーバのパフォーマンスを向上させます。

前提条件

- モニタするサーバを [Perspective Resources] ビューに追加します。
- サーバを認証します。

手順

1. [Perspective Resources] で DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。
3. [Data Assurance Server] を選択します。
4. DA サーバを選択し、次のいずれかを実行します。
 - [Resource] > [System Configuration] を選択します。
 - DA サーバを選択した際に表示されるボタンをクリックし、[System Configuration] をクリックします。
5. [Run Value] カラムで、サーバパラメータの現在の値を変更します。
6. (オプション) 適用されていない変更を取り消すには、[Restore to Default] をクリックします。
7. [Apply] をクリックします。

『Replication Server Data Assurance Option ユーザーズガイド』 > 「パフォーマンスとチューニング」を参照してください。

Data Assurance サーバのロギングレベルと監査レベルの設定

Data Assurance サーバのロギングレベルと監査トレースレベルを設定します。

1. [Perspective Resources] ビューで DA サーバを選択します。
2. [Resource] > [Administration Console] を選択します。

管理とモニタ

3. [Browse] タブで [Data Assurance Servers] を選択し、DA サーバを選択します。
4. DA サーバを選択した際に表示されるボタンをクリックし、[Logging Configuration...] を選択します。
5. 監査トレースレベルとロギングレベルを選択します。
6. [Apply] をクリックし、次に [OK] をクリックします。

SAP Control Center for Data Assurance のトラブルシューティング

SAP Control Center for Data Assurance で発生する問題のトラブルシューティングを行います。

比較で LOB カラムの差異を検出できない

問題: ジョブ比較の結果で、データベース内のハッシュカラムの比較の矛盾が記録されません。

解決法 1: LOB フェッチサイズを増やす

不整合は image のようなラージオブジェクト (LOB) カラムに存在する可能性があります。デフォルトでは、DA サーバは LOB カラムの最初の 1024 バイトのみを比較するので、LOB 値の一部は比較されません。

この問題を解決するには、**lob_fetch_size** の値を増やします。

解決法 2: LOB フェッチサイズを増やす

ソースおよびターゲットのカラム値で、同じ MD5/SHA/CRC32 ハッシュ値が生成される場合があります。

この問題を解決するには、[literal] オプションを使用して、ローを再度比較します。

参照:

- Data Assurance サーバパラメータの設定 (175 ページ)

外部ソート・オプションの設定

問題: 外部ソートを設定するように DA エージェントを設定しましたが、データベースが引き続きソート処理を実行しています。

テーブル内のローの数が **external_sort_activate_size** の値 (デフォルトで 1000 万) よりも少ないので、有効なソート・オプションがアクティブになりません。

解決法: **external_sort_activate_size** の値を減らし、ソースおよびターゲットのテーブル内のローの数よりも少なくします。

参照：

- Data Assurance サーバパラメータの設定 (175 ページ)

DA サーバメモリ不足エラー

問題:DA サーバでメモリ領域が不足し、パフォーマンスの問題が発生します。

解決法 1：比較の最大同時スレッド数を減らす

比較中に、DA サーバは、さまざまな速度で DA エージェントからロー・データを受信するため、サーバは常に各ソースとターゲットのローを何十または何百もバッファリングする可能性があります。個別のローが大きく (ユーザ・データベース・テーブルに依存)、比較の数が多い (ユーザが設定) と、このバッファにより、DA サーバでメモリ不足が発生します。

この問題を解決するには、**comparer_max_concurrent_threads** を現在よりも低い値に設定します。

解決法 2：LOB フェッチサイズを減らす

設定パラメータ **lob_fetch_size** が高い値に設定されている場合があります。

この問題を解決するには、**lob_fetch_size** を現在よりも低い値に設定します。

解決法 3：外部ソートの最大サイズを減らす

外部ソート・オプションは、大量のメモリを使用します。デフォルトでは、外部ソートは、メモリに何千ものローを保持します。通常、このことは問題になりませんが、各ローのサイズと、同じ Java 仮想マシン (JVM) 内で同時に発生するアクティビティによって問題が発生する可能性があります。たとえば、DA エージェントを使用して同時に 5 つの比較を行うと、必要なメモリは 5 倍に増えます。または "ローカル・エージェント" が使用されると、ソースおよびターゲットのエージェントと比較関数は同じ JVM メモリ割り当てを共有します。

この問題を解決するには、**external_sort_max_size** 設定パラメータの値を変更して、DA エージェントがメモリに保存するローの数を減らします。

解決法 4：DA サーバが使用できるメモリを増やす

グローバルな解決法:多くのメモリで起動するように DA サーバを設定すると、上記のメモリ不足の問題のすべての原因に対応できます。デフォルトでは、DA サーバを実行する JVM は 512 MB を使用します。DA サーバの **RUN_<instance>.bat** ファイルを編集して、値を増やします (プラットフォームと使用可能なシステム・メモリの量によって異なります)。

参照：

- Data Assurance サーバパラメータの設定 (175 ページ)

SAP Control Center の基本機能に関する問題

起動と停止、認証、アラート、スケジューリングなどの基本機能に関連する問題をトラブルシューティングします。

SAP Control Center が起動しない

問題: SAP Control Center サーバが起動しない。

解決法 1：ポートの競合

解決法: SCC が、このマシン上の他のサーバまたはアプリケーションに使用されているポートを使用している可能性があります。ポートの競合を確認するには、次の手順を実行します。

1. 次のコマンドを実行します。

```
scc --info ports
```

SAP Control Center とサービスが受信するすべてのポートを一覧表示します。各ポートが使用されているかどうかを示し、各ポートで実行中のサービスを表示します。SCC が実行中でない場合は、表示されているポートすべてが競合を示します。

2. 競合を発見した場合は、**scc --port** を使用して、SAP Control Center サービスが使用するポートを変更します。

解決法 2：メモリ不足

起動しようとしたときにこのエラーが発生する可能性があります。 Could not create the Java virtual machine. 最大メモリ設定を増やします。

参照：

- ポートの設定 (96 ページ)

ログインできない

問題: SAP Control Center Web コンソールにログインできません。

解決法: SAP Control Center が以下のように設定されていることを確認してください。

- オペレーティングシステムを経由するログインが許可されていること
- ログインアカウントに適切な権限が付与されていること

確認する方法については、SAP Control Center 管理者にお問い合わせください。

参照：

- ユーザ承認 (99 ページ)
- セキュリティのセットアップ (78 ページ)

ブラウザを再表示 ([F5] キー) するとログアウトしてしまう

問題: [F5] キーを押してブラウザをリフレッシュすると、SAP Control Center からログアウトされます。

解決法: SAP Control Center にログインしている場合は、[F5] キーを使用しないでください。ブラウザのリフレッシュでは、SAP Control Center 内のデータはリフレッシュされませんが、ブラウザでロードされたアプリケーションまたはページはリフレッシュされます。この場合は、SAP Control Center が構築されている Adobe Flash です。したがって、[F5] キーを押すと現在ログインしている SAP Control Center などのサーバからログアウトされることになります。

十分な期間のパフォーマンス統計が表示されない

問題: 長期間にわたるパフォーマンスカウンタをグラフ表示しようとしても、統計チャートには、直近のデータしか表示されません。

解決法: レポジトリの消去オプションを変更して、必要な期間の統計データを保持して利用できるようにすることを、SAP Control Center 管理者に依頼してください。デフォルトでは、ディスク領域の消費を少なくするために統計は頻繁に消去されます。

参照：

- レポジトリ消去の設定 (160 ページ)
- パフォーマンスカウンタのグラフ表示: 統計チャート (140 ページ)

オンラインヘルプのリセット

問題: SAP Control Center オンラインヘルプが破損しているか、見つかりません (404 エラー)。

解決法: オンラインヘルプファイルをクリアして、SCC で強制的に新しいファイルを構築します。

1. SAP Control Center を停止する。
2. 次のディレクトリを削除します。

```
<SCC-installation-directory>%SCC-3_3%services
%EmbeddedWebContainer%container%Jetty-6.1.22%work
%Jetty_0_0_0_0_8282_help.war__help__.smpe97
```

ヒント： Windows では、削除エラーが表示されることがあります。エラーの内容にかかわらず、パスの長さによって発生する場合があります。エラーを削除するには、Jetty_0_0_0_0_8282_help.war__help__.smpe97 フォルダを「J」などの短い名前に変更します。次に名前を付けたフォルダを削除します。

3. 次のファイルを削除します。

```
<SCC-installation-directory>%SCC-3_3%services
%EmbeddedWebContainer%container%Jetty-6.1.22%contexts
%_help.xml
<SCC-installation-directory>%SCC-3_3%services
%SybaseControlCenter%help%com.sybase.infocenter.scc.zip
<SCC-installation-directory>%SCC-3_3%services
%SybaseControlCenter%help%help.war
<SCC-installation-directory>%SCC-3_3%services
%SybaseControlCenter%help%help_info.xml
```

4. SCC を起動します。サーバが起動したら、ヘルプが再構築されます。これには、数分かかります。
5. ヘルプを表示するには、 <https://<your-SCC-host>:8283/help/index.jsp> に移動します。

注意： 再起動直後にヘルプを表示しようとすると、ファイルが見つからないことを示すエラーが表示されます。数分待ってから、もう一度試してください。

データ収集が完了しない

問題： 収集が頻繁にタイムアウトするか、REJECT_DUPLICATE_RESOURCE_AND_COLLECTION ポリシーについてのエラーが生成されます。ただし、モニタされているリソースに顕著な問題は見つかりません。

エラーがログに記録され、収集履歴画面に表示されます。

解決法： 収集が長時間を要する理由を究明します。たとえば、ネットワークの遅延によって、SAP Control Center とモニタされるサーバとの間のトラフィックが遅速になっている、などです。

ネットワーク遅延や他のリソース関連の問題が発生している場合、収集を実行する間隔が、収集が終了するのに必要な時間よりも短いことがあります。この問題を解決するには、収集を実行する間隔を長くします。

参照：

- ジョブのデータ収集間隔の変更 (148 ページ)

起動時のメモリ警告

問題: SAP Control Center の起動時に、システムメモリまたはヒープメモリの割り付けについての警告が表示されます。

解決法: 最大メモリ設定 (`SCC_MEM_MAX` または `jvmopt=-Xmx`) を増やします。

参照：

- メモリ使用の設定 (68 ページ)

SCC メモリ不足エラー

問題: SAP Control Center によって OutOfMemory エラーが生成されます。

解決法:

- OutOfMemory によって SAP Control Center のヒープ領域が不足していることが通知された場合は、最大メモリ設定を増やします (`SCC_MEM_MAX` または `jvmopt=-Xmx`)。
- OutOfMemory によって SAP Control Center の永続的な生成領域が不足していることが通知された場合は、永続メモリ設定を増やします (`SCC_MEM_PERM` または `jvmopt=-XX:MaxPermSize`)。
- OutOfMemory エラーが繰り返される場合は、メモリリークの可能性があります。OutOfMemory エラーは、次のようなヒープダンプを生成します。
 - SAP Control Center を Windows のサービスとして実行している場合:
C:/windows/system32
 - SAP Control Center を UNIX のサービスとして実行している場合:
<SCC-install-directory>/SCC-3_3/bin

分析のために、製品の保守契約を結んでいるサポートセンタにヒープダンプをお送りください。

参照：

- メモリ使用の設定 (68 ページ)

用語解説: SAP Control Center for Data Assurance

Replication Server Data Assurance (DA) Option に関連する SAP Control Center 用語の定義を示します。

可用性 – リソースがアクセス可能で応答しているかどうかを示します。

収集 – 監視対象サーバから値が同時に収集される、指定された事前定義の主要パフォーマンス指標のセット。ここからパフォーマンスや可用性のデータが供給され、SAP Control Center 画面やチャートに表示されます。スケジューラを使用してコレクションの一覧を表示し、実行する収集、頻度、および実行時間を制御します。

接続プロファイル – データベース接続を確立するために必要な情報。

データベース – 特定の目的のために編成された、関連するデータテーブルとその他のオブジェクトの集まり。

Data Assurance のジョブ – compareset を比較する方法と日時を定義するロー比較ジョブまたはスキーマ比較ジョブ。

Data Assurance システムデータベース (DASD) – システムの設定および構成の設定が保存される DA サーバデータベース。

データ転送ストリーム (DTS) – ストリームデータとの比較時に DA エージェントが使用するアプリケーションプロトコル。

イベント – ユーザのログイン、サービスの開始/停止、または状態変更など、システム内のアクティビティ。アラート機能を使用してシステムイベントを検出し、通知を受け取ります。

ヒートチャート – 現在の観点に登録されているすべてのリソースの可用性および選択したパフォーマンスおよび状態測定基準のグラフィックビュー。

一貫性のないロー – プライマリデータベースと複製データベースの両方に存在するが、比較される 1 つ以上のカラムで値が異なるテーブルロー。

Java データベースコネクティビティ (JDBC) – Java アプリケーションで SQL (Structured Query Language) を使用して複数のデータベース管理システムにアクセスするための API (アプリケーションプログラムインタフェース)。

jConnect – SAP の高性能 JDBC ドライバ。

ジョブ – SAP Control Center でスケジューラによって実行されるタスク。

主要パフォーマンス指標 (KPI) – モニタ対象リソースのステータスやパフォーマンスの評価に使用される測定基準の1つ。KPI 値には、状態(実行中、エラー、停止など)も数値も使用できます。KPI は、コレクションにグループ化されています(また、一部の製品モジュールでは KPA (主要パフォーマンス領域)にもグループ化されます。KPI 値は、定期収集ジョブによって収集され、モニタリング画面、統計、およびヒートチャートに表示されます。KPI の例としては、リソースの状態や CPU 使用率などがあります。

管理対象リソース – 「リソース」を参照してください。

欠落したロー – プライマリデータベースには存在するが、複製データベースには存在しないテーブルロー。

孤立したロー – 複製データベースには存在するが、プライマリデータベースには存在しないテーブルロー。

パースペクティブ – SAP Control Center の名前付きタブ。管理対象リソース(サーバなど)の収集に関する情報やそれらのリソースに関連付けられているビューのセットが表示されます。観点のビューは観点のユーザによって選択されています。必要な数の観点を登録し、それらをカスタマイズして、リソースをモニタまたは管理できます。観点を使用して、場所、部門、またはプロジェクトなど各自の環境に合った方法でリソースをグループ化できます。

プライマリキー – 各ローをユニークに識別するテーブルカラムのセット。

製品モジュール – 特定の Sybase 製品を管理およびモニタする SAP Control Center のプラグインコンポーネント。SCC 製品モジュールは SAP ASE、Data Assurance (Replication Server のオプション)、複製 (Replication Server、Replication Agent、Mirror Replication Agent)、SAP Sybase Event Stream Processor、および SAP Sybase IQ に利用可能です。

複製 – 1つのデータベースのデータの変更(レコードの作成、更新、削除など)が、別のデータベースの対応するレコードにも適用されるプロセス。

レポジトリ – SAP Control Center に含まれるデータベース。管理対象リソースに関する情報に加え、ユーザ設定データ、運用データ、パフォーマンス統計が保存されます。

リソース – SAP Control Center がモニタまたは管理できるサーバ、エージェント、またはその他のエンティティ。SCC が管理できるリソースには SAP ASE、Data Assurance Server、Replication Server、Replication Agent、Mirror Replication Agent、SAP Sybase Event Stream Processor、SAP Sybase IQ、および特定のサブコンポーネントなどがあります。

Replication Server Data Assurance (DA) Option – 2つ以上の SAP Adaptive Server Enterprise (SAP ASE) データベース間でローデータとスキーマを比較し、不一致を

レポートする SAP サーバプログラム。SAP Control Center では、Replication Server DA Option をモニタおよび管理する製品モジュールは SCC for DA と呼ばれます。

Replication Server システムデータベース (RSSD) – SAP Replication Server のシステムテーブルを格納する SAP ASE データベース。SAP Replication Server システムテーブルを、RSSD と SAP SQL Anywhere ERSSD のどちらに格納するかを選択できます。

Remote Method Invocation (RMI) – DA サーバと DA エージェント間の通信に使用されるリモートプロシージャコール。

SCC エージェント – 管理対象サーバ上で実行される SAP Control Center 用のリモートコマンドおよび制御エージェント。SCC エージェントは Sybase サーバの一部として自動的にインストールされます。

SCC 対応ログインアカウント – 適切な SAP Control Center ロールのマッピングにより SAP Control Center の特権を付与されたユーザアカウント。(ルールは通常、アカウント自体ではなくアカウントが属するグループにマッピングされています。) ユーザアカウントおよびグループは SAP Control Center にネイティブであるか、SAP Control Center 認証が委任されているオペレーティングシステムまたは LDAP ディレクトリサービスで作成されたものです。SAP Control Center にログインするには、SCC 対応のアカウントを使用する必要があります。

スケジュール – タスク (統計セットの収集など) および SAP Control Center でタスクを実行する時間の定義。

スキーマ – データベースの構造。

TDS (Tabular Data Stream) – Open Client と SAP Open Server が情報を交換するために使用されるアプリケーションプロトコル。

トポロジ – ある環境におけるサーバの相互接続関係を図で表したもの。環境の可用性を視覚的に図示するネットワーク図です。

ビュー (SCC) – SAP Control Center 観点内のウィンドウで、1 つ以上の管理対象リソースに関する情報を表示します。一部のビューでは、管理対象リソースまたは SCC 自体との対話が可能です。たとえば [Perspective Resources] ビューには、現在の観点で管理されているすべてのリソースがリストされます。その他のビューでは、アラートの設定、複製環境のトポロジの表示、パフォーマンス統計のグラフ化を実行できます。

索引

記号

- Xmx 最大メモリオプション 31, 71
- XX:MaxPermSize 永続メモリオプション 31, 71
- [Perspective Resources] ビュー
 - アイコン 4
 - アイコンの表示/非表示 3
 - 説明 149, 152
 - 表示ツールとオプション 5
- [Save data collected from this job] チェックボックス 114
- [View] メニュー 7

A

- Adobe Flex 12
- Adobe Flex のキーボードショートカット 12
- ALL ログingleレベル 163

C

- compareset
 - 削除 125
 - 作成 123
 - 表示 126
 - 変更 124
 - 編集 124
- comparesets 123
- csi_config.xml ファイル 38, 83

D

- DASD 183
- Data Assurance 184
 - 主要パフォーマンス指標 117
 - データベース接続の削除 172
- Data Assurance エージェント
 - スタンドアロンエージェント 169
 - リモートエージェント 169
 - ローカルエージェント 169
- Data Assurance サーバ
 - データベース接続の作成 118

- データベース接続の編集 171
- モニタリング設定 110
- ログファイル 161

- Data Assurance システムデータベース 183
- Data Assurance の DTS 183
- Data Assurance のジョブ 183
 - スケジューリング 132
- Data Assurance のデータ転送ストリーム 183
- DEBUG ログingleレベル 163

E

- ERROR ログingleレベル 163

F

- F11 (ブラウザの全画面モードの切り替え) 7
- F5 (ブラウザのリフレッシュ)
 - ログアウト SAP Control Center 180
- FATAL ログingleレベル 163
- Flash Player 15

G

- groups 57, 106

H

- help コマンド (コンソール) 166

I

- info コマンド (コンソール) 166
- INFO ログingleレベル 163

J

- Java システムプロパティ
 - 情報の表示 166
- jConnect 183
- JDBC 183

索引

K

KPI 184

L

LDAP

SCC ログインが認証されるようにするための設定 34, 79

設定プロパティ 39, 85

認証の設定 38, 83

log4j.properties ファイル 164

O

ODBC ドライバ

登録 14, 60

OutOfMemory エラー、SCC 182

P

passencrypt ユーティリティ 50, 95

R

Red Hat Linux 認証 37, 82

REJECT_DUPLICATE_RESOURCE_AND_COLLECTION ポリシーエラー 181

Remote Method Invocation (DA) 185

Replication Server Data Assurance Option 184
データベース接続 171

Replication Server Data Assurance のオプション
データ収集 116

Replication Server システムデータベース 185

resource explorer
起動アイコン 3

Resource Explorer

検索 151

説明 149

表示ツールとオプション 5

RMI (DA) 185

role-mapping.xml ファイル 48, 93

RSSD 185

RSSD ユーザ名、認証に使用 17, 113

S

SAP Control Center

[F5] キーによる意図しないログアウト
180

Sybase Control Center へのブラウザの接続
15

UNIX でのサービスとしての起動 24, 64

UNIX での起動 24, 64

UNIX での停止 24, 64

Windows でのサービスとしての起動 20,
60

Windows での起動 20, 60

Windows での停止 20, 60

アクセスビリティ 12

キーボードショートカット 8

コンソールコマンド 166

コンポーネントバージョンの表示 10

ログアウト 77

ログイン 32, 76

ログファイル 162

起動 14, 59

起動できない 179

表示ツールとオプション 5

SAP Control Center for Data Assurance

概要 1

新機能 2

SAP Control Center からのログアウト

意図しない、[F5] キーを使用してのブラウザの再表示 180

SCC エージェント 185

UNIX でのサービスとしての起動 24, 64

UNIX での起動 24, 64

UNIX での停止 24, 64

Windows でのサービスとしての起動 20,
60

Windows での起動 20, 60

Windows での停止 20, 60

scs コマンド 72

使用した起動 SAP Control Center 14, 59

SCC コンポーネントのバージョン

表示 10

SCC でのカラムのフィルタリング 7

SCC ビューのレイアウト 154

SCC 管理者グループ 48, 93

SCC 対応のログインアカウント 185

SCC_MEM_MAX 28, 30, 31, 68, 70, 71, 182

SCC_MEM_PERM 28, 30, 31, 68, 70, 71

scs.bat 14, 20, 60

scc.sh 24, 64
 sccadmin アカウント
 説明 15
 sccAdminRole 57, 106
 sccd シェルスクリプト 24, 64
 sccUserRole 57, 106
 shutdown コマンド (コンソール) 167
 sql.ini ファイル、sql.ini ファイルからリソース
 のインポート 111
 status コマンド (コンソール) 168
 SUSE Linux 認証 37, 82
 sybase グループ 48, 93

T

Tabular Data Stream 185
 TDS 185

U

UNIX
 SCC または SCC エージェントの起動、停
 止 24, 64
 バックグラウンドでの SCC または SCC エ
 ージェントの実行 24, 64
 フォアグラウンドでの SCC または SCC エ
 ージェントの実行 24, 64
 認証の設定 36, 81
 UNIX 認証用のプラグ可能認証モジュール 36,
 81

W

WARN ログingleレベル 163
 Windows
 起動、SCC または SCC エージェントの停止
 20, 60
 認証の設定 35, 80
 Windows サービスの jvmopt メモリオプション
 28, 31, 68, 71

あ

アイコン
 SCC ツールバー 3
 サーバステータス用 4

ビューのセクションの最小化/最大化 7
 アクセシビリティ 12
 アプリケーションメニュー 2
 アラート
 履歴のレポジトリ消去の効果 160

い

一貫性のないロー、DA 183
 イベント 183
 インクリメンタルバックアップ 155
 インストール後の作業 15
 インストール後の設定 15
 インタフェースファイル、インタフェースフ
 ァイルからリソースのインポート
 111
 インポート
 interface ファイル 120
 接続 120

え

エージェント接続
 削除 170
 作成 117
 変更 169
 編集 169
 エラー
 OutOfMemory 182
 REJECT_DUPLICATE_RESOURCE_AND
 _COLLECTION ポリシー 181
 データ収集のタイムアウト 181

お

オペレーティングシステム
 SCC ログインが認証されるようにするた
 めの設定 34, 79
 オンラインヘルプ
 リセット 180

か

外部ソートの問題 177
 カラム
 ソート 5

索引

カラムによつてのソート 5
カラムの比較の問題、データベースハッシュ
177

監査トレースレベル
設定 175

監視
Data Assurance 173

き

キーボードショートカット 8
機能、新しい
SAP Control Center for Data Assurance 2

く

クライアントログ、表示 162
グラフ表示用統計 140
グリッド形式、使用 5
グループ
LDAP、SCC 役割へのマッピング 48, 93
OS、SCC 役割へのマッピング 48, 93
SCC 管理者 48, 93
sybase 48, 93
モニタリング役割と管理役割の割り当て
55, 100
ログインアカウントの追加 56, 103
ログインの削除 103
作成 56, 101
削除 102
役割の削除 101

け

欠落したロー、DA 184

こ

更新
スキーマ比較 135
孤立したロー、DA 184
コレクション 183
コンソール
コマンド 166
説明 165

さ

サーバ
データ収集スケジュールの変更 148

一括でのインポート 111

可用性の表示 18, 139

検索 151

登録解除 149

認証 17, 113

サーバ、Data Assurance

SAP Control Center への登録 16, 110

サーバログ、Data Assurance の表示 161

サーバログ、表示 162

サービス

リスト 166

有効化/無効化 72

サービス、UNIX

SCC UNIX サービス用メモリオプションの
設定 31, 71

SCC または SCC エージェントをサービス
として実行 24, 64

サービス、Windows

SCC または SCC エージェントをサービス
として実行 20, 60

設定 SAP Control Center メモリオプション
31, 71

削除

Data Assurance ジョブ 137

Data Assurance のデータベース接続 172

エージェント接続 170

ローまたはスキーマひかくジョブの比較
137

作成

compareset 123

Data Assurance サーバのデータベース接続
118

Data Assurance のジョブ 127

RSSD に基づくジョブ 132

エージェント接続 117

スキーマ比較ジョブ 134

し

システムプロパティ
情報の表示 166

システムワイド機能
設定 33, 78

実行

スキーマ比較 136

ロー比較 136

- ジョブ 183
 - Data Assurance 126
 - Data Assurance の作成 127
 - Data Assurance の変更 131
 - Data Assurance の編集 131
 - サスペンド 148
 - 履歴の結果の削除 138
 - レジューム 148
 - 収集間隔の変更 148
- ジョブ履歴
 - 削除 138
 - レポートの表示 138
- ジョブ履歴の結果 138
- 新機能
 - SAP Control Center for Data Assurance 2

す

- スキーマ、DA 185
- スキーマ比較
 - 更新 135
 - 作成 134
 - 実行 136
 - 設定 134
 - 変更 135
 - 編集 135
- スケジューラ
 - サスペンド 148
 - レジューム 148
- スケジューリング
 - Data Assurance のジョブ 132
- スケジュール 144, 185
 - ジョブから削除 147
 - ジョブへの追加 146
 - データ収集ジョブの作成 114
 - 表示 147
- スタンドアロンエージェント 169
- ステータス
 - Data Assurance 117

せ

- セキュリティ 34, 79
 - 設定 33, 78
- セキュリティプロバイダ
 - 設定 34, 79

- 接続、DA 183
- 設定
 - Data Assurance パラメータ 175
 - オプション 121
 - スキーマ比較ジョブ 134

た

- タイムアウト
 - データ収集のエラー 181
 - ログインセッション用の設定 54, 99

つ

- ツールバーアイコン 3

て

- 定義 183–185
- データパーティション境界値
 - 表示 126
- データベース、DA 183
- データベースハッシュカラムの比較の問題 177
- データ収集
 - タイムアウトのトラブルシューティング 181
- データ収集ジョブ
 - スケジュールの削除 147
 - スケジュールの追加 146
 - スケジュールの表示 147
 - データを保存しない 114
 - 再開 146
 - 作成 114
 - 削除 145
 - 実行 145
 - 中断 146
 - 追加 114
 - 停止 145
 - 履歴の表示 148
- データ収集スケジュール
 - 追加 114
 - 変更 148
- テキストの規則 10
- テスト
 - エージェント接続 171, 173

索引

と

- トポロジ、DA 185
- トポロジ、Data Assurance
 - 表示 174
- ドライバ
 - ODBC、登録 14, 60
- トラブルシューティング
 - Data Assurance 177
 - 外部ソートの問題 177
 - データベースハッシュカラムの比較の問題 177
 - メモリ不足エラー 178

は

- パースペクティブ 184
 - リソースの削除 150
 - リソースの追加 150
 - 作成 152
 - 削除 152
 - 説明 152
 - 名前の変更 153
 - パースペクティブのヒートチャートビュー 18, 139
 - パスワード
 - SCC デフォルトログインアカウント 15
 - レポジトリデータベース dba アカウント用、変更 72
 - 暗号化 50, 95
 - バックアップ
 - スケジューリング 155
 - スケジュールの変更 157
 - バックアップからのリストア 158
 - 強制 157
 - 説明 155
 - 中断と再開 157
 - バックグラウンド、バックグラウンドでの SCC
 - または SCC エージェントの実行 24, 64
 - バッジ、ステータス 4
 - パフォーマンスモニタリング 140
 - パラメータ
 - Data Assurance の設定 175
- ### ひ
- ヒートチャート 183
 - アイコン 4

- カラムのカスタマイズ 18, 139
 - 起動アイコン 3
 - 表示 18, 139
 - 表示されるリソースのフィルタリング 18, 139
 - 表示ツールとオプション 5
- ### 比較
- スキーマ 134
 - ロー 126
- ### ビュー
- セクションの最大化と最小化 7
- ### ビュー、SCC 185
- パースペクティブの前面に移動 153
 - メニュー 2
 - 開く 153
 - 管理用アイコン 3
 - 観点での並べ替え 154
 - 元のサイズに戻す 153
 - 最小化する 153
 - 最大化する 153
 - 説明 153
 - 閉じる 153
- ### 表示
- compareset 126
 - Data Assurance のジョブ 137
 - Data Assurance のジョブのステータス 138
 - Data Assurance のジョブのレポート 138
 - エージェントのプロパティ、Data Assurance 170
 - ジョブリスト、Data Assurance 137
 - ジョブ履歴レポート 138
 - データパーティション境界値 126
 - データベース接続プロファイル 173
 - トポロジ、Data Assurance 174

ふ

- フォアグラウンド、フォアグラウンドでの SCC
 - または SCC エージェントの実行 24, 64
- フォントサイズ、変更 8
- 複写 184
- プライマリキー、DA 184
- フルバックアップ 155

プロパティ
リソース、変更 151

へ

変更

compareset 124
Data Assurance ジョブ 131
エージェント接続 169
スキーマ比較 135

編集

compareset 124
Data Assurance サーバのデータベース接続
171
Data Assurance ジョブ 131
エージェント接続 169
システムプロパティ、Data Assurance 175
スキーマ比較 135

ほ

ポート

デフォルト 72
情報の表示 166
設定 51, 96
変更 72

ポートの競合 179

め

メッセージレベル 163

メッセージロー
使用 143

メニュー、アプリケーション、およびビュー
2

メモリ

起動時の警告 182
情報の表示 166
設定 28, 68

メモリ、不足 179

メモリ不足エラー、DA サーバ 178

メモリリーク 182

も

モニタ

Data Assurance エージェント 19, 174

Data Assurance サーバ 19, 174

モニタリング

パフォーマンス 140

ゆ

ユーザアカウント

デフォルト 104
ネイティブ SCC、追加 104
ネイティブ SCC、未使用 34, 79

ユーザインタフェース、説明 2

ユーザ情報

変更 106

よ

用語

SCC for Data Assurance 183

用語解説

SCC for Data Assurance の用語 183

り

リソース 184

データ収集スケジュールの変更 148
パースペクティブからの削除 150
パースペクティブへの追加 150
一括でのインポート 111

可用性の表示 18, 139

管理コンソールでの検索とフィルタリング
143

管理コンソールでの表示対象の選択 143

管理コンソールのカラムによるフィルタ
リング 5

検索 151

参照と管理 142

接続プロパティの変更 151

説明 149

登録解除 149

認証 17, 113

名前の変更 151

リソース、Data Assurance

SAP Control Center への登録 16, 110

リソースのステータスアイコンとバッジ 4

索引

れ

- レポジトリ 155, 184
 - データベース dba パスワードの変更 72
 - バックアップ 157
 - バックアップからのリストア 158
 - バックアップスケジュールの変更 157
 - バックアップのスケジュールリング 155
 - 消去の設定 160

ろ

- ローカルエージェント 169
- ロー比較
 - 実行 136
- ロギングレベル 163
- ログ
 - Data Assurance ログ、表示 161
 - SCC エージェントログ、説明 161
 - アラートサービスログ、説明 161
 - エージェントログ、表示 162
 - クライアントログ、説明 161
 - クライアントログ、表示 162
 - コンポーネントログ、説明 161
 - サーバログ、説明 161
 - サーバログ、表示 162
 - スクリプト実行ログ、説明 161
 - レポジトリログ、説明 161
 - レポジトリログ、表示 162

- ロギングレベルの変更 163
 - 設定 164
- ログアウト SAP Control Center 77
- ログイン SAP Control Center 32, 76
 - トラブルシューティング 179
- ログイン SAP Control Center - 最初のユーザ 15
- ログインアカウント
 - サスペンド 106
 - デフォルト 104
 - ネイティブ SCC、追加 104
 - モニタリング役割と管理役割の割り当て 55, 100
 - 削除 105
 - 事前定義 57, 106
 - 自動作成 (UNIX) 36, 81
 - 自動作成 (Windows) 35, 80
 - 認証 17, 113
 - 変更 106
 - 役割とグループによる権限の付与 48, 93
 - 役割の削除 101
 - 有効期限の終了日、設定 106
- ログインアカウント、デフォルト
 - 説明 15
- ログインアカウントの有効期限の終了日 106
- ログインセッションタイムアウト
 - 設定 54, 99
- ログインセッションのタイムアウトろぐいんせっしょんのたいむあうと 77
- ログインモジュール 34, 79