Identity Console
管理ガイド

2022 年 9 月

保証と著作権

保証と著作権、商標、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、https://www.netiq.com/company/legal を参照してください。

目次

本書およびライブラリについて

『*管理ガイド*』には、NetIQ Identity Console (Identity Console) 製品に関する概念的な情報が含まれています。本書には、用語の定義および実装シナリオを記載しています。

最新バージョンの『*NetIQ Identity Console 管理ガイド*』については、NetIQ Identity Console オンラインヘルプサイトにある英語版のマニュアルを参照してください。

本書の読者

このガイドはネットワーク管理者を対象としています。

ライブラリに含まれているその他の情報

ライブラリには次の情報リソースが含まれています。

インストールガイド

Identity Console をインストールする方法について説明します。本書はネットワーク管理者を対象としています。

NetIQ 社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという 3 つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普遍の課題

実際、直面するあらゆる課題の中で、これらは、物理環境、仮想環境、およびクラウドコンピューティング環境の安全な評価、監視、および管理を行うために必要な制御を脅かす最大の要因かもしれません。

重要なビジネスサービスの改善と高速化を可能にする

当社は、IT 組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様の IT 組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントな IT ソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作する IT ソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としています。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ID およびアクセスのガバナンス
- アクセス管理

- セキュリティ管理
- システムおよびアプリケーション管理
- ワークロード管理
- サービス管理

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、各地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通 :	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ :	1-888-323-6768
電子メール :	info@netiq.com
Web サイト :	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通 :	www.netiq.com/support/contactinfo.asp
北米および南米 :	1-713-418-5555
ヨーロッパ、中東、アフリカ :	+353 (0) 91-782 677
電子メール :	support@netiq.com
Web サイト :	www.netiq.com/support

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。改善のためのご提案は、www.netiq.com/documentation に掲載されている本マニュアルの HTML 版で、各ページの下にある［**[コメントを追加]**］をクリックしてください。Documentation-Feedback@netiq.com 宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQ のオンラインコミュニティである Qmunity は、他のユーザや NetIQ のエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQ エキスパートとのやり取りを提供する Qmunity は、頼みにしている IT 投資が持つ可能性を余すことなく実現するために必要な知識の習得に役立ちます。詳細については、http://community.netiq.com を参照してください。

1 Identity Console とは何か

Identity Console は、インターネットと Web ブラウザを介してどこからでもネットワーク管理用のユーティリティにアクセスできる、最先端の Web ベースの管理コンソールです。アクセスは仮想化され、セキュリティ保護され、カスタマイズされます。Identity Console を使用すると、管理タスクを簡単に分散化できます。

Identity Console の機能

Identity Console には、次のような機能があります。

- eDirectory のオブジェクト、ユーザ、スキーマ、パーティション、レプリカ、権利などを管理します
- Identity Manager ドライバおよびドライバセットを管理します
- ドライバのパフォーマンス統計の管理と表示
- オブジェクトの点検、ドライバのデータフローの表示、エンタイトルメントの管理、ワークオーダーなど
- パスワード同期ステータスとドライバの設定の管理
- パスワードポリシーおよびログインメソッドの管理
- 証明書の管理
- 各種のネットワークリソースを管理します
- データを保護するためのセキュリティ手段を強化します
- より大規模な eDirectory オブジェクトを管理できるようにスケーラビリティを強化します
- One SSO Provider (OSP) を使用して、Identity Console ポータルへのセキュリティ保護されたログインが可能になります
- 業界の最新の UI 技術を基盤としています
- Docker コンテナにより、インストールと設定が容易です

2 Identity Console にアクセスする方法

サポート対象の任意の Web ブラウザから Identity Console にアクセスして、備わっている全機能を利用することができます。その他の Web ブラウザを使って Identity Console にアクセスすることもできますが、正式なサポート対象外のブラウザを使用した場合の正常な動作は保証されず、サポートもいたしません。

重要 : サポートされている Web ブラウザについては、「*Identity Console インストールガイド*」を参照してください。

Identity Console へのアクセス

サーバベースの Identity Console にアクセスするには、次の手順を実行します。

1. サポートされる Web ブラウザのアドレス (URL) フィールドに次のアドレスを入力します。

   セキュリティ保護されたログイン : https://< *サーバ IP アドレス* / ホスト名 >:< ポート >/identityconsole/

   この例では、< *サーバ IP アドレス* > の IP アドレスは IPv4 である必要があります。使用するデフォルトのポートは 9000 です。
2. ユーザ DN とパスワードを使用してログインします。
3. eDirectory ツリーの IP または LDAP セキュアポート付属またはなしの DNS を指定します。

注

- Identity Console のいずれかのタブを更新すると、セキュリティ上の理由でユーザがログアウトされます。
- ブラウザで重複する Identity Console タブを開くと、セキュリティ上の理由でユーザがログアウトされます。
- DN は、cn=admin,ou=sa,o=system 形式で指定する必要があります。
- eDirectory がデフォルト以外のポートで設定されている場合は、ポート番号を指定する必要があります。

---

3 Identity Console インタフェースのナビゲート

このセクションでは、Identity Console の Web インタフェースを使用してナビゲートする方法について説明します。

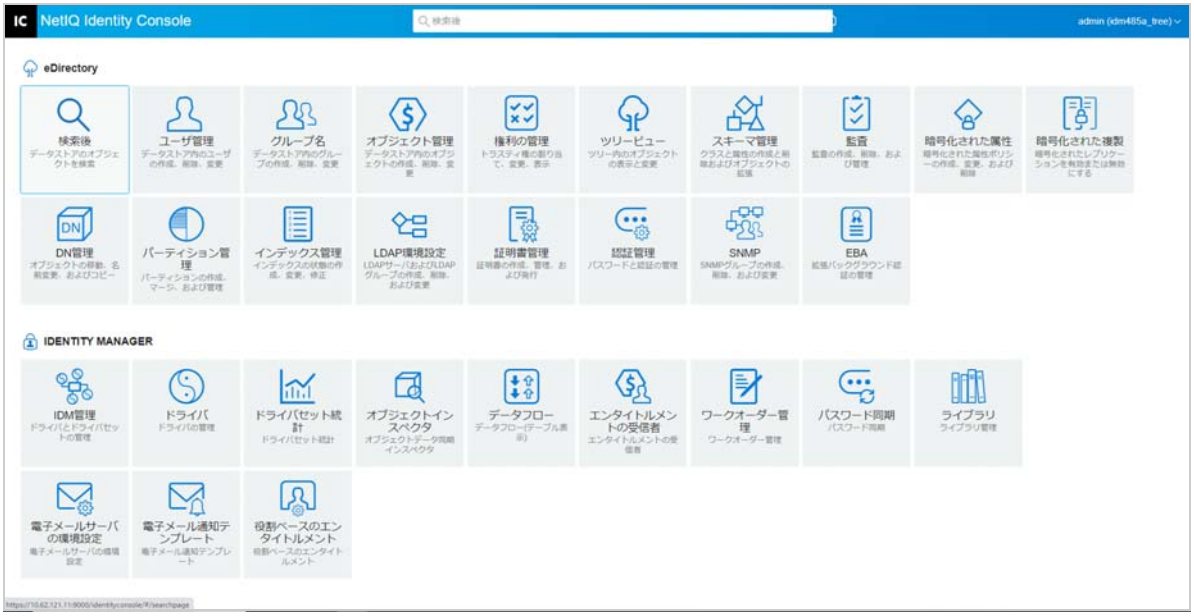
検索 (技術プレビュー)

[検索技術プレビュー] には、検索機能の導入レイアウトが表示されます。このプレビューでは、キーワードを指定し、検索フィールドで検索する情報ソースを決定し、一致する結果を表示することができます。このオプションを使用すると、Identity Console アプリケーションの任意のページで簡単にリソースを探してアクセスできます。

Identity Console インタフェース

Identity Console インタフェースは、eDirectory および Identity Manager モジュールで構成されています。

図 3-1 *Identity Console インタフェース*



重要 : このガイドで使用されているいくつかの GIF アニメーションは、オンラインヘルプでのみ機能します。PDF に切り替えると、スクリーンショットのみが表示されます。

表 3-1 Identity Console の Web ポータルにあるさまざまなモジュールの説明

モジュール名	説明
検索	データストア内のオブジェクトを検索しますからダウンロードします。詳細については、25 ページの第 4 章「検索の実行」を参照してください。
ユーザ管理	データストア内のユーザを作成、削除、および変更します . 詳細については、29 ページの第 5 章「ユーザの管理」を参照してください。
グループ管理	データストア内のグループを作成、削除、および変更します。詳細については、39 ページの第 6 章「グループを管理する」を参照してください。
オブジェクト管理	データストア内のオブジェクトを作成、削除、および変更しますからダウンロードします。詳細については、45 ページの第 7 章「オブジェクトの管理」を参照してください。
権利の管理	トラスティと権利を割り当て、変更、および表示しますからダウンロードします。詳細については、53 ページの第 8 章「権利の管理」を参照してください。
ツリービュー	ツリー内のオブジェクトを表示および変更します . 詳細については、57 ページの第 9 章「ツリービュー」を参照してください。
スキーマ管理	クラス、補助クラス、属性を作成、削除したり、オブジェクトを拡張したりしますからダウンロードします。詳細については、61 ページの第 10 章「スキーマの管理」を参照してください。
監査	CEF 監査を有効または無効にしたり、管理したりします . 詳細については、69 ページの第 11 章「監査イベントの管理」を参照してください。
暗号化属性	暗号化属性ポリシーを作成、修正、削除、および表示します . 詳細については、75 ページの第 12 章「暗号化属性の管理」を参照してください。
暗号化レプリケーション	暗号化複製を有効または無効にしたり、表示したりしますからダウンロードします。詳細については、79 ページの第 13 章「暗号化複製の管理」を参照してください。
DN 管理	オブジェクトを移動、名前変更、およびコピーします . 詳細については、45 ページの第 7 章「オブジェクトの管理」を参照してください。

モジュール名	説明
パーティション管理	パーティションとレプリカを作成、マージ、および移動します。詳細については、81 ページの第 14 章「パーティションおよびレプリカの管理」を参照してください。
インデックス管理	インデックスの状態を作成、変更、および変更します。詳細については、87 ページの第 15 章「インデックスの管理」を参照してください。
LDAP 環境設定	LDAP オブジェクトを作成、削除、および変更します。詳細については、91 ページの第 16 章「LDAP オブジェクトを環境設定する」を参照してください。
証明書管理	サーバ証明書と CA 証明書を作成および管理します。詳細については、95 ページの第 17 章「証明書の管理」を参照してください。
認証管理	login.post-login メソッドおよびシーケンスを作成および管理します。このモジュールを使用して、パスワードポリシーおよび秘密の質問を管理できます。詳細については、113 ページの第 18 章「認証フレームワークの管理」を参照してください。
SNMP	SNMP グループを作成、削除、および変更します。詳細については、129 ページの第 19 章「SNMP グループオブジェクトの管理」を参照してください。
EBA	拡張バックグラウンド認証を管理します。詳細については、133 ページの第 20 章「拡張バックグラウンド認証の管理」を参照してください。
IDM 管理	Identity Manager ドライバおよびドライバセットを管理します。詳細については、137 ページの第 21 章「ドライバおよびドライバセットの管理」を参照してください。このモジュールを使用して、ドライバセットのプロパティも管理できます。詳細については、145 ページの第 22 章「ドライバセットのプロパティの管理」を参照してください。
ドライバのプロパティ	さまざまなドライバのプロパティを管理します。詳細については、159 ページの第 23 章「ドライバプロパティの管理」を参照してください。
ドライバセット統計	ドライバセット統計を管理および表示します。詳細については、191 ページの第 24 章「ドライバセット統計の管理」を参照してください。

モジュール名	説明
オブジェクトインスペクタ	オブジェクトの関連付けとデータの同期を管理します。詳細については、193 ページの第 25 章「Identity Manager オブジェクトの点検」を参照してください。
データフロー	ドライバのデータフローを管理および表示する。詳細については、195 ページの第 26 章「データフローの管理」を参照してください。
エンタイトルメントの受信者	エンタイトルメントの受信者を管理します。詳細については、197 ページの第 27 章「エンタイトルメント受信者の管理」を参照してください。
ワークオーダー管理	ワークオーダーを管理します。詳細については、199 ページの第 28 章「ワークオーダーの管理」を参照してください。
パスワード同期	パスワード同期とステータスを管理します。詳細については、203 ページの第 29 章「パスワードステータスと同期の管理」を参照してください。
ライブラリ管理	ライブラリを管理します。詳細については、207 ページの第 30 章「ライブラリの管理」を参照してください。
電子メールサーバ設定	電子メールサーバオプションを管理します。詳細については、209 ページの第 31 章「電子メールサーバオプションの管理」を参照してください。
電子メール通知テンプレート	電子メールテンプレートを管理します。詳細については、211 ページの第 32 章「電子メールテンプレートの管理」を参照してください。

Identity Console を使用した eDirectory の管理

このセクションでは、Identity Console ポータルを使用して eDirectory サーバを管理するために実行できるさまざまなタスクについて説明します。

4 検索の実行

[検索] タイルでは、ディレクトリツリーで実行する検索操作を指定し、結果を表示することができます。このオプションを使用すると、さまざまなオブジェクト、ユーザ、グループ、およびその他を検索することができます。データストア内のさまざまなオブジェクトの検索操作を実行するには、次の手順に従います。

1 検索するオブジェクト名を指定します。名前の一部を指定するには、アスタリスクワイルドカードを使用します。例 : ldap*、*cert、*server* 等。このフィールドにアスタリスクのみを指定した場合は、選択した [**タイプ**] と [**コンテキスト**] に基づいて、すべての検索結果が Identity Console から返されます。

注 : コンテキストブラウザを使用すると、検索フィールドにアスタリスク (*) を指定して、eDirectory ツリー全体を参照できます。ワイルドカード検索を使用して、コンテキストブラウザでオブジェクトをフィルタすることもできます。たとえば、admin* などです。コンテキストブラウザのこの動作は、Identity Console のさまざまなモジュールでサポートされています。

---

2 [**タイプ**] フィールドで、検索のオブジェクトのタイプを選択します。指定したタイプのオブジェクトのみが Identity Console に表示されます。このフィールドでは、デフォルトで [**ユーザ**] タイプが選択されています。

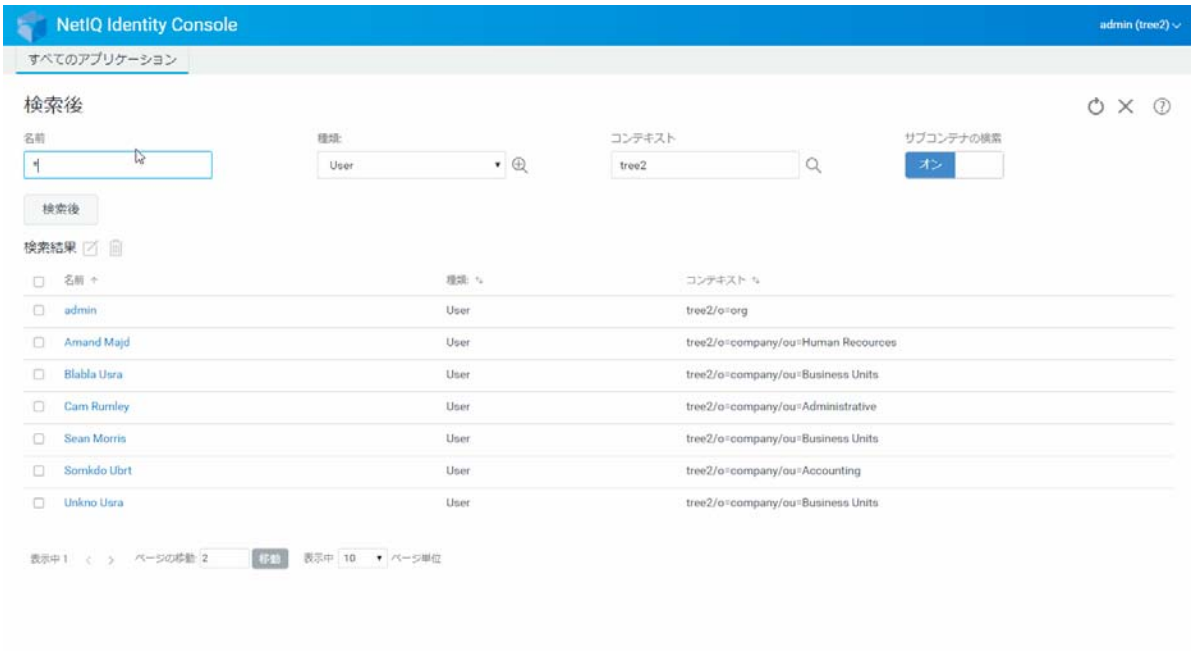
追加で属性レベルの検索設定を定義するには、アイコンをクリックします。詳細については、26 ページの 「詳細検索の設定」を参照してください。

3 [**コンテキスト**] フィールドで、検索操作の開始コンテナを指定します。

4 従属コンテナを検索に含める場合は、[サブコンテナを検索] オプションで [**オン**] を選択します。

5 検索後 ボタンをクリックします。

図4-1 検索操作の実行



詳細検索の設定

[高度な選択] によって、詳細な設定に基づいて目的のオブジェクトをディレクトリで検索できる環境が実現します。

オブジェクトタイプ : 検索するオブジェクトベースクラスを指定します。例 : ユーザ。

補助クラス : 検索に含める補助クラスを指定するには、＋アイコンをクリックします。

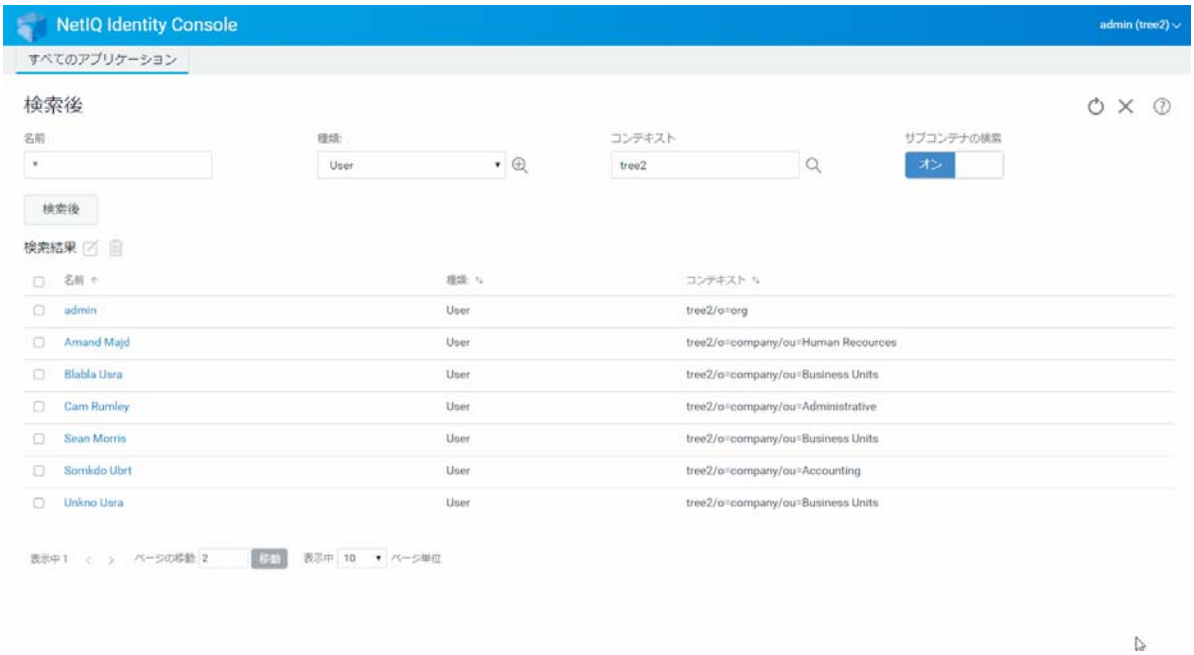
属性 : フィルタの一部として使用する属性 (プロパティ) を指定します。

演算子 : フィルタに適用する論理演算子を指定します。指定できる値は、次のとおりです。

値 : フィルタとして使用する属性値を指定します。値の一部を示すワイルドカードとして、アスタリスク (*) を使用できます。例 : smi*、*th、*mit*。

さらに、＋ Rule アイコンを使用してリストに 2 つ目の属性を追加することで、複数の属性フィルタを連結してフィルタグループにすることができます。複数の属性フィルタを使用する場合は、論理 AND または論理 OR で関連付けます。

図4-2 詳細検索の設定


NetIQ Identity Console
admin (tree2)
すべてのアプリケーション
検索後
名前
種類:
User
コンテキスト
tree2
サブコンテナの検索
オン
検索後
検索結果
名前
種類:
コンテキスト
admin
User
tree2/o=org
Amand Majd
User
tree2/o=company/ou=Human Recources
Blabla Usra
User
tree2/o=company/ou=Business Units
Cam Rumley
User
tree2/o=company/ou=Administrative
Sean Morris
User
tree2/o=company/ou=Business Units
Somkdo Ubrt
User
tree2/o=company/ou=Accounting
Unkno Usra
User
tree2/o=company/ou=Business Units
表示中 1
ページの移動: 2
移動
表示中 10
ページ単位

5 ユーザの管理

データストアの主要な目的は、ユーザとユーザのネットワークアクセスを管理することです。Identity Console Web ポータルを使用すると、次のユーザ関連タスクを実行できます。

ユーザの作成

新しいユーザオブジェクトを作成するには、次を実行します。

1 Identity Console のランディングページから、[**[ユーザ管理]**] オプションをクリックします。

2 ＋アイコンをクリックします。

3 [ユーザの作成] ページで、少なくとも、必須のユーザ関連情報を入力し、

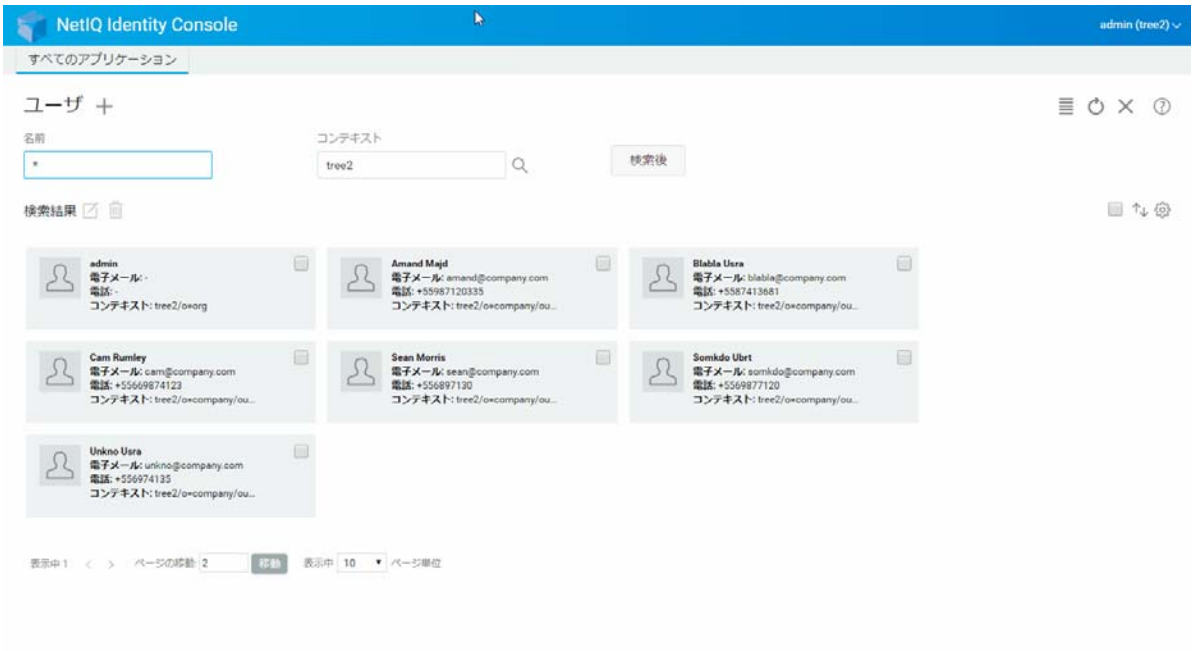
作成

ボタンをクリックします。

- **[[ユーザ名]]**
- **[コンテキスト]**
- **[名字]**
- **[[パスワード]]**

4 ユーザオブジェクトが作成されたことを示す確認メッセージが表示されます。

図 5-1 ユーザの作成

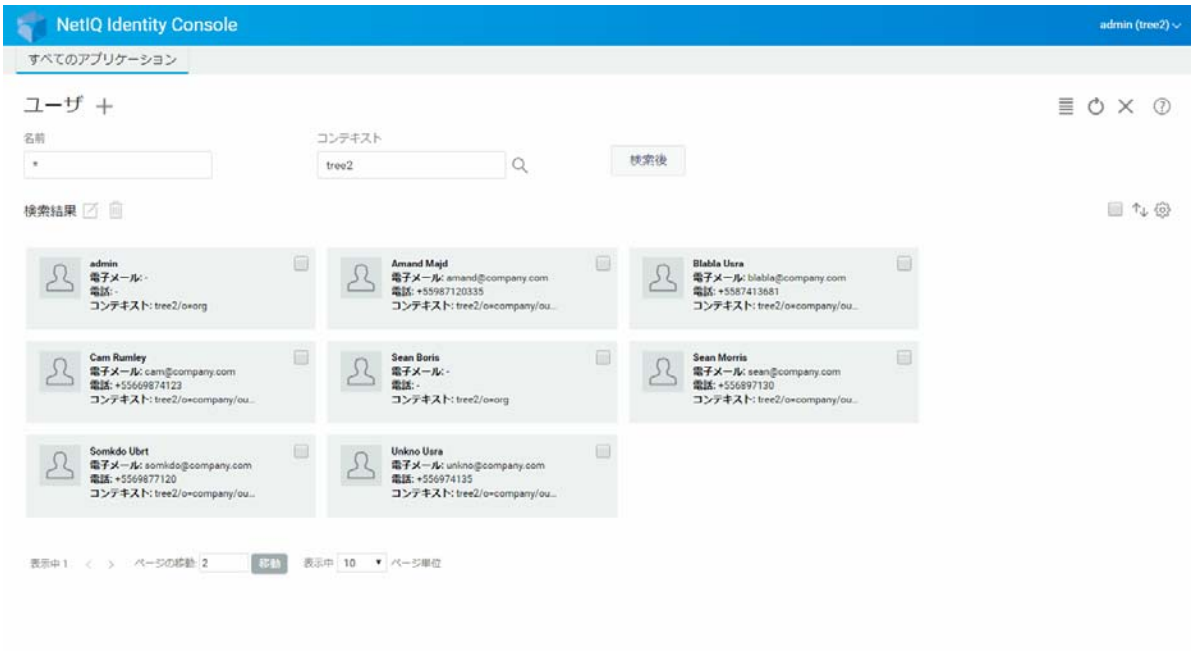


ユーザの削除

ユーザオブジェクトを削除するには、次を実行します。

1. Identity Console のランディングページから、[**[ユーザ管理]**] オプションをクリックします。
2. オブジェクトの名前とコンテキストを入力するか、検索機能を使用して特定し、検索後 ボタンをクリックします。
3. ユーザリストからユーザオブジェクトを選択し、🗑アイコンをクリックします。
4. ユーザオブジェクトが削除されたことを示す確認画面が表示されます。

図5-2 ユーザの削除

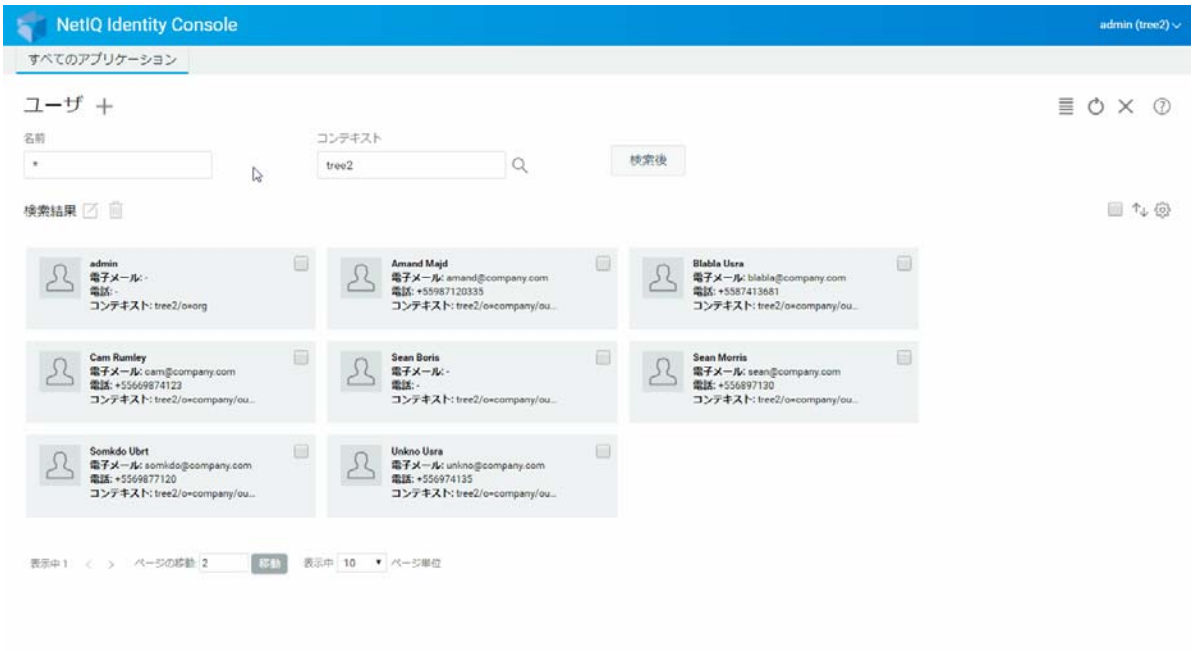


ユーザの変更

ユーザオブジェクトを変更するには :

1. Identity Console のランディングページから、[**[ユーザ管理]**] オプションをクリックします。
2. オブジェクトの名前とコンテキストを入力するか、検索機能を使用して特定し、検索後 ボタンをクリックします。
3. ユーザリストからユーザオブジェクトを選択し、アイコンをクリックします。
4. 必要な変更を加えてから、保存 ボタンをクリックします。
5. ユーザオブジェクトが変更されたことを示す確認メッセージが表示されます。

図5-3 ユーザの変更



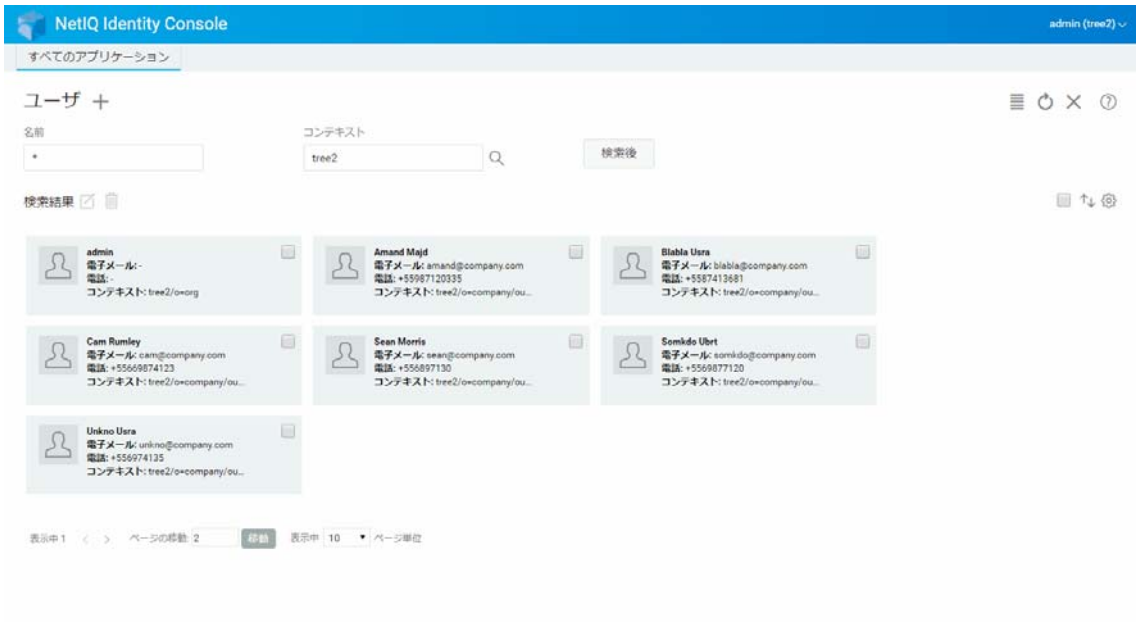
ユーザの検索

ユーザオブジェクトを検索するには :

1 Identity Console のランディングページから、[**[ユーザ管理]**] オプションをクリックします。

2 ユーザを検索するときは、名前を指定するか、名前とコンテキストの両方を指定することができます。必要な詳細を指定したら、検索後 アイコンをクリックします。

図5-4 ユーザの検索

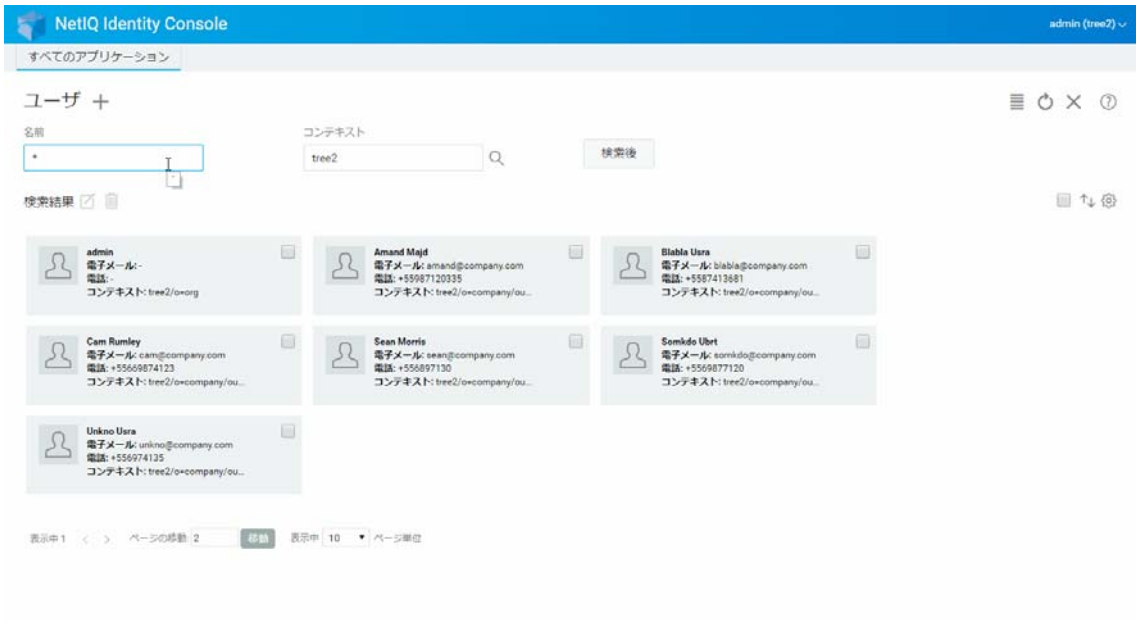


パスワード制限の設定

パスワード制限を使用すると、次の操作を実行できます。

- ユーザは各自のパスワードを変更できます
- ログイン時にパスワードを強制できます
- パスワードの強度を指定できます
- 定期的なパスワード変更を強制できます
- パスワードの有効期限を指定できます
- 固有パスワードの作成を強制できます
- パスワードが期限切れになった場合の猶予ログイン期間を指定できます。

図5-5 パスワード制限



ユーザアカウントの無効化と有効化を実行できます

ユーザアカウントを無効にするには、次の手順を実行します。

1 アカウントを無効にする必要があるユーザを選択し、アイコンをクリックします。

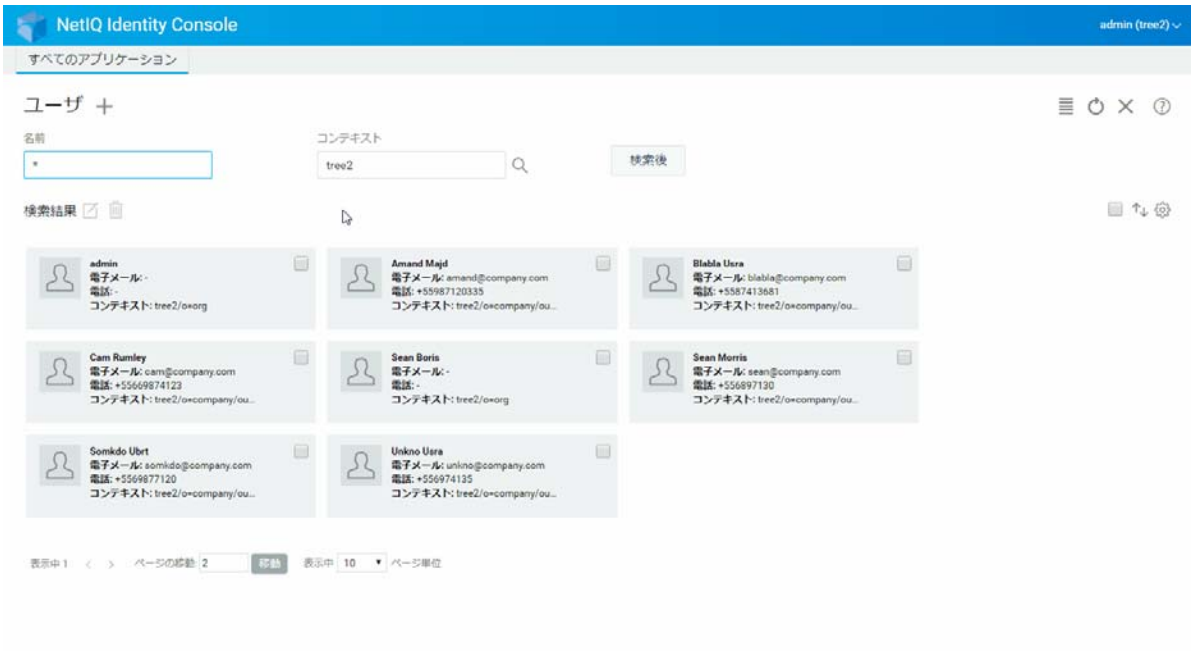
2 [**[ユーザの変更]**] ページの [**[制限]**] タブをクリックします。

3 [**[ログイン制限]**] タブを展開し、[**[アカウント無効]**] チェックボックスをオンにします。

4 保存 アイコンをクリックします。

5 これで、ユーザアカウントが無効になりました。無効にされたユーザアカウントを有効にするには、[**[アカウント無効]**] チェックボックスをオフにします。

図5-6 ユーザアカウントの無効化と有効化



アカウントの有効期限の設定

ユーザのアカウントの有効期限を設定するには、次の手順を実行します。

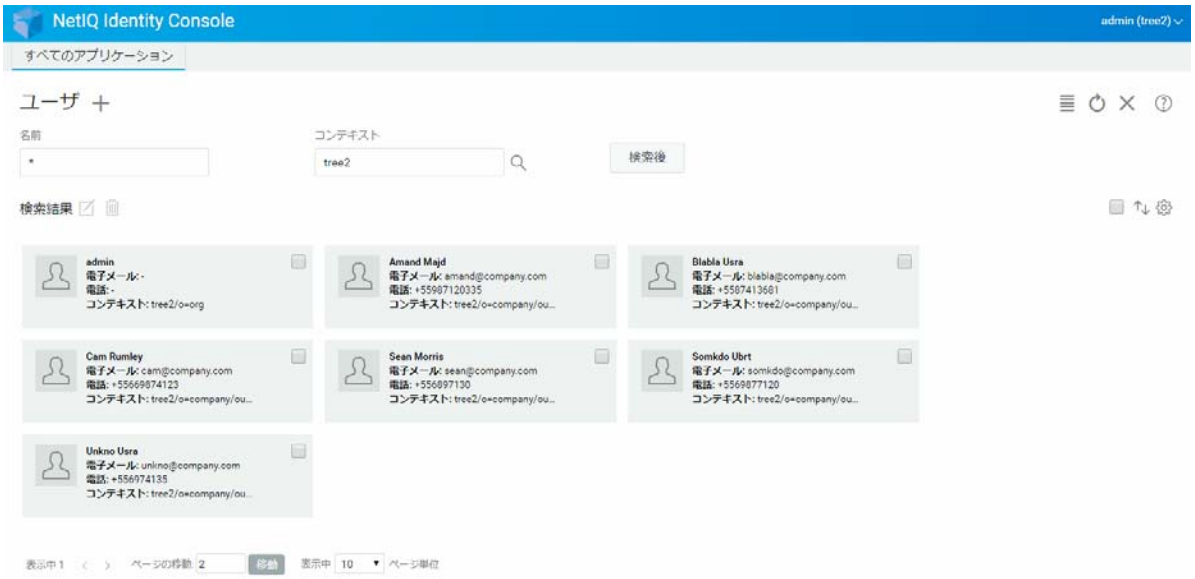
1 アカウントの有効期限を設定する必要のあるユーザを選択し、アイコンをクリックします。

2 [**[ユーザの変更]**] ページの [**[制限]**] タブをクリックします。

3 [**[ログイン制限]**] タブを展開し、[**[アカウントの有効期限]**] チェックボックスをオンにし、[**[有効期限]**] を指定します。

4 保存 アイコンをクリックします。

図 5-7 アカウントの有効期限の設定

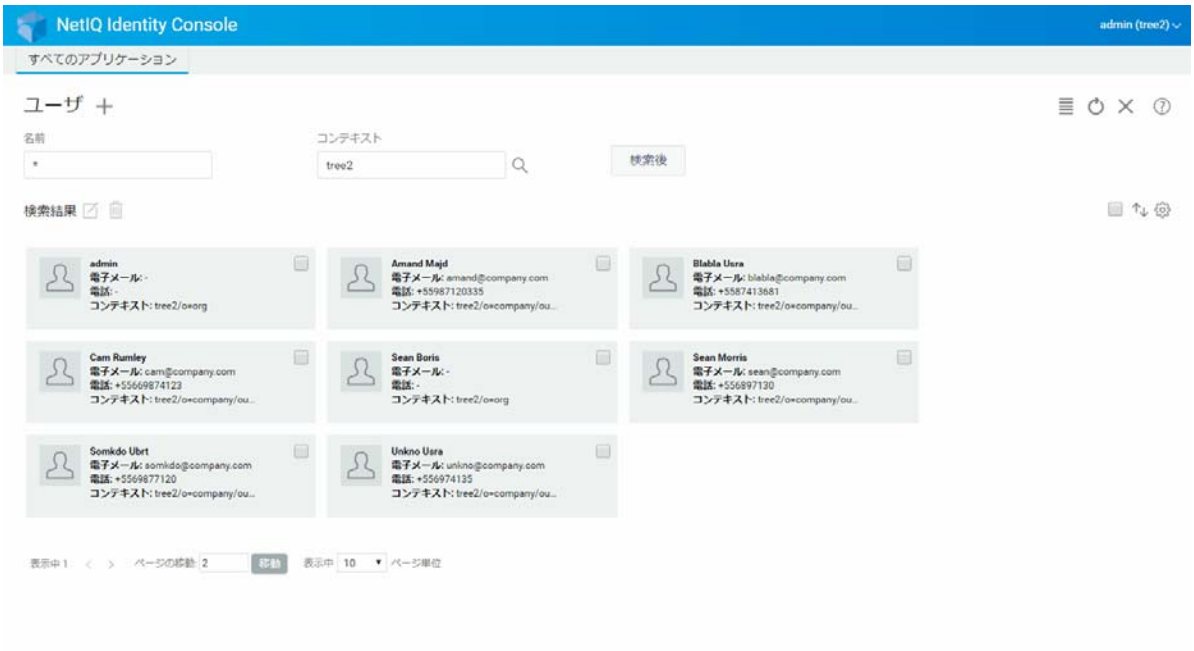


不正侵入者ロックアウトの確認とクリア

Identity Console Web ポータルを使用して、ユーザアカウントの不正侵入者ロックアウトの詳細を表示することができます。不正侵入者ロックアウトの詳細を表示するには :

1. 不正侵入者ロックアウトの詳細を確認する必要のあるユーザを選択し、アイコンをクリックします。
2. [**[ユーザの変更]**] ページの [**[制限]**] タブをクリックします。
3. [**[不正侵入者ロックアウト]**] タブを展開し、不正侵入者ロックアウトの詳細を表示します。
4. 次に、[**[ロックアウトのクリア]**] タブを選択して、ロックのクリア ボタンをクリックします。
5. 保存 ボタンをクリックします。

図5-8 不正侵入者ロックアウトの確認とクリア



6 グループを管理する

グループには、通常、多数のメンバーが含まれています。グループを作成したユーザは、自動的にグループの所有者になります。グループ管理機能を使用すると、次の操作を実行できます。

グループオブジェクトの使用方法と設定方法の詳細については、『*NetIQ eDirectory 9.2 管理ガイド* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)』を参照してください。

グループの作成

グループを作成するには :

1 Identity Console のランディングページから、[**[グループ管理]**] オプションをクリックします。

2 ＋アイコンをクリックします。

3 [グループの作成] ページで、次の詳細を入力します。

- グループ名を指定します
- コンテキストを指定します

新しいグループを dynamicGroup クラスのダイナミックグループにするには、[**[ダイナミックグループ]**] を選択します。それ以外の場合、グループはスタティックグループとして作成されます。

新しいグループをネストされたグループにするには、[**[ネストされたグループ]**] を選択します。これにより、補助クラス nestedGroupAux でグループが作成されます。

注 : スタティックグループをダイナミックグループまたはネストされたグループに変換するには、オブジェクトを変更するで説明されている手順に従います。これにより、選択したグループオブジェクトが、それぞれ dynamicGroupAux クラスまたは nestedGroupAux クラスに属するように拡張されます。

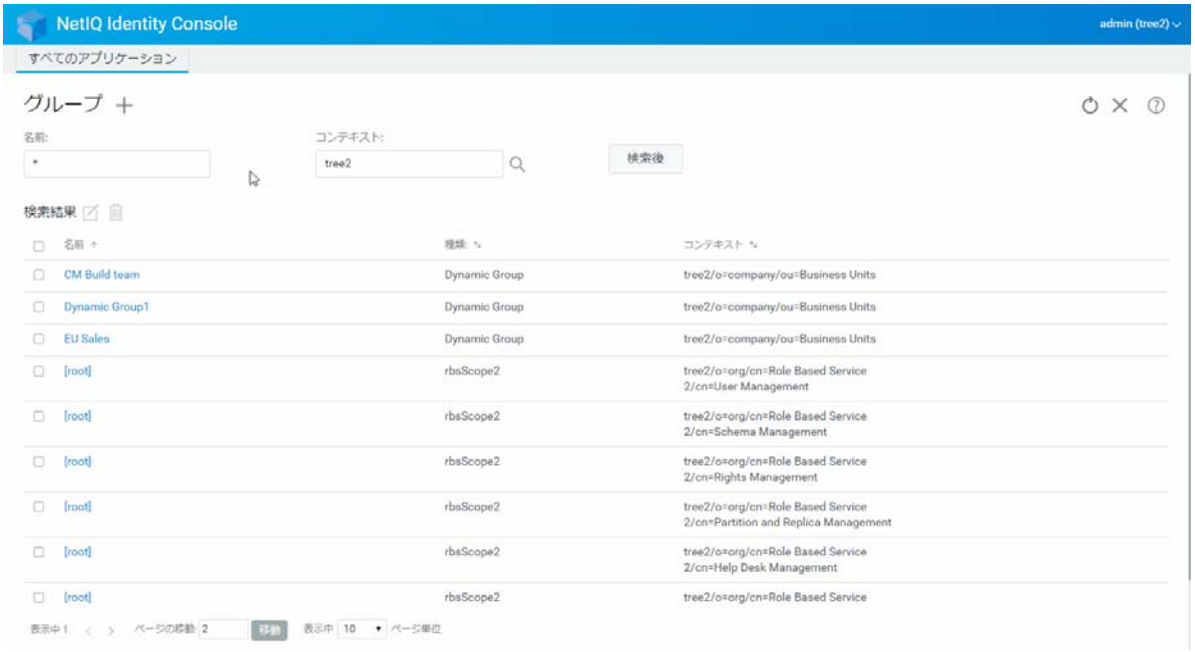
グループはネストかダイナミックのいずれかにすることができます。ネストおよびダイナミックの両方であるグループを作成することはできません。

---

4 必要な詳細を指定したら、作成 ボタンをクリックします。

5 グループが作成されたことを示す確認メッセージが表示されます。

図 6-1 グループの作成



グループの削除

グループを削除するには :

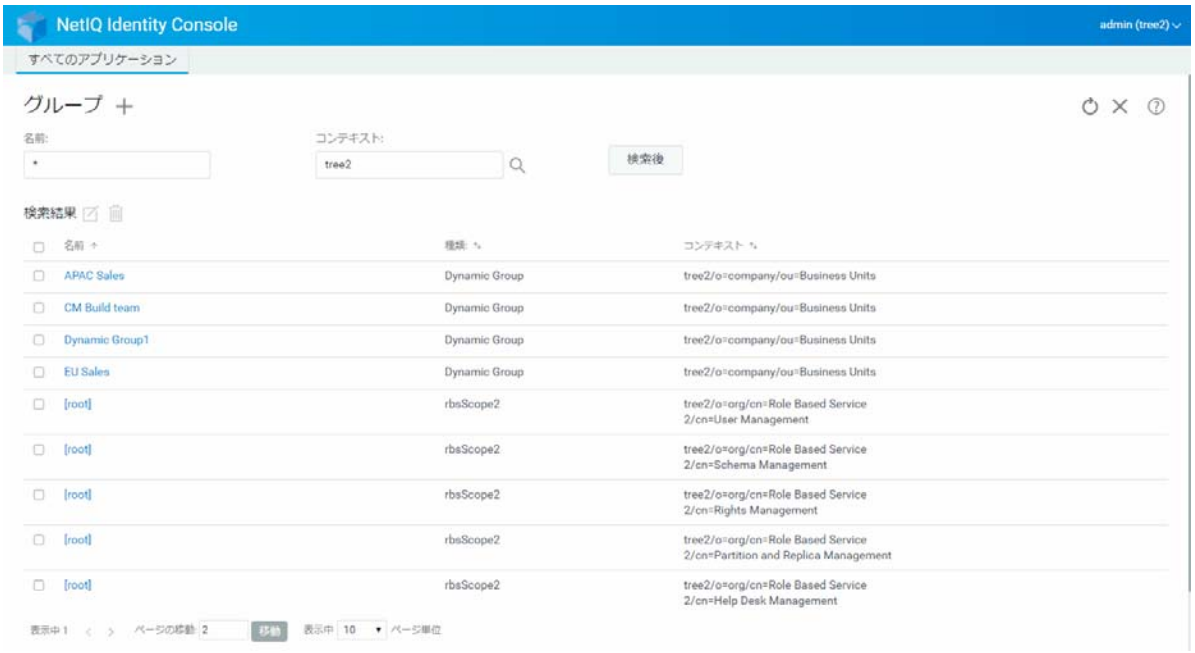
1 Identity Console のランディングページから、[**[グループ管理]**] オプションをクリックします。

2 グループの名前とコンテキストを指定するか、検索機能を使用して特定し、検索後 ボタンをクリックします。

3 削除する必要があるグループを選択し、🗑アイコンをクリックします。

4 グループが削除されたことを示す確認メッセージが表示されます。

図 6-2 グループの削除



グループの変更

グループを変更するには :

1 Identity Console のランディングページから、[**[グループ管理]**] オプションをクリックします。

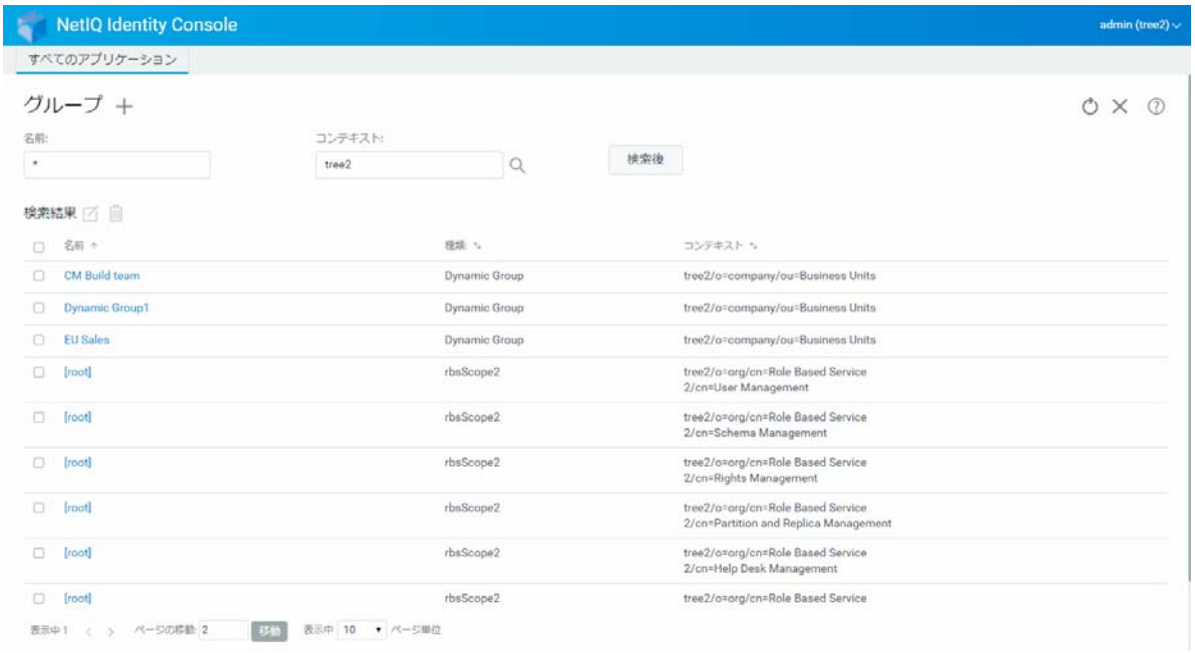
2 グループの名前とコンテキストを入力して、検索後 ボタンをクリックします。

3 変更する必要があるグループを選択し、アイコンをクリックします。

4 必要な変更を加えてから、保存 ボタンをクリックします。

5 グループが変更されたことを示す確認メッセージが表示されます。

図6-3 グループの変更



グループメンバーの追加または変更

グループメンバーを追加または変更するには :

1 Identity Console のランディングページから、[**[グループ管理]**] オプションをクリックします。

2 グループの名前とコンテキストを入力して、検索後 ボタンをクリックします。

3 グループを選択して、アイコンをクリックします。

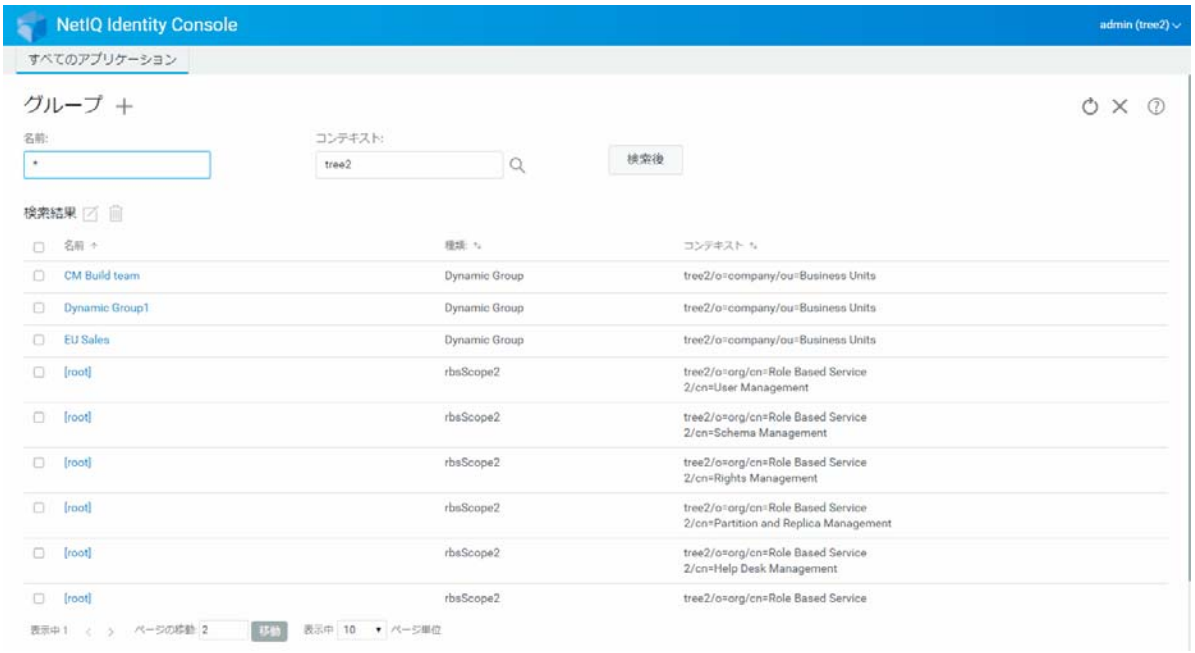
4 [**[グループの変更]**] ページの [**[メンバー]**] タブをクリックします。

5 グループに新しいメンバーを追加するには、アイコンを使用します。グループからメンバーを削除する場合は、アイコンをクリックします。

6 変更を行った後、保存 ボタンをクリックします。

7 グループが変更されたことを示す確認メッセージが表示されます。

図 6-4 グループメンバーの追加または変更

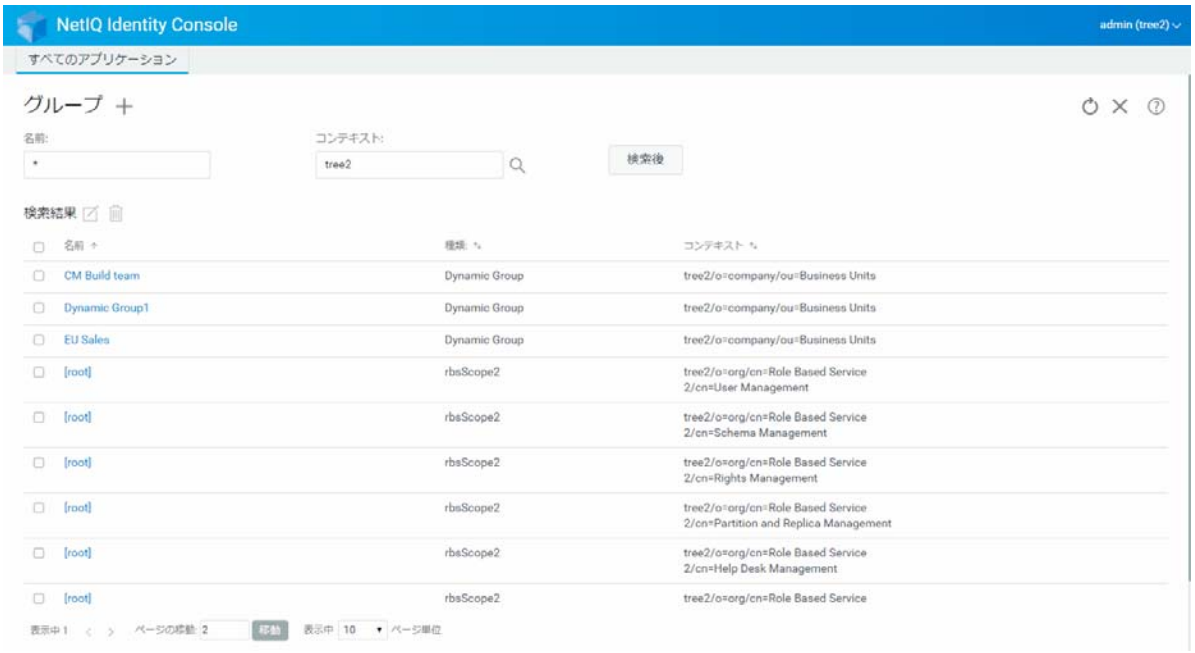


グループの検索

グループを検索するには :

1. Identity Console のランディングページから、[**[グループ管理]**] オプションをクリックします。
2. グループを検索するときは、名前を指定するか、名前とコンテキストの両方を指定することができます。
3. 必要な詳細を指定したら、検索後 アイコンをクリックします。

図6-5 グループの検索


NetIQ Identity Console
admin (tree2)
すべてのアプリケーション
グループ
名前:
*
コンテキスト:
tree2
検索後
検索結果
名前
種類:
コンテキスト
CM Build team
Dynamic Group
tree2/o=company/ou=Business Units
Dynamic Group1
Dynamic Group
tree2/o=company/ou=Business Units
EU Sales
Dynamic Group
tree2/o=company/ou=Business Units
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=User Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Schema Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Rights Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Partition and Replica Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Help Desk Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service
表示中 1
ページの移動: 2
移動
表示中 10
ページ単位

7 オブジェクトの管理

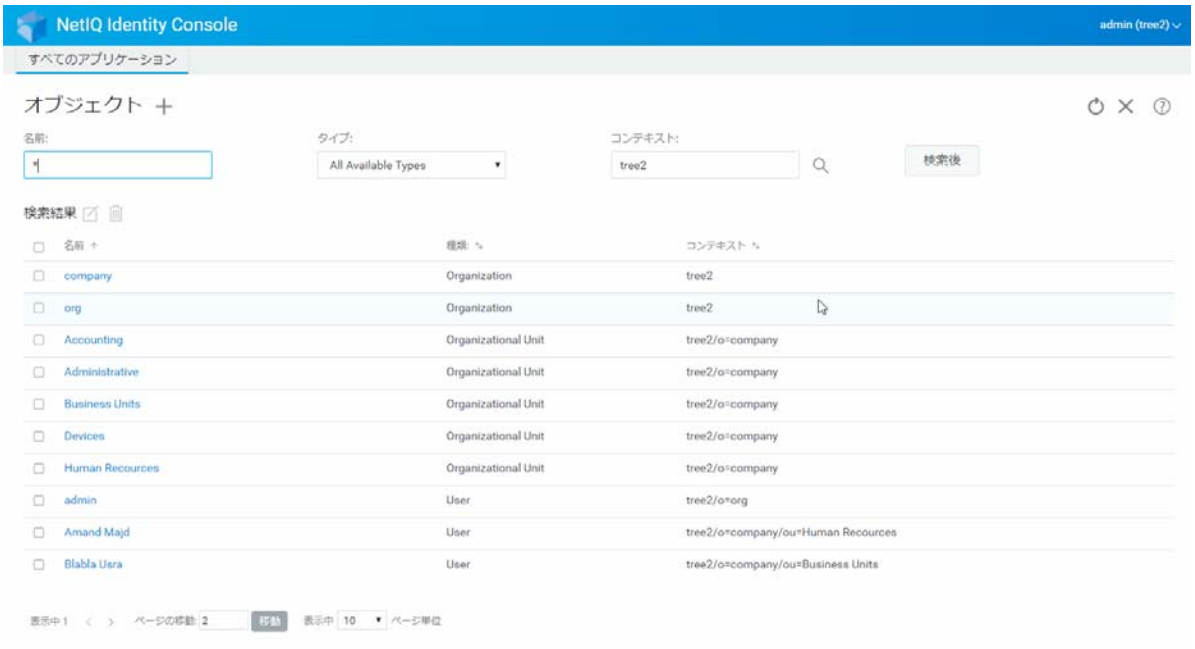
Identity Console では、データストア内のさまざまなオブジェクトを管理できます。このモジュールを使用して、オブジェクトの作成、変更、削除、および検索を行うことができます。

オブジェクトを作成する

新しいオブジェクトを作成するには :

1. Identity Console のランディングページから、[**[オブジェクト管理]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [オブジェクトの作成] ページで、次の詳細を入力します。
   - オブジェクト名を指定します
   - タイプを指定します
   - コンテキストを指定します
4. 必要な詳細をすべて入力したら、[**[次へ]**] > [**[作成]**] をクリックします。
5. オブジェクトが作成されたことを示す確認メッセージが表示されます。

図 7-1 オブジェクトの作成

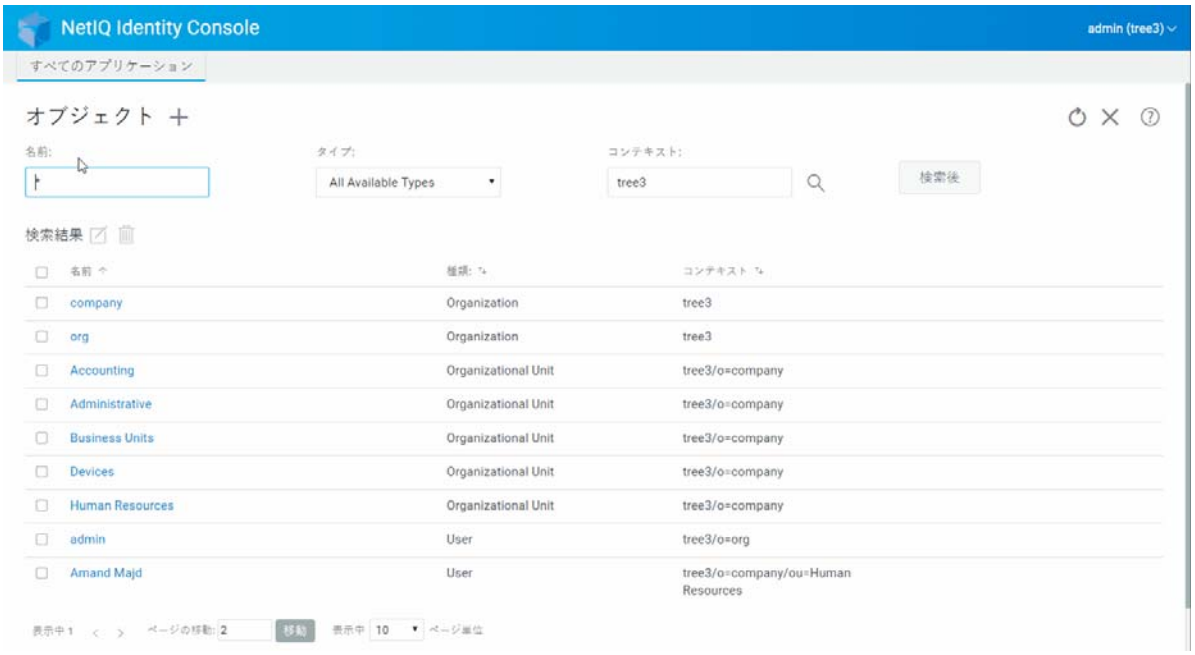


オブジェクトの削除

オブジェクトを削除するには :

1. Identity Console のランディングページから、[**[オブジェクト管理]**] オプションをクリックします。
2. オブジェクトの名前、タイプ、およびコンテキストを指定するか、検索機能を使用して特定し、検索後 ボタンをクリックします。
3. 検索リストからオブジェクトを選択し、アイコンをクリックします。
4. オブジェクトが削除されたことを示す確認メッセージが表示されます。

図7-2 オブジェクトの削除



オブジェクトを変更する

オブジェクトを変更するには :

1 Identity Console のランディングページから、[**[オブジェクト管理]**] オプションをクリックします。

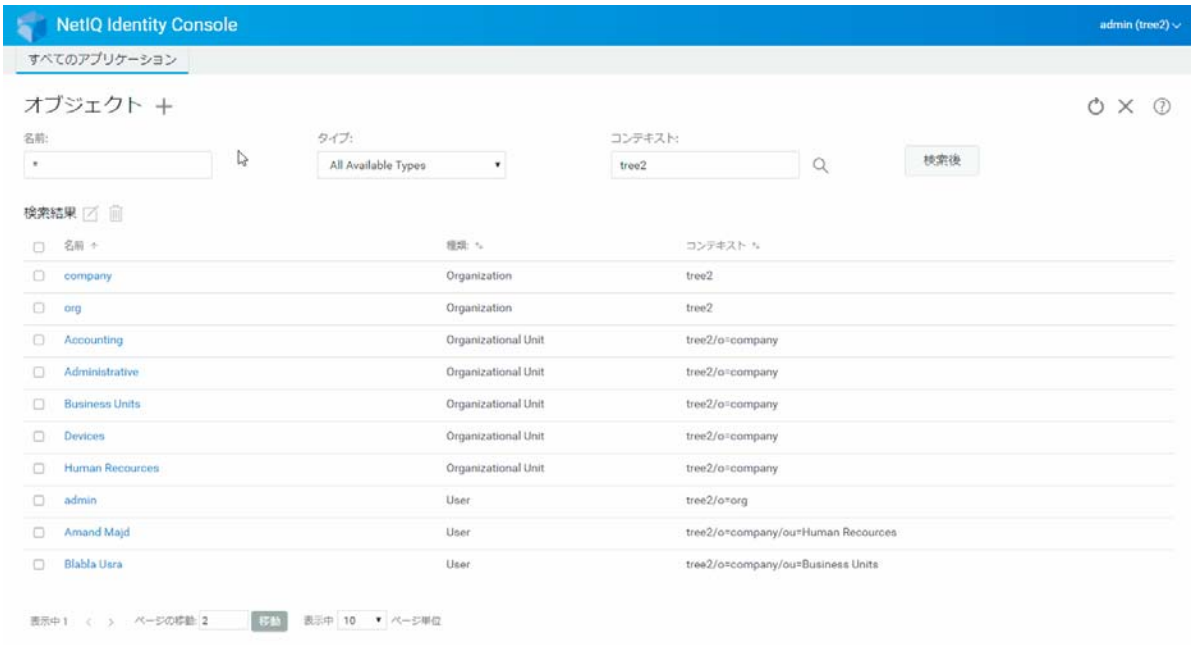
2 オブジェクトの名前、タイプ、およびコンテキストを入力し、検索後ボタンをクリックします。

3 検索リストからオブジェクトを選択し、アイコンをクリックします。

4 必要な変更を加えてから、保存ボタンをクリックします。

5 オブジェクトが変更されたことを示す確認メッセージが表示されます。

図7-3 オブジェクトの変更

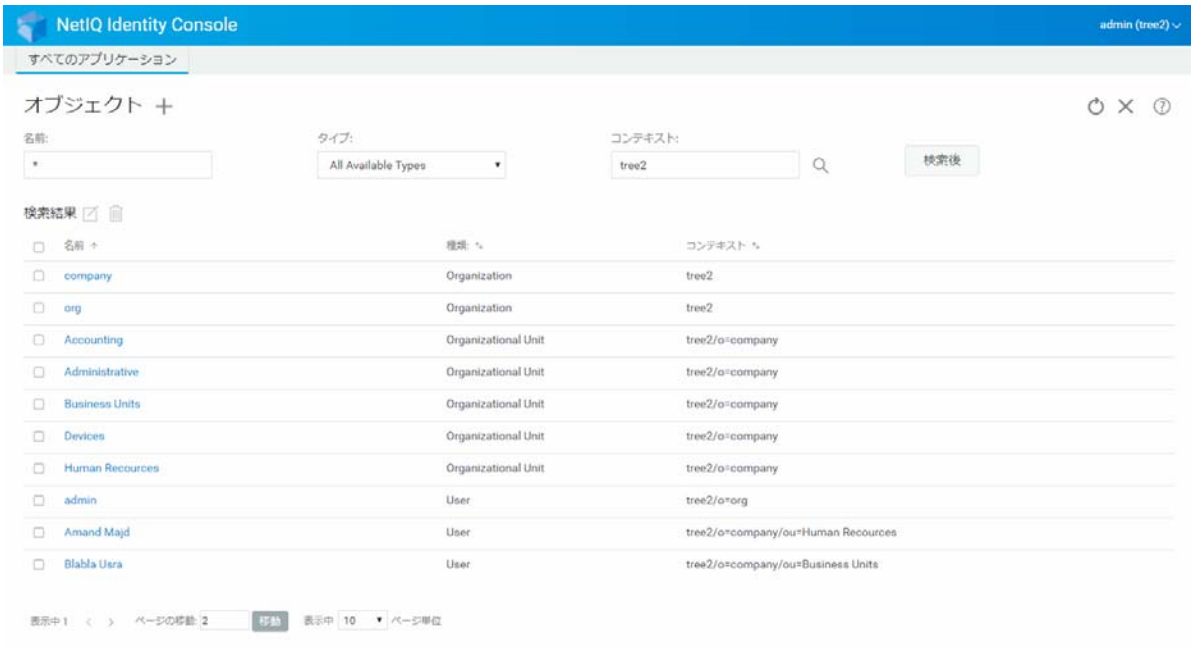


オブジェクトの検索

オブジェクトを検索するには :

1. Identity Console のランディングページから、[**[オブジェクト管理]**] オプションをクリックします。
2. オブジェクトを検索するときは、名前を指定するか、名前、タイプ、およびコンテキストを指定することができます。
3. 必要な詳細を指定したら、検索後 ボタンをクリックします。

図7-4 オブジェクトの検索



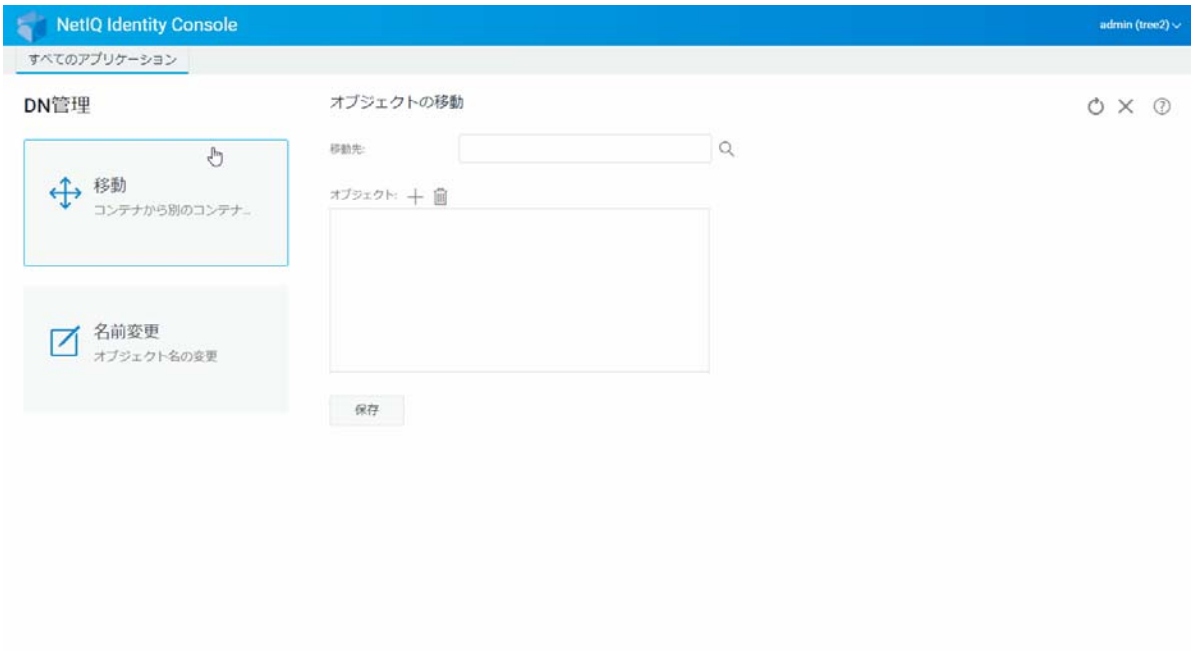
オブジェクトの移動

オブジェクトを移動するには :

1. Identity Console のランディングページから、[**[DN 管理]**] オプションをクリックします。
2. デフォルトでは、[**[オブジェクトの移動]**] オプションが選択されています。
3. [**[移動先]**] フィールドで、オブジェクトの移動先のコンテナを選択します。
4. ＋アイコンをクリックして、別のコンテナに移動するオブジェクトを追加します。

   選択したオブジェクトを削除するには、🗑アイコンをクリックします。
5. 保存 ボタンをクリックします。
6. オブジェクトが正常に移動されたことを示す確認メッセージが表示されます。

図7-5 オブジェクトの移動



オブジェクトの名前変更

オブジェクトの名前を変更するには :

1 Identity Console のランディングページから、[**[DN 管理]**] オプションをクリックします。

2 [**[オブジェクトの名前変更]**] オプションを選択します。

3 [**[オブジェクト名]**] フィールドで、検索機能を使用して、名前を変更する必要があるオブジェクトを特定します。

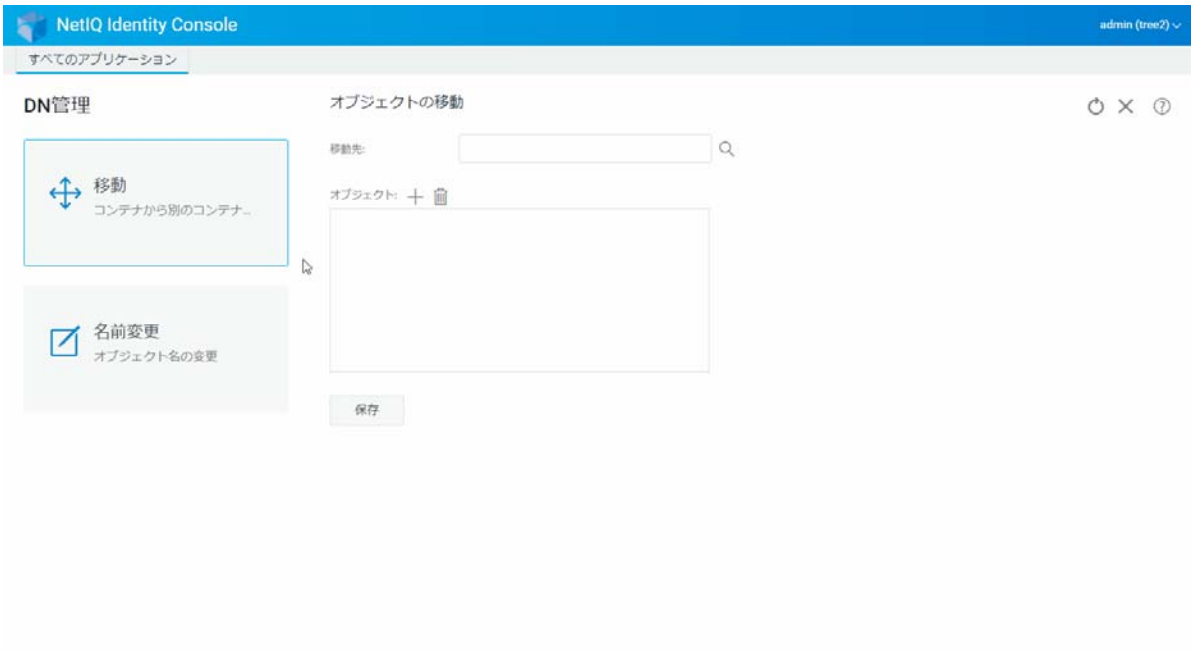
4 [**[新しい名前]**] フィールドに、オブジェクトの新しい名前のみを指定します。コンテキストは指定しないでください。

5 必要に応じて、[古い名前を保存] を選択します。

6 保存 ボタンをクリックします。

7 オブジェクトが正常に名前変更されたことを示す確認メッセージが表示されます。

図7-6 オブジェクトの名前変更



8 権利の管理

権利は、eDirectory のトラスティ権とトラスティの両方を意味します。ツリーを作成すると、デフォルトの権利割り当てによって、ネットワークに一般的なアクセスとセキュリティが提供されます。Identity Console では、権利に関連する次のようなタスクを実行できます。

- 53 ページの 「権利継承フィルタの変更」
- 54 ページの 「トラスティ権の変更」
- 55 ページの 「有効な権利の表示」

eDirectory オブジェクトの権利については、『*NetIQ eDirectory 9.2 管理ガイド* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)』を参照してください。

権利継承フィルタの変更

eDirectory には、個別の従属項目の権利継承をブロックするための、権利継承フィルタ (IRF) メカニズムが用意されています。

権利継承フィルタの詳細については、『*NetIQ eDirectory 9.2 管理ガイド* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)』を参照してください。

1. Identity Console のランディングページから、[**[権利の管理]**] オプションをクリックします
2. [**[権利継承フィルタ]**] を選択します。

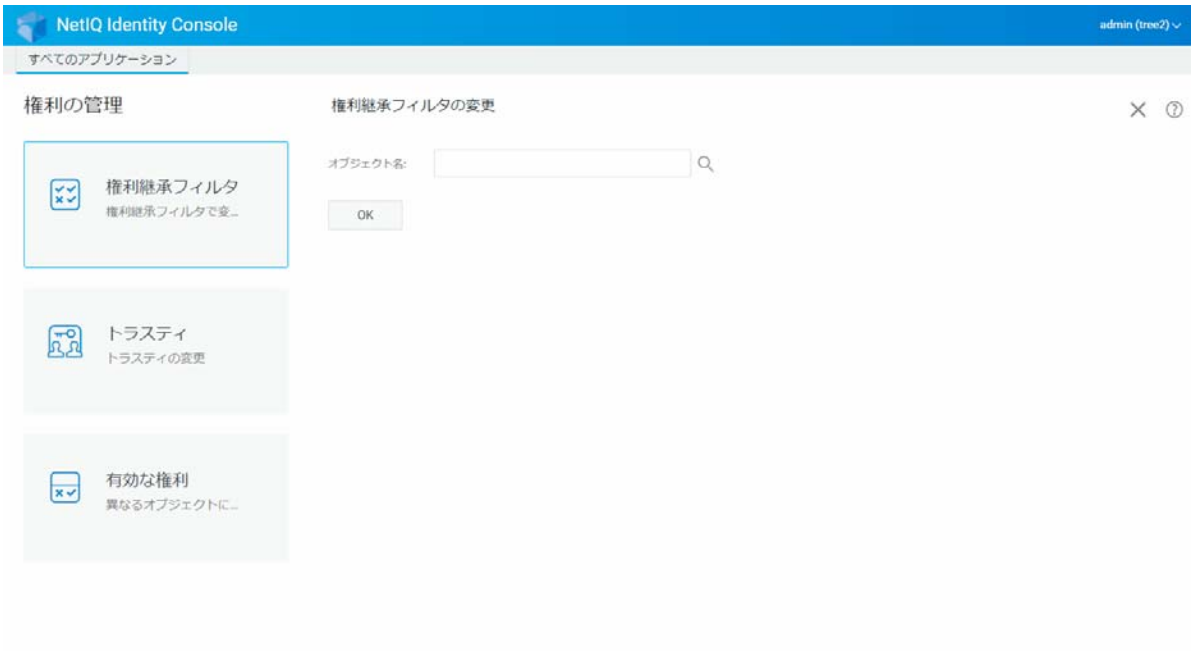
   注 : 権利継承フィルタはデフォルトで選択されています。

3. 権利継承フィルタを変更するオブジェクトのフルネームを指定するか、オブジェクトセレクタアイコンを使用してオブジェクトを検索し、[**[OK]**] をクリックします。

   これで、すでにオブジェクトに設定された権利継承フィルタのリストが表示されます。
4. [**[プロパティ]**] で、必要に応じて権利継承フィルタのリストを編集し、[**[適用]**] をクリックします。

   フィルタのリストを編集するには、オブジェクトの ACL プロパティに対するスーパバイザ権またはアクセス制御権を持っている必要があります。オブジェクトの継承された権利を全体的にブロックするフィルタは、オブジェクトのすべてのプロパティおよび個々のプロパティに対して設定できます。

図8-1 権利継承フィルタの変更



トラスティ権の変更

トラスティは、ディレクトリツリー内の別のオブジェクトに対する明示的な権利が許可されているオブジェクトです。特定のオブジェクトのトラスティリストを変更するには、次を実行します。

1 Identity Console のランディングページから、[**[権利の管理]**] オプションをクリックします

2 [**[トラスティ]**] を選択します。

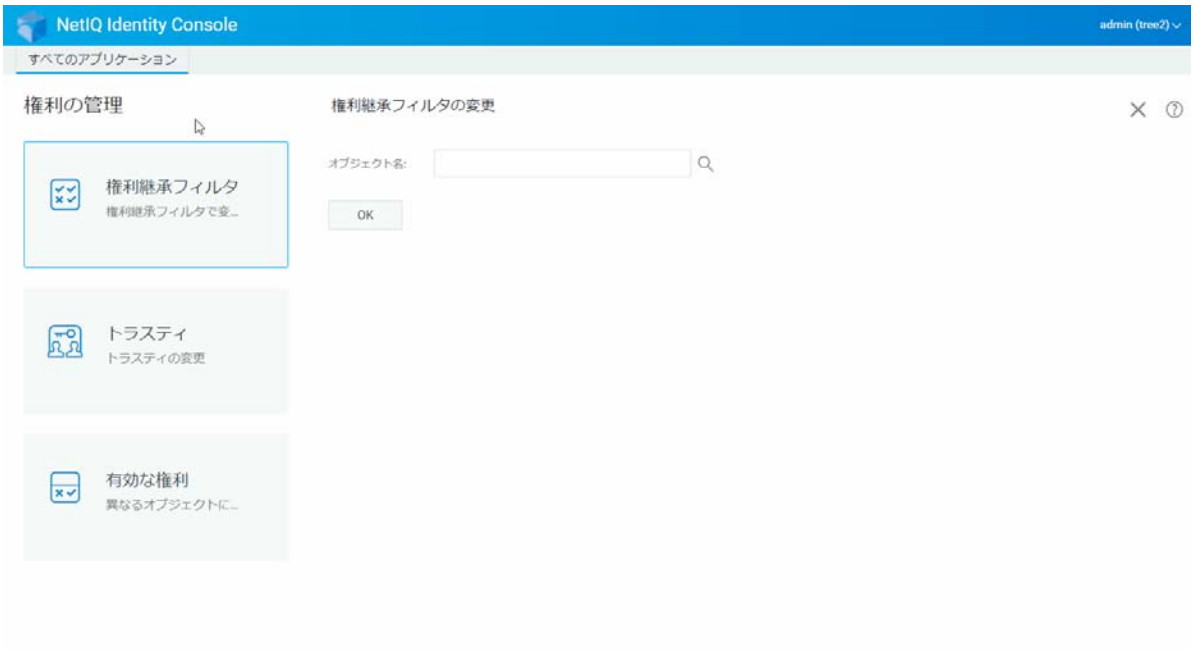
3 トラスティリストを表示するオブジェクトの名前を指定するか、オブジェクトセレクタアイコンを使用してオブジェクトを検索し、[**[OK]**] をクリックします。

これにより、オブジェクトに現在割り当てられているトラスティのリストが表示されます。

4 必要に応じてトラスティリストを変更して、[**[OK]**] をクリックします。

- トラスティを追加するには、アイコンをクリックします。
- チェックボックスを選択してアイコンをクリックすると、トラスティが削除されます。
- トラスティに割り当てられている権利は、そのトラスティの [**[割り当てられた権利]**] リンクを選択して変更します。

図8-2 トラスティ権の変更



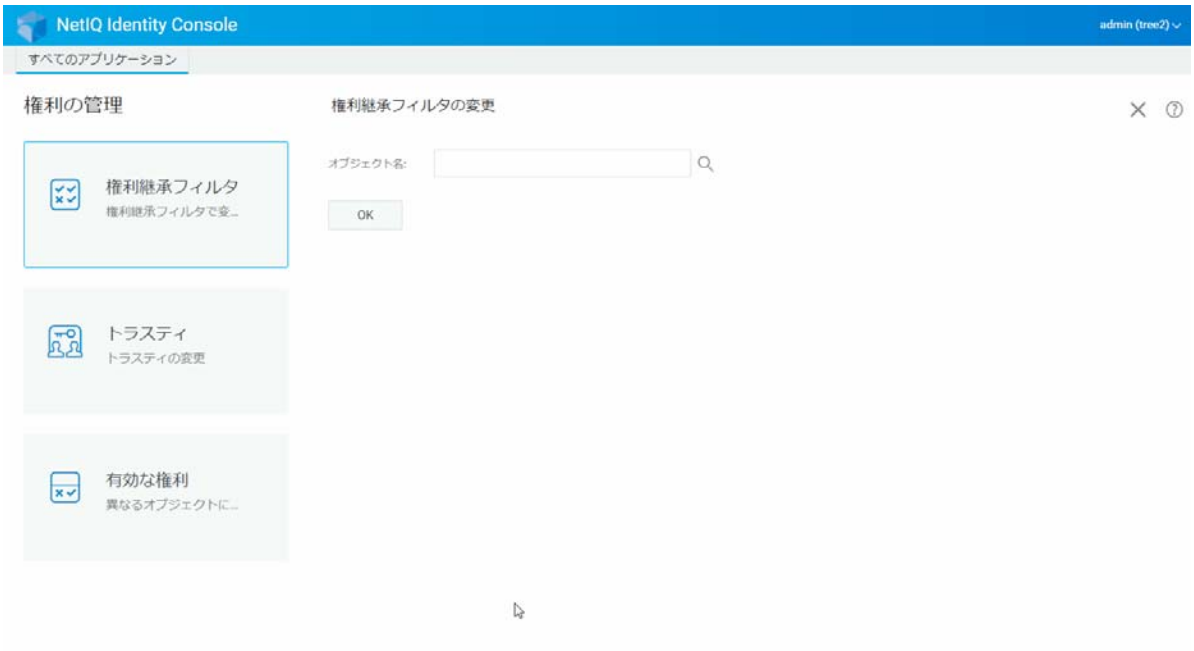
有効な権利の表示

有効な権利とは、ディレクトリツリー内のいずれかの場所でオブジェクトが持つ、明示的な権利と継承した権利の組み合わせです。あるオブジェクトが持つ、別のオブジェクトに対する有効な権利を表示するには、次を実行します。

1. Identity Console のランディングページから、[**[権利]** の管理] オプションをクリックします
2. [**[有効な権利]**] を選択します。
3. 権利を表示するトラスティの名前を指定するか、オブジェクトセレクタアイコンを使用してオブジェクトを検索し、[**[OK]**] をクリックします。
4. [オブジェクト名] フィールドで、トラスティの有効な権利を表示するオブジェクトの名前を指定します。

   eDirectory では有効な権利が計算され、[**[有効な権利]**] フィールドに表示されます。

図8-3 有効な権利の表示



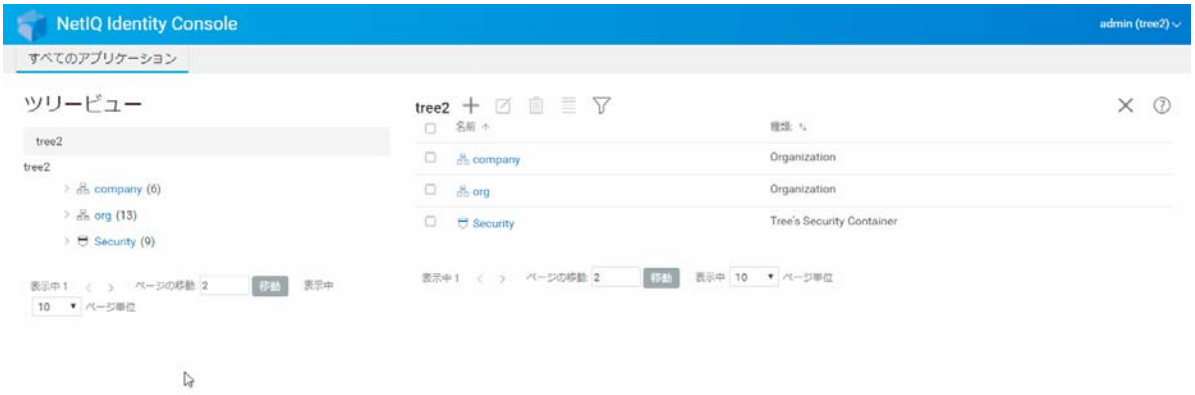
9 ツリービュー

ツリービューでは、ディレクトリツリーをブラウズして、ツリー内のさまざまなオブジェクトを作成、削除、および変更することができます。ツリービューには、ナビゲーションフレームとコンテンツフレームがあります。

ツリービューのナビゲーションフレーム

ツリービューでは、ナビゲーションフレームにディレクトリ構造が表示されます。ナビゲーションフレームには、ボリューム (ファイルシステム) やオブジェクトなどのコンテナが表示されます。ナビゲーションフレームの下に表示されるすべてのオプションは、クリックすることにより、ディレクトリ構造をブラウズできます。デフォルトでは、ナビゲーションフレームにはコンテナごとに最大 10 個の従属オブジェクトが表示されますが、ツリービューのナビゲーションフレームパネルの下で、この設定を変更することができます。

図 9-1 *ツリービューのナビゲーションフレーム*



ツリービューのコンテンツフレーム

ナビゲーションフレームでコンテナオブジェクトの 1 つを選択すると、そのコンテナに含まれるすべてのオブジェクトがコンテンツフレームに表示されます。コンテンツフレームには、ディレクトリオブジェクトが実際に表示され、変更することができます。コンテンツフレームのヘッダには、いくつかの利用可能なアクションがあります。

タイトルバー : コンテンツフレームのタイトルバーには、現在選択されているコンテナオブジェクトの名前が表示されます。

オブジェクトリストヘッダ : オブジェクトリストヘッダでは、次のような操作ができます。

- **[追加]**: アイコンをクリックすると、新しいオブジェクトが追加されます。
- **[変更]**: オブジェクトを選択してアイコンをクリックすると、選択したオブジェクトのプロパティブックが開き、属性を変更することができます。複数のオブジェクトをまとめて変更することはできません。
- **[削除]**: オブジェクトを選択して、アイコンをクリックすると、選択したオブジェクトが削除されます。複数のオブジェクトをまとめて削除することができます。リーフ以外のオブジェクトは削除できません。
- **[アクション]**: オブジェクトを選択して、アイコンをクリックすると、選択したオブジェクトに対してサポートされているタスクのドロップダウンメニューが表示されます。タスクを実行するには、ドロップダウンメニューからタスクを選択して、必要な情報を入力します。
- **[オブジェクト数]**: ツリービューでは、ページの下部に、現在のページにあるオブジェクトの数が表示されます。デフォルトでは、コンテンツフレームにはコンテナごとに最大 20 個の従属オブジェクトが表示されますが、この設定は変更できます。
- **[すべて選択]**: ヘッダにあるチェックボックスは、現在のページのオブジェクトを「すべて選択する」チェックボックスとして機能します。
- **[ソート]**: ［**[名前]**］列と［**[タイプ]**］列の両方がソート可能です。これらのいずれかをクリックすると、オブジェクトのソート方法が、アルファベットの昇順と降順とで切り替わります。
- **[検索フィルタ]**: アイコンをクリックすると、フィルタのポップアップウィンドウが表示されます。このオプションを使用すると、オブジェクトリストに表示されるオブジェクトを制限するフィルタを作成できます。必要に応じて、オブジェクトタイプおよびオブジェクト名をフィルタすることができます。

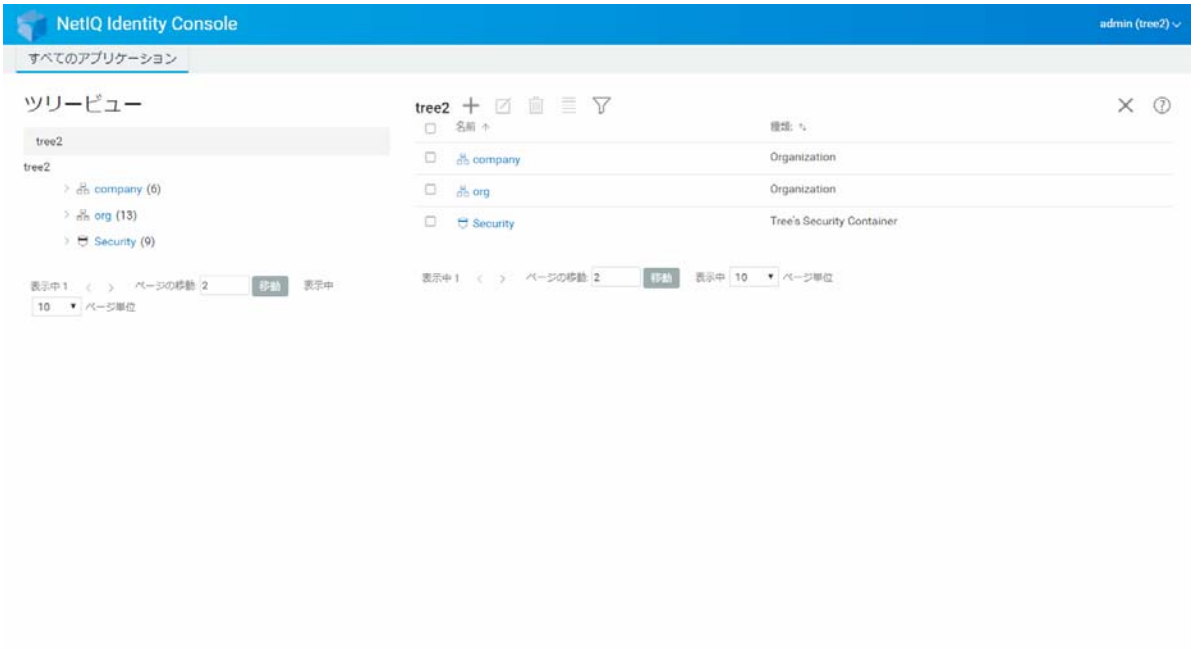
  オプションを選択すると、ほとんどすべてのオブジェクト属性を使用してフィルタを作成できる、［詳細フィルタ］ダイアログが開きます。詳細については、26 ページの 「詳細検索の設定」を参照してください。

1 つのオブジェクトに対してアクションを実行するには、そのオブジェクトのチェックボックスをオンにし、オブジェクトリストのヘッダからアクションアイコンを選択します。現在参照中のコンテナでアクションを実行するには、(現在レベルの) オブジェクトを選択します。このオプションを使用すると、次のアクションを実行できます。

- 53 ページの 「権利継承フィルタの変更」
- 54 ページの 「トラスティ権の変更」
- 67 ページの 「オブジェクトの拡張」
- 50 ページの 「オブジェクトの名前変更」

- パスワードの設定
- 55 ページの 「有効な権利の表示」

図 9-2 *ツリービューのコンテンツフレーム*



10 スキーマの管理

ディレクトリスキーマでは、ツリー内に作成できるオブジェクトのタイプ (ユーザ、プリンタ、グループなど) を定義します。また、オブジェクトの作成時にどの情報が必須またはオプションであるかを定義します。Identity Console では、次のようなスキーマ関連のタスクが提供されます。

属性を作成する

属性のカスタムタイプを独自に定義し、それをオプション属性として既存のオブジェクトクラスに追加できます。ただし、必須属性を既存のクラスに追加することはできません。属性を作成するには、次を実行します。

1. Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [属性の作成] ページで、次の詳細を入力します。
   - 属性名
   - ASN1 ID (オプション)
   - 構文
   - 属性フラグ
4. 必要な詳細をすべて入力したら、作成 ボタンをクリックします。
5. 属性が作成されたことを示す確認メッセージが表示されます。

図 10-1 属性を作成する

クラスを作成する

[**[スキーマ管理]**]オプションを使用すると、独自のクラスを定義できます。次に、そのクラスで定義されているプロパティを使用して個々のオブジェクトを拡張できます。クラスを作成するには :

1 Identity Console のランディングページから、[**[スキーマ管理]**]オプションをクリックし、[**[クラス]**] を選択します。

2 ＋アイコンをクリックします。

3 [属性の作成] ページで、次の詳細を入力します。

- クラス名
- ASN1 ID (オプション)
- クラスフラグ : 次のいずれかのクラスフラグを選択します。
  - **有効なクラス** : オブジェクトの作成に使用できる有効なクラスを作成する場合は、このフラグを設定します。
  - **有効でないクラス** : 属性のグループのプレースホルダとして使用します。有効でないクラスは、オブジェクトの作成には使用できませんが、他のクラスの属性の継承元クラスとして指定することはできます。たとえば、Person クラスは有効でないクラスであり、その属性は User クラスによって継承されます。
  - **補助クラス** : クラス全体ではなく個々のオブジェクトのみと関連付けることができる属性の集まりです。

- **コンテナクラス :** コンテナクラスに指定する場合は、このフラグを設定します。コンテナクラスを使用して作成したオブジェクトは、コンテナオブジェクトになります (OU など)。リーフオブジェクトクラスについては、このフラグを設定しないでください。

注 : [有効なクラス] または [有効でないクラス] を選択した場合は、[スーパークラス] の値も指定する必要があります。[補助クラス] を選択した場合、[スーパークラス] はオプションになります。

---

4 必要な詳細をすべて入力したら、[**[次へ]**] をクリックします。

5 次の画面で、オプション属性、必須属性、およびネーミング属性を選択し、[**[OK]**] をクリックします。

6 クラスが作成されたことを示す確認メッセージが表示されます。

クラスへの属性の割り当て

組織の情報に関するニーズが変わった場合、またはツリーのマージを準備している場合に、オプション属性を既存のクラスに追加できます。既存のクラスに属性を追加するには、次を実行します。

注 : 必須属性は、クラスの作成時にのみ定義できます必須属性とは、オブジェクトの作成時に指定する必要のある属性です。

---

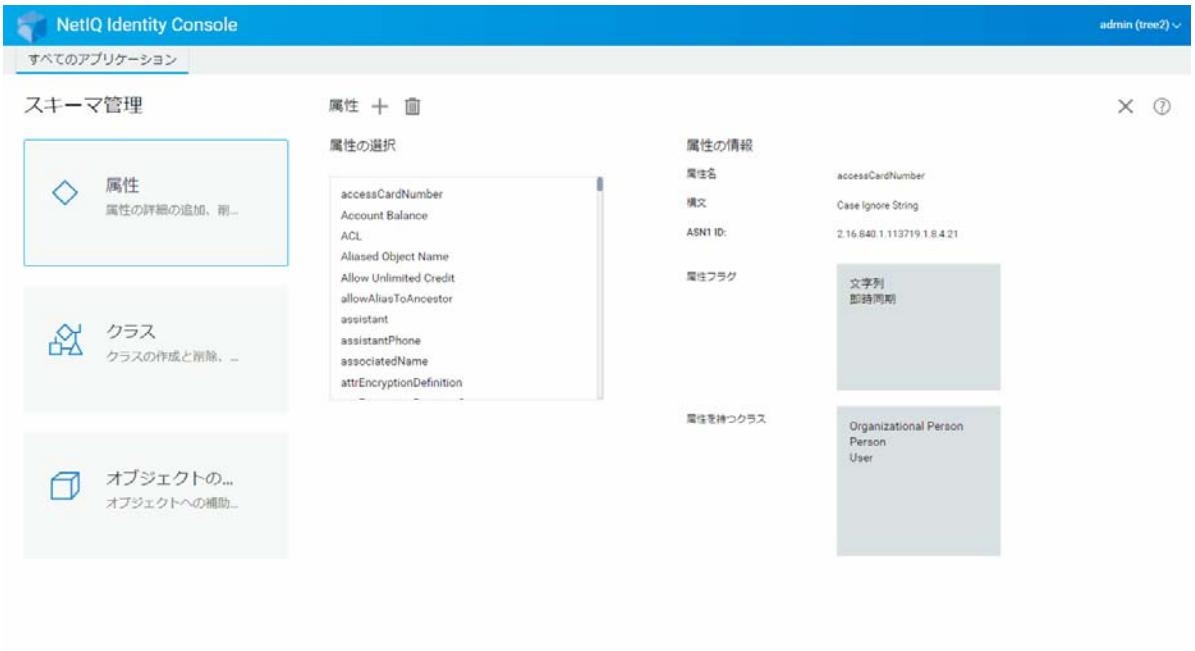
1 Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックし、[**[クラス]**] を選択します。

2 [**[クラスの選択]**] の下に表示されているクラスをクリックします。

3 画面の右側に、対応するクラス情報が表示されます。

4 [┼属性 **[] オプションの隣にある]** ボタンをクリックし、追加する属性を選択して、[**[追加]**] > [**[保存]**] をクリックします。

図 10-2 クラスへの属性の割り当て

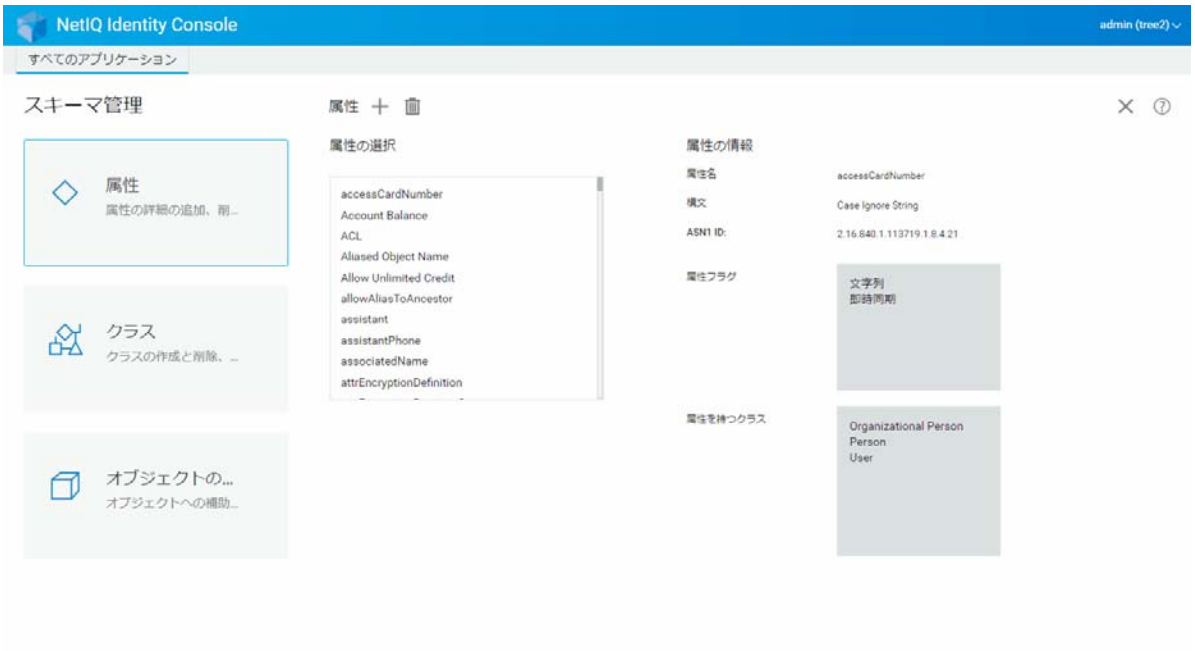


属性情報を表示する

属性を使用する構文、フラグ、クラスなど、属性の構造上の詳細を表示できます。属性情報を表示するには、次を実行します。

1. Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックし、[**[属性]**] を選択します。
2. [**[属性の選択]**] の下に表示されている属性をクリックします。
3. 画面の右側に、対応する属性情報が表示されます。

図 10-3 属性情報を表示する



属性を削除する

使用されていない属性は、その属性が eDirectory ツリーのベーススキーマの一部でない限り、削除できます。これは、2 つのディレクトリツリーをマージした後、または属性が古くなった場合に有効です。属性を削除するには、次を実行します。

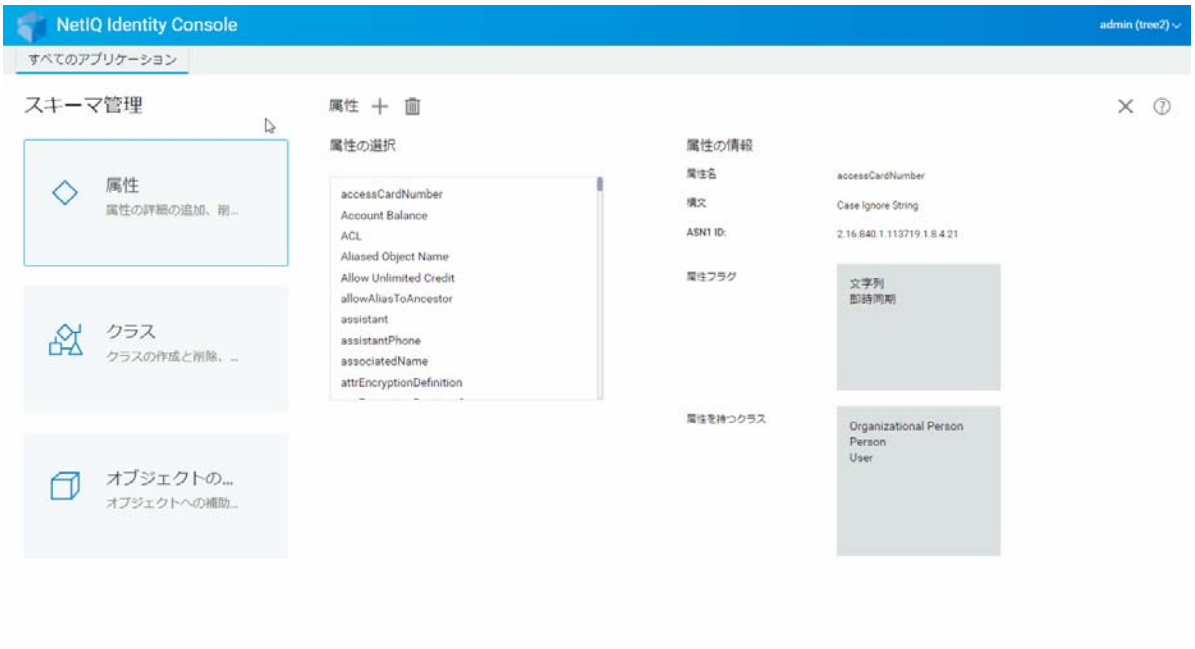
1 Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックし、[**[属性]**] を選択します。

2 削除する属性を [**[属性の選択]**] リストで選択し、アイコンをクリックします。

注 : アイコンは、削除可能な属性を選択した場合にのみ有効になります。

3 **[OK]** をクリックして、削除を確認します。

図 10-4 属性を削除する



クラスを削除する

使用されていないクラスは、そのクラスが eDirectory ツリーのベーススキーマの一部でない限り、削除できます。Identity Console では、ローカルにレプリカ作成されたパーティションで現在使用されているクラスは削除できません。クラスを削除するには、次を実行します。

1 Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックし、[**[クラス]**] を選択します。

2 削除するクラスを [**[クラスの選択]**] リストで選択し、アイコンをクリックします。

注 : アイコンは、削除可能なクラスを選択した場合にのみ有効になります。

3 **[OK]** をクリックして、削除を確認します。

図 10-5 クラスを削除する

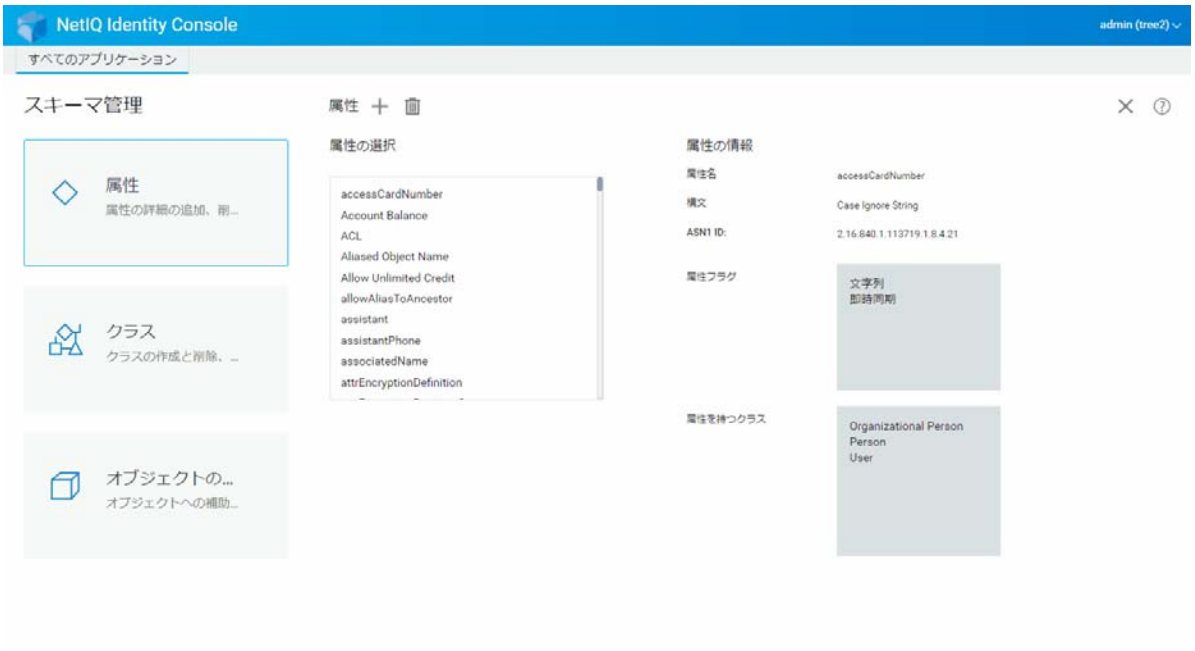
オブジェクトの拡張

オブジェクトを拡張するには、次の手順に従います。

1. Identity Console のランディングページから、[**[スキーマ管理]**] オプションをクリックし、[**[オブジェクト拡張]**] を選択します。
2. オブジェクトの名前を指定するか、オブジェクトセレクタを使用して拡張するオブジェクトを選択し、アイコンをクリックします。
3. アイコンをクリックし、補助クラスを選択して、[**[OK]**] をクリックします。

   注 : 選択した補助クラスに必須属性が関連付けられている場合、[**[必須属性]**] ポップアップウィンドウに必要な値を入力するように求めるメッセージが表示されます。
4. 補助クラスがオブジェクトに追加されたことを示す確認メッセージが表示されます。
5. オブジェクトから既存の補助クラスを削除するには、クラスを選択して、アイコンをクリックします。

図 10-6 オブジェクトの拡張



11 監査イベントの管理

この章では、Identity Console を使用してさまざまな監査イベントを管理する方法について説明します。この機能を使用して、NCP サーバの監査イベントを有効または無効にすることができます。

CEF 監査イベントの設定

1 ユーザ名とパスワードを使用して Identity Console にログインします。

2 [[監査]] を選択します。

3 監視する NCP サーバを選択してから、[[OK]] をクリックします。

注 : NCP サーバに対して CEF イベントを初めて有効にした後は、デフォルトでいくつかのイベントが選択されています。

---

4 CEF 監査イベントを設定します。

- **イベントの環境設定 :** 環境に必要な監査に基づいて、次のイベントを有効または無効にします。

注 : デフォルトでは、［イベントの環境設定］セクションの下に個々のイベントカテゴリが折りたたまれます。個々のイベントを選択するには、各カテゴリを展開できます。

オプション	説明
セキュリティイベント	イベントをログに記録するセキュリティイベントを選択します。メンバーの追加または削除、不正侵入者の検出、パスワード変更、ユーザの認証などのイベントをログに記録できます。
オブジェクトイベント	イベントをログに記録するオブジェクトイベントを選択します。オブジェクトの作成、削除、名前変更、移動、検索を行うイベントをログに記録できます。
属性イベント	イベントをログに記録する属性イベントを選択します。属性の読み込みと削除、属性値の追加、削除、比較を行うイベントをログに記録できます。
LDAP イベント	イベントをログに記録する LDAP イベントを選択します。

- **詳細設定 :** 詳細設定を使用して、次の操作を実行できます。
  - **Global:** 重複したエントリのグローバル設定を選択またはクリアすることができます。
    - **複製されたイベントを送信しない :** 他のサーバからの複製に起因する重複イベントの受信を停止する場合にこのオプションを選択します。
  - **ログイベントの値 :** イベントがテキストファイルに記録されます。サイズが 768 バイトを超えるイベントの値が「大きい値」と見なされます。どんなサイズのイベントでもログに記録できます。
    - **大きい値をログに記録 :** このオプションは、サイズが 768 バイトを超えるイベントをログに記録する場合に選択します。
    - **属性値のログ記録 :** 属性値を表示するにはこのオプションを選択します。これは、［**[値の追加]**］イベントと［**[値の削除]**］イベントにのみ適用されます。
    - **暗号化属性値のログ記録 :** 暗号化された属性値を表示するにはこのオプションを選択します。これは、［**[値の追加]**］イベントと［**[値の削除]**］イベントにのみ適用されます。

    注 : イベントサイズが 768 バイトサイズを超えている場合は、イベントの値が切り詰められてログファイルに保存されます。

CEF イベントタイプについて

イベントを次のカテゴリに記録するように、CEF を設定できます。

- セキュリティ
- オブジェクト

- 属性
- LDAP

次のデフォルトセットのイベントタイプを監査できます。

カテゴリ	イベントタイプ
セキュリティ	• ACL が変更されました • メンバーの追加 • メンバーの削除 • 不正侵入者が検出されました • ログインが無効化されました • ログインが有効化されました • ログイン • 同等セキュリティの変更 • 監査の環境設定 • パスワードの変更 • アカウントのロック解除 • ログアウト • 接続 • なりすまし • 認証 • パスワードの確認 • ログイン環境設定の変更 • 資格情報の照会
オブジェクト	• オブジェクトの作成 • オブジェクトの削除 • オブジェクトのリネーム • オブジェクトの移動 • DSA の読み取り • 検索
属性	• 属性の読み込み • 属性の削除 • 値の追加 • 値の削除 • 属性値の比較

カテゴリ	イベントタイプ
LDAP	• LDAP バインド • LDAP レスポンスのバインド • LDAP バインド解除 • LDAP 接続 • LDAP 検索 • LDAP 検索の応答 • LDAP 検索エントリの応答 • LDAP 追加 • LDAP 追加の応答 • LDAP 比較 • LDAP 比較の応答 • LDAP 変更 • LDAP レスポンスの変更 • LDAP 削除 • LDAP レスポンスの削除 • LDAP DN の変更 • LDAP DN レスポンスの変更 • LDAP 破棄 • LDAP 拡張操作 • LDAP システム拡張操作 • LDAP 拡張操作の応答 • LDAP サーバの環境設定の変更 • 不明な LDAP 操作 • LDAP パスワードの変更

CEF 監査フィルタの設定

CEF は、フィルタとイベント通知を使用して、特定のタイプのイベントが発生したとき、または、発生しなかったときにレポートを作成できます。1 つまたは複数の固有オブジェクトクラスまたは属性のイベントを、イベントタイプに応じてフィルタ処理することもできます。CEF は、生成されたすべてのイベントを eDirectory サーバで設定済みのフィルタに照らして評価し、それらのフィルタに一致するイベントのみをログに記録します。

このセクションでは、システムフィルタと通知の設定に必要な情報を提供します。

- 73 ページの 「除外フィルタを使用した eDirectory イベントのフィルタリング」
- 73 ページの 「CEF オブジェクトイベントのフィルタリング」
- 74 ページの 「CEF 属性イベントのフィルタリング」

除外フィルタを使用した eDirectory イベントのフィルタリング

[[除外フィルタ]] リンクをクリックして、イベントを生成する必要がないオブジェクトクラスと属性のためのフィルタを設定します。オブジェクトクラスと属性を選択できます。

不要な eDirectory イベントのフィルタを設定するには :

1. Identity Console で、ホームページから［ [監査]］を選択します。
2. 監視する NCP サーバを選択してから、［ [OK]］をクリックします。
3. ［ [詳細設定]］に移動し、［ [フィルタ]］の下の［ [除外フィルタ]］をクリックします。

   ［CEF 除外フィルタリング］ウィンドウが表示されます。
4. ［ [使用可能なオブジェクトクラス]］リストで、イベントを収集しないオブジェクトクラスを選択し、右矢印をクリックしてそれらを［ [選択されたオブジェクトクラス]］リストに移動します。
5. ［ [使用可能な属性]］リストで、任意の数の属性を選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。
6. [OK] をクリックします。

設定済みのフィルタを使用して、CEF 監査モジュールは、すべての選択済みオブジェクトクラスと属性に関するイベントの生成を停止します。

CEF オブジェクトイベントのフィルタリング

オブジェクト用のフィルタリングを設定して、特定のイベントのみを検索することができます。たとえば、誰かが eDirectory でユーザアカウントを作成したら通知が届くようにするには、新しいユーザオブジェクトの作成に関するイベントをログに記録するため、ユーザオブジェクトクラスを選択するフィルタを作成できます。

アカウントフィルタリングを設定するには、［オブジェクトイベント］リンクをクリックして、クラスを選択してから、［ [OK]］をクリックしてアプリケーションを終了します。

アカウント管理イベントのフィルタを設定するには :

1. Identity Console で、ホームページから［ [監査]］を選択します。
2. 監視する NCP サーバを選択してから、［ [OK]］をクリックします。
3. ［ [詳細設定]］に移動し、［ [フィルタ]］の下の［ [オブジェクトイベント]］をクリックします。

   ［CEF オブジェクトフィルタリング］ウィンドウが表示されます。
4. ［ [使用可能なオブジェクトクラス]］リストで、任意のオブジェクトクラスを選択し、右矢印をクリックしてそのオブジェクトクラスを［ [選択されたオブジェクトクラス]］リストに移動し、［ [OK]］をクリックします。

設定済みのフィルタを使用して、CEF 監査モジュールはすべての選択されたオブジェクトクラスに関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

CEF 属性イベントのフィルタリング

[**[属性イベント]**] リンクをクリックして、属性イベントのフィルタを設定します。たとえば、誰かが eDirectory で新しい属性値を追加したら通知が届くようにするため、新しい値の追加に関するイベントをログに記録するフィルタを作成できます。

属性イベントのフィルタを設定するには :

1. Identity Console で、ホームページから［ **[監査]**］を選択します。
2. 監視する NCP サーバを選択してから、［ **[OK]**］をクリックします。
3. ［ **[詳細設定]**］に移動し、［ **[フィルタ]**］の下の［ **[属性イベント]**］をクリックします。

   ［ **[属性設定のフィルタリング]**］ウィンドウが表示されます。
4. ［ **[使用可能なオブジェクトクラス]**］リストで、イベントを収集するオブジェクトクラスを選択し、右矢印をクリックしてそれらを［ **[選択されたオブジェクトクラス]**］リストに移動します。
5. ［ **[使用可能な属性]**］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

   注 : オブジェクトクラスを選択すると、そのオブジェクトクラスのすべての属性の属性イベントすべてが選択されます。この場合は、選択したオブジェクトクラスのすべての属性に関するすべての属性イベントを取得することになります。
6. ［ **[OK]**］をクリックします。

フィルタを設定すると、CEF 監査モジュールはすべての選択済みオブジェクトクラスと属性に関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

12 暗号化属性の管理

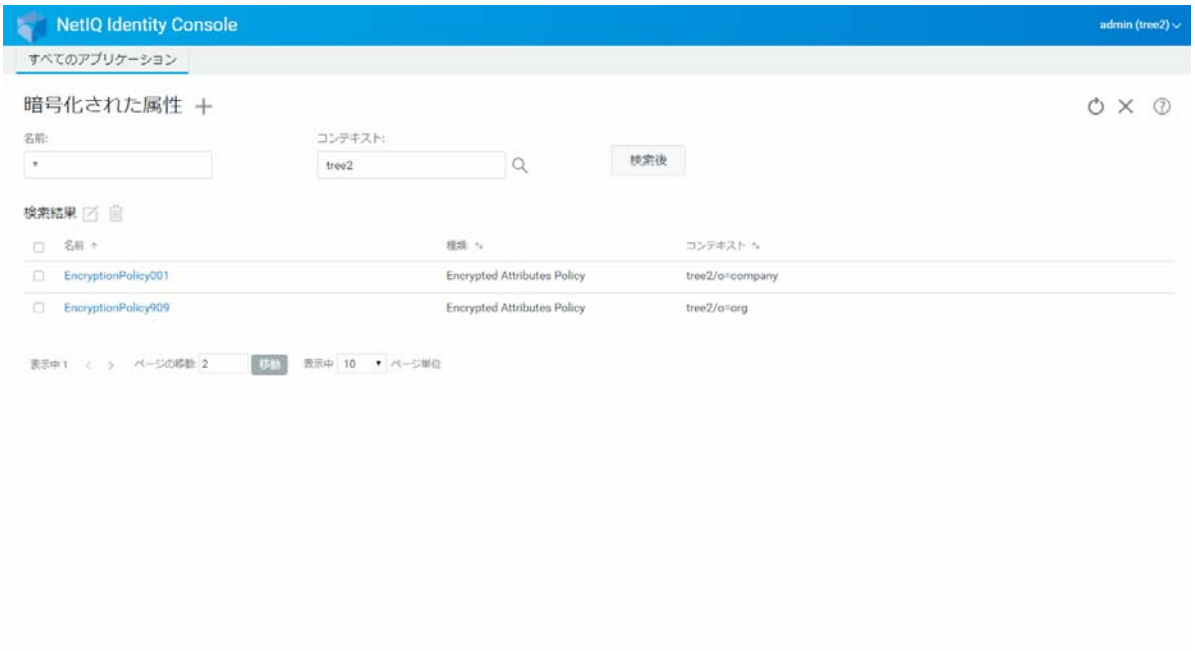
Identity Console では、暗号化された属性を eDirectory サーバから安全に読み込むことができます。Identity Console を使用すると、これらの暗号化属性に対していくつかのポリシーを作成、変更、または削除することができます。

暗号化属性のポリシーの作成

新しい属性ポリシーを作成するには :

1. Identity Console のランディングページから、[**[暗号化された属性]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [暗号化された属性ポリシーの作成] ページで、次の詳細を入力します。
   - ポリシー名を指定します
   - コンテキストを入力するか、選択します
   - NCP サーバを選択します
   - 属性を選択します
4. 必要な詳細情報をすべて指定したら、[**[終了]**] をクリックします。
5. ポリシーが作成されたことを示す確認メッセージが表示されます。

図 12-1 暗号化属性ポリシーの作成

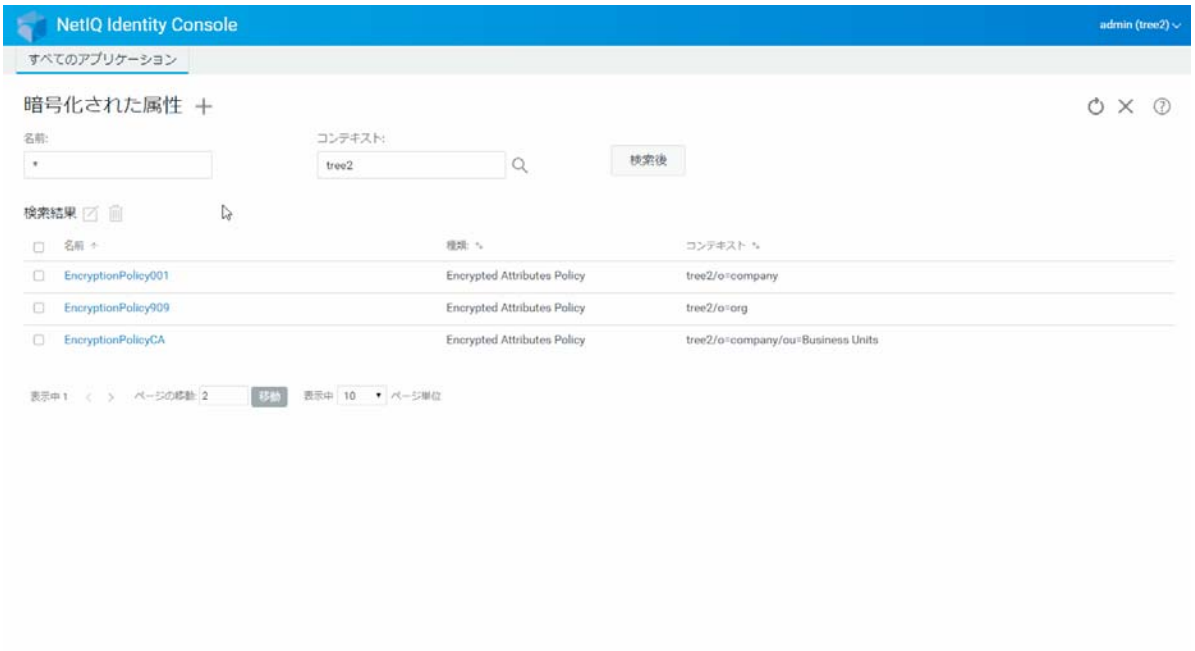


暗号化属性ポリシーの削除

暗号化属性ポリシーを削除するには :

1. Identity Console のランディングページから、[**[暗号化された属性]**] オプションをクリックします。
2. 属性の名前とコンテキストを指定するか、検索機能を使用して特定し、検索後 ボタンをクリックします。
3. リストから属性を選択して、アイコンをクリックします。
4. ポリシーが削除されたことを示す確認メッセージが表示されます。

図 12-2 暗号化属性ポリシーの削除



暗号化属性ポリシーの変更

暗号化属性ポリシーを変更するには :

1 Identity Console のランディングページから、[**[暗号化された属性]**] オプションをクリックします。

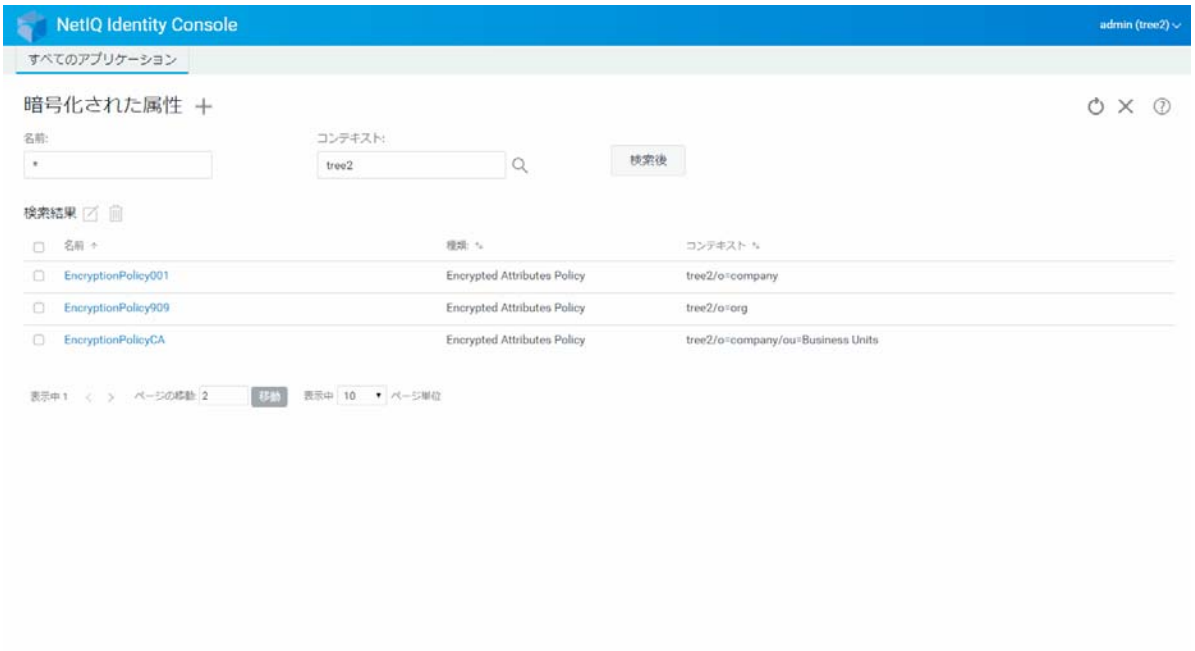
2 オブジェクトの名前とコンテキストを入力して、検索後 ボタンをクリックします。

3 オブジェクトリストから属性を選択し、アイコンをクリックします。

4 必要な変更を加えてから、保存 ボタンをクリックします。

5 ポリシーが変更されたことを示す確認メッセージが表示されます。

図12-3 暗号化属性ポリシーの変更



13 暗号化複製の管理

暗号化複製を有効にするには、暗号化複製を有効にするようにパーティションを設定する必要があります。設定はパーティションの Root オブジェクトに保存されます。選択できるのは、パーティションレベルで暗号化複製を有効にするかどうかということだけです。パーティションレベルで暗号化複製を有効にすると、そのパーティションをホストしているすべてのレプリカの間で行われる複製が暗号化されます。たとえば、パーティション P1 のレプリカとして、R1、R2、R3、および R4 があるとします。これらすべてのレプリカ間の複製を暗号化することができます。

- 79 ページの 「パーティションの暗号化複製を有効にする」

パーティションの暗号化複製を有効にする

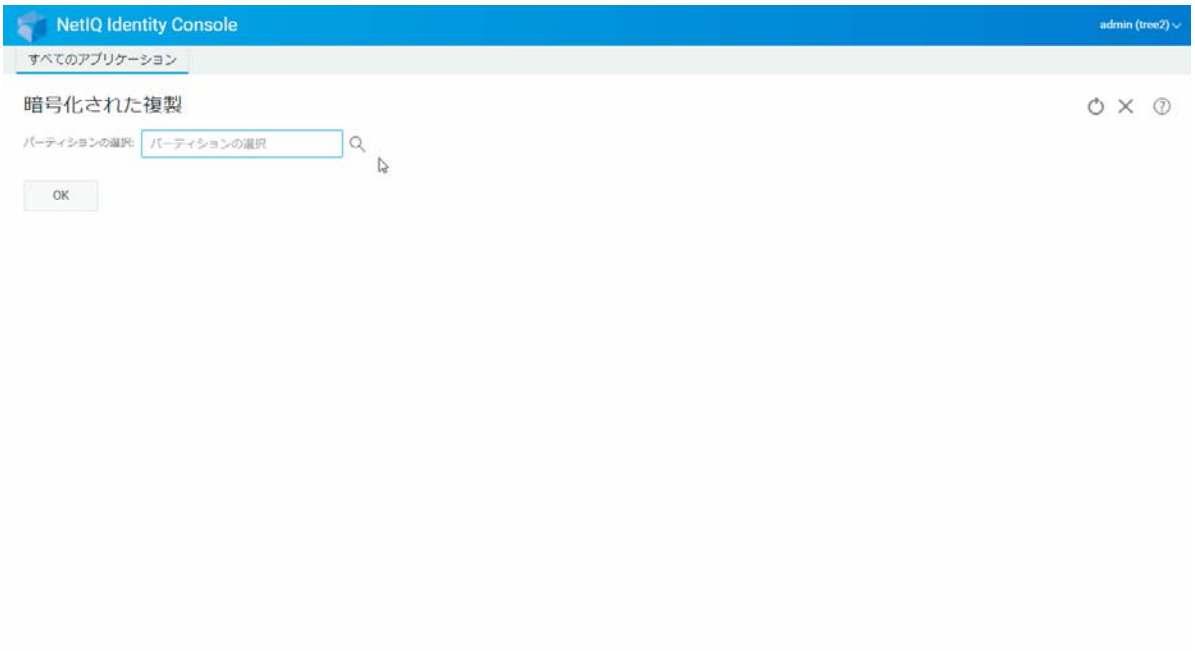
パーティションの暗号化複製を有効にするには :

注 : パーティションレベルで暗号化複製を有効にするには、そのパーティションをホストしているすべてのサーバで eDirectory 9.2 以降が実行されている必要があります。

---

1. Identity Console のランディングページから、[**[暗号化された複製]**] オプションをクリックします。
2. 暗号化複製を有効にするパーティションを指定またはブラウズします。
3. [**[複製の暗号化を有効にする]**] オプションを選択します。パーティションの暗号化複製を無効にしているときは、このオプションを選択解除します。
4. **[完了]** をクリックします。
5. 暗号化複製が有効になっていることを示す確認メッセージが表示されます。

図 13-1 パーティションの暗号化複製を有効にする



14 パーティションおよびレプリカの管理

パーティションおよびレプリカ操作により、ディレクトリサーバ全体での eDirectory の物理的な設計と配布を管理できます。

パーティションによって、eDirectory ツリーの論理区分が作成されます。たとえば、1 つの部門を選択し、これを新しいパーティションとして作成すると、選択した部門およびその従属オブジェクトすべてが親パーティションから分割されます。選択した部門は、新しいパーティションのルートになります。新しいパーティションのレプリカは、ペアレントパーティションのレプリカと同じサーバに存在します。また、新しいパーティションのオブジェクトは、そのパーティションのルートオブジェクトに属します。

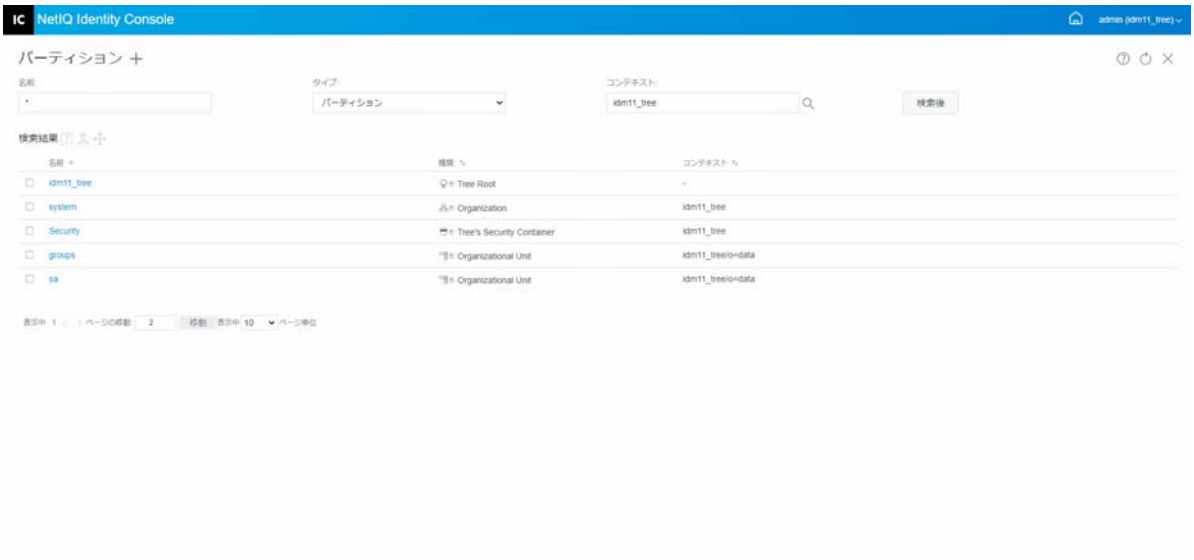
パーティションモジュールを使用して、次のタスクを実行できます。

パーティションの作成

新しいパーティションを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[パーティション管理]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [パーティションの作成] ページで、新しいパーティションのルートとして使用するコンテナを指定するか、オブジェクトセレクタの🔍アイコンを使用してコンテナを特定して、[**[作成]**] をクリックします。
4. パーティションが作成されたことを示す確認メッセージが表示されます。

図 14-1 新規パーティションの作成

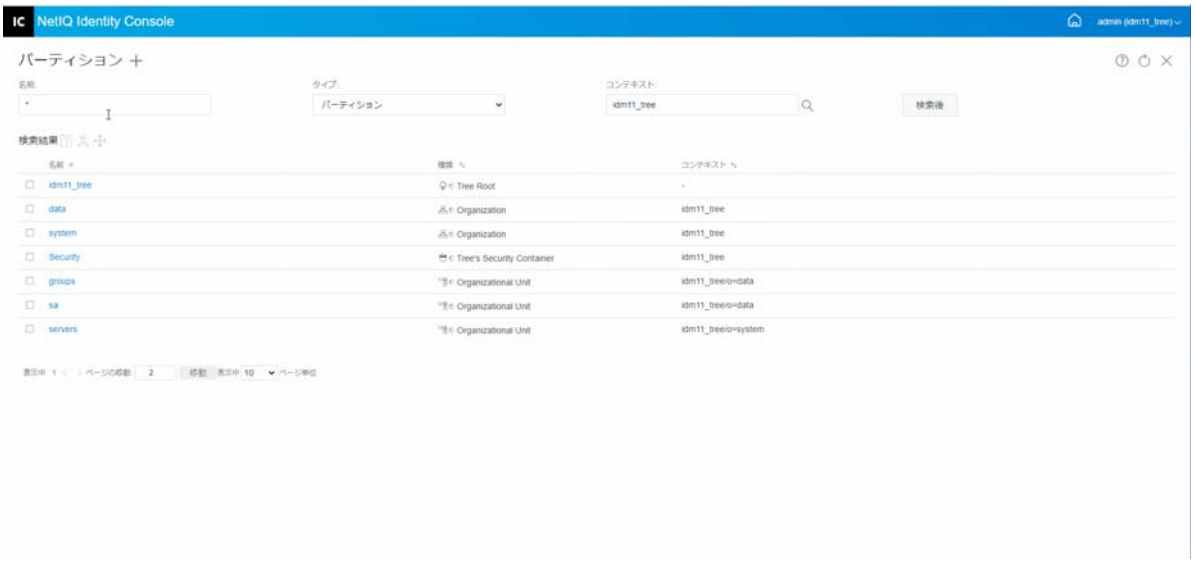


パーティションのマージ

パーティションをその親パーティションとマージするには、次の手順を実行します。

1. Identity Console のランディングページから、[**[パーティション管理]**] オプションをクリックします。
2. パーティションの名前、タイプ、およびコンテキストを指定するか、検索機能を使用して特定し、検索後 ボタンをクリックします。
3. 検索リストからパーティションを選択し、アイコンをクリックして、[**[OK]**] をクリックします。
4. パーティションがマージされたことを示す確認メッセージが表示されます。

図 14-2 パーティションのマージ



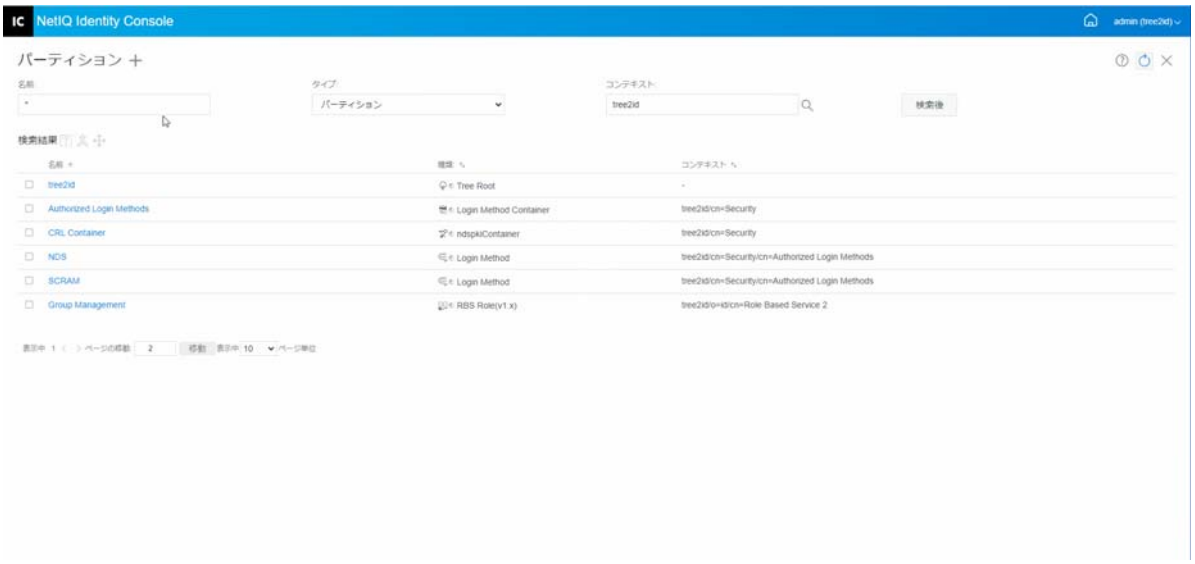
パーティションの変更

パーティションを変更するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[パーティション管理]**] オプションをクリックします。
2. パーティションの名前、タイプ、およびコンテキストを入力し、検索後 ボタンをクリックします。
3. 検索リストからパーティションを選択し、アイコンをクリックします。
4. [**[フィルタ]**] の下の [**[編集]**] オプションをクリックして、レプリカフィルタとその対応するクラスと属性を変更し、[**[OK]**] をクリックします。

   [**[タイプ]**] フィールドで [**[サーバ]**] を選択した場合は、すべてのサーバのリストが表示されます。各サーバをクリックすると、サーバ内のすべてのパーティションのリストが表示されます。
5. パーティションが変更されたことを示す確認メッセージが表示されます。

図 14-3 パーティションの変更



パーティションの移動

パーティションを移動することで、ディレクトリツリー内のサブツリーを移動できます。これは切り取り / 接ぎ木操作とも呼ばれます。移動できるのは、サブオーディネートパーティションがないパーティションだけです。サブオーディネートパーティションがある場合は、移動操作を行う前にそれらのパーティションをマージする必要があります。

パーティションを移動する場合、eDirectory ではパーティションのルートオブジェクトへのすべての参照が変更されます。オブジェクトの共通名は変更されませんが、コンテナ (およびそのサブオーディネートコンテナすべて) の完全識別名は変更されます。

注 : パーティションを移動する場合は、eDirectory の包含ルールに従う必要があります。たとえば、部門はディレクトリツリーのルートの直下には移動できません。これは、ルートの包含ルールにより、地域、国、または組織のみが移動を許可されているためです。

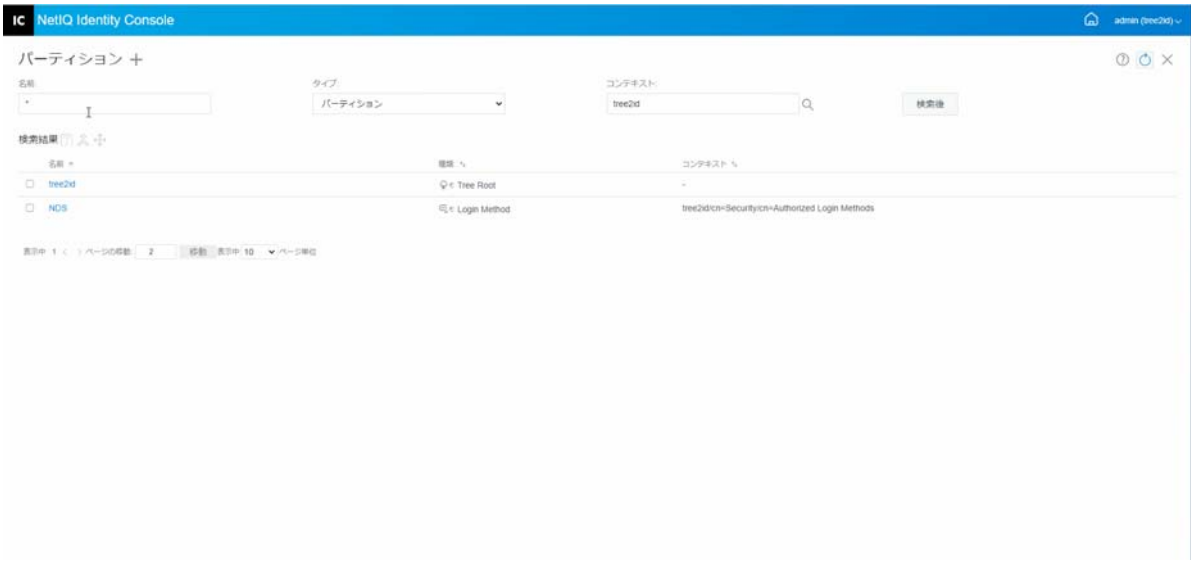
パーティションを移動するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[パーティション管理]**] オプションをクリックします。
2. パーティションの名前、タイプ、およびコンテキストを入力し、検索後 ボタンをクリックします。
3. 検索リストからパーティションを選択し、✣ アイコンをクリックします。
4. 指定したパーティションの移動先のコンテナオブジェクトを選択し、[**[OK]**] をクリックします。

注 : [**[移動したパーティションの代わりに別名を作成します]**] によって、パーティションの新しい場所にポインタが作成されます。これにより、新しい場所を反映して操作を更新するまで、古い場所に依存する操作が続行されます。ユーザは、引き続きネットワークにログインし、元のディレクトリの場所でオブジェクトを検索できます。

5 パーティションが正常に移動されたことを示す確認メッセージが表示されます。

図 14-4 *パーティションの移動*



15 インデックスの管理

インデックスマネージャは、サーバオブジェクトの属性の 1 つで、データベースインデックスの管理に使用します。eDirectory では、データベースインデックスを使用することによって、クエリの処理速度が大幅に向上します。

NetIQ eDirectory には、基本的なクエリの機能を提供する一連のインデックスが付属しています。これらデフォルトのインデックスの対象となる属性を次に示します。

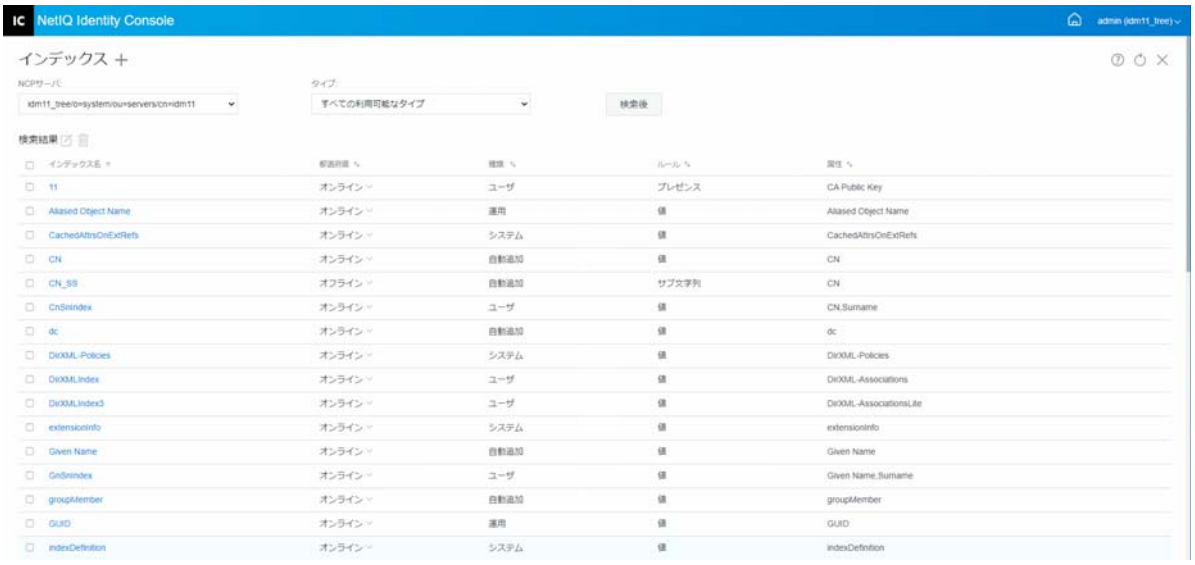
インデックスモジュールを使用して、次のタスクを実行できます。

インデックスの作成

新しいインデックスを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[インデックス管理]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. インデックス名を入力します。
4. 使用可能な NCP サーバのリストからサーバを選択します。
5. 必要な属性を選択します。
6. インデックスのルールを選択します。
   - 6a **部分文字列 :** 属性値文字列のサブセットを照合します。たとえば、「der」という値を含む「LastName」を検索するクエリを実行すると、「Derington」、「Anderson」、および「Lauder」が照合の結果として返されます。下位文字列インデックスは、作成や維持を行うときに最も多くのリソースが消費されるインデックスです。
   - 6b **存在 :** 特定の属性値ではなく、属性の存在のみ必要です。Login Script 属性を持つエントリをすべて検索するクエリは、存在インデックスを使用します。
   - 6c **値 :** 属性の値全体または値の最初の部分を照合します。たとえば、値一致は、「Jensen」に一致する「LastName」のあるエントリの検索や、「Jen」で始まる「LastName」があるエントリの検索に使用できます。
7. 作成 ボタンをクリックします。
8. インデックスが作成されたことを示す確認メッセージが表示されます。

図 15-1 新しいインデックスの作成



インデックスを削除する

インデックスを削除するには、次の手順を実行します。

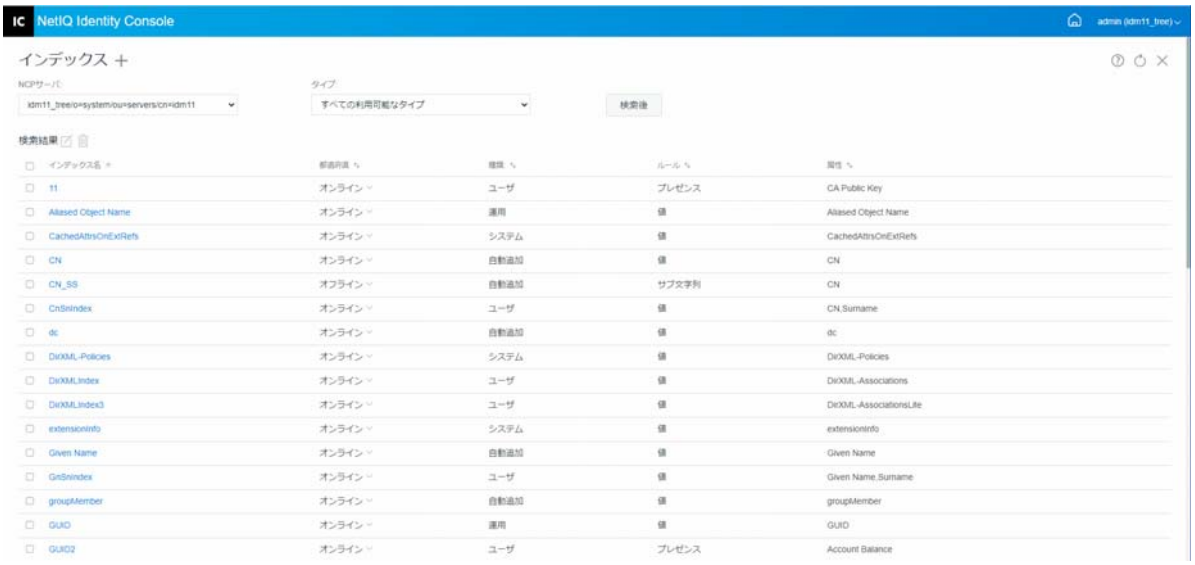
1 Identity Console のランディングページから、[**[インデックス管理]**] オプションをクリックします。

2 NCP サーバとインデックスのタイプを選択し、検索後 ボタンをクリックします。

3 検索リストからインデックスを選択し、🗑アイコンをクリックします。

4 インデックスが削除されたことを示す確認メッセージが表示されます。

図 15-2 インデックスを削除する



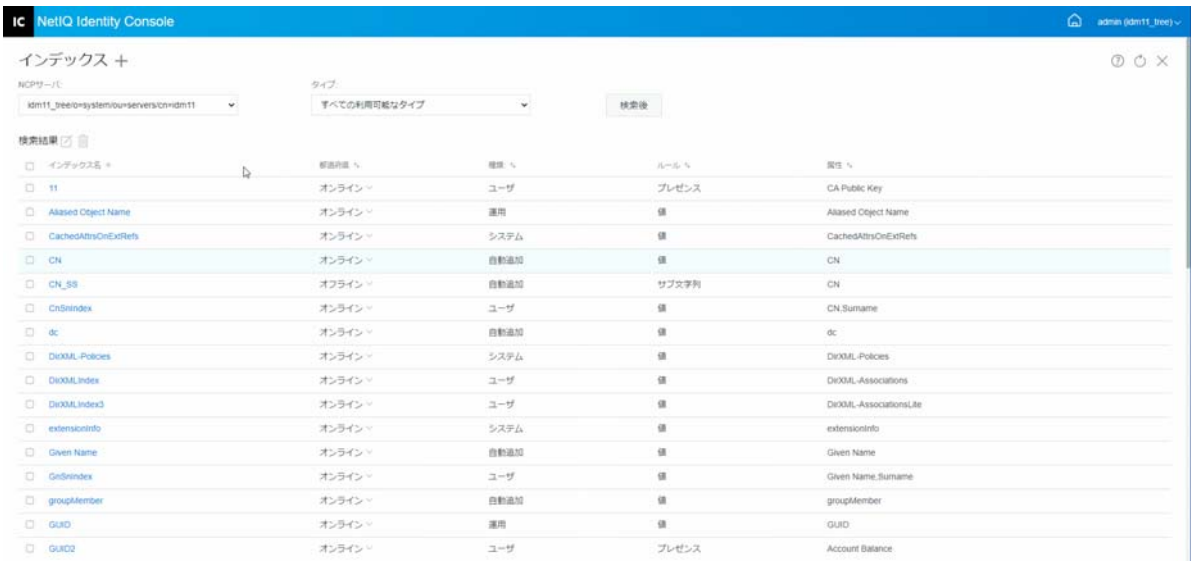
インデックスのコピー

あるサーバで便利に使用されているインデックスがあり、このインデックスを他のサーバでも使用する場合は、他のサーバにインデックス定義をコピーできます。またプレディケートデータを調べると、これとは逆のケースが発生する場合もあります。つまり、複数のサーバで使用されていたインデックスが、そのいずれかのサーバで不要になるといったケースです。このような場合、インデックスが不要になった単一のサーバからインデックスを削除できます。

インデックスをコピーするには、次の手順を実行します。

1. Identity Console のランディングページから、[**[インデックス管理]**] オプションをクリックします。
2. NCP サーバとインデックスのタイプを選択し、検索後 ボタンをクリックします。
3. 検索リストからインデックスを選択し、アイコンをクリックします。
4. インデックスをコピーしたい NCP サーバを選択し、保存 ボタンをクリックします。
5. インデックスが変更されたことを示す確認メッセージが表示されます。

図 15-3 *インデックスのコピー*



インデックスの状態の変更

一時的にインデックスをオフラインにすることで、処理のピーク時にパフォーマンスを調整できます。たとえば、ユーザ定義のインデックスの使用をすべて中断すると、バルクロードを高速化できます。オブジェクトを追加または変更するときは定義されているイン

デックスを更新する必要があり、すべてのインデックスをアクティブにするとデータのバルクロードの速度が遅くなるためです。バルクロードが完了すると、再びインデックスをオンラインにできます。

インデックスをオフラインにするには、次の手順を実行します。

1 Identity Console のランディングページから、[**[インデックス管理]**] オプションをクリックします。

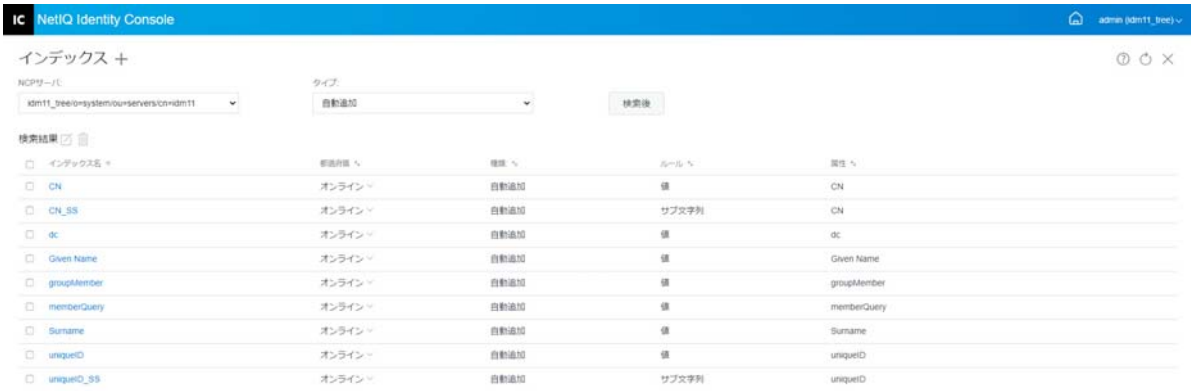
2 NCP サーバとインデックスのタイプを選択し、検索後 ボタンをクリックします。

3 インデックスのリストから［ **[状態]**］のドロップダウンリストをクリックします。インデックスの状態には以下のものがあります。

- **［Online］:** 現在実行中
- **オフライン :** [一時停止中］. インデックスを再度起動できます。

注 : システムおよび運用タイプのインデックスの状態は変更できません。このようなインデックスは削除することもできません。

図 15-4 *インデックスをオフラインにする*



16 LDAP オブジェクトを環境設定する

eDirectory のインストール時に、LDAP サーバオブジェクトと LDAP グループオブジェクトが作成されます。LDAP サービスのデフォルト設定は、これらの 2 つのオブジェクト上のディレクトリにあります。Identity Console で LDAP 管理タスクを使用することで、デフォルトの設定を変更できます。

LDAP サーバオブジェクトとは、サーバ固有の設定データのことです。ただし、LDAP グループオブジェクトには、複数の LDAP サーバ間で共有できる便利な設定情報が含まれています。このオブジェクトは、共通の設定データと LDAP サーバグループを提供します。サーバは共通データを持っています。

複数の LDAP サーバオブジェクトを、1 つの LDAP グループオブジェクトと関連させることができます。関連するすべての LDAP サーバは、サーバ固有の設定をそれぞれの LDAP サーバオブジェクトから取得しますが、共通する情報や共有情報は LDAP グループオブジェクトから取得します。

LDAP モジュールを使用して、次のタスクを実行できます。

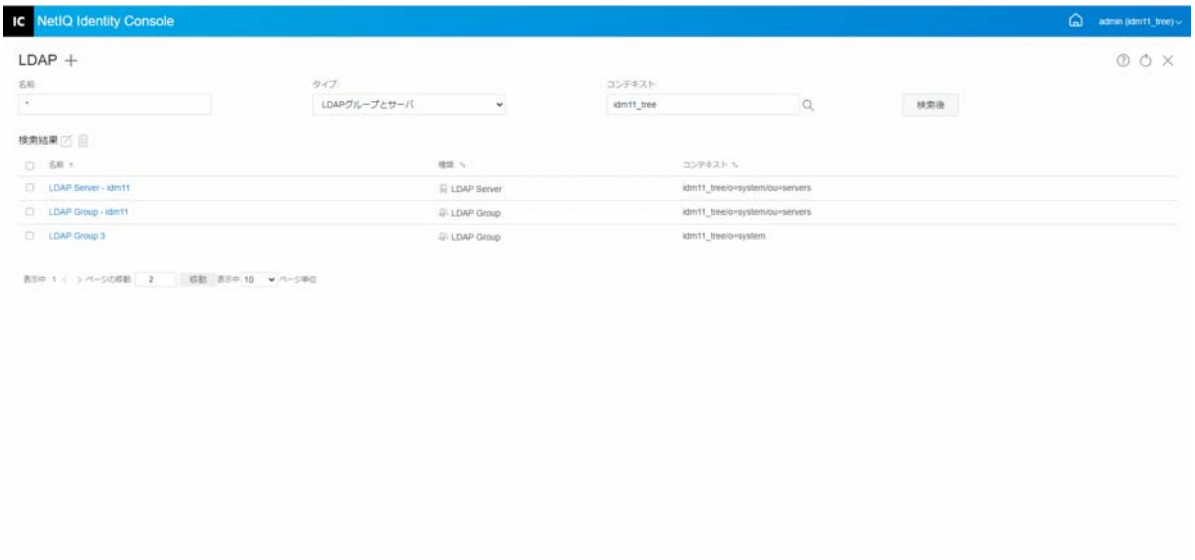
- 91 ページの 「LDAP オブジェクトの作成」
- 92 ページの 「LDAP オブジェクトの削除」
- 93 ページの 「LDAP オブジェクトの変更」

LDAP オブジェクトの作成

新しい LDAP オブジェクトを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[LDAP 環境設定]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [LDAP オブジェクトの作成] ページで、名前、タイプ、およびコンテキストを指定するか、検索コンテキストの🔍アイコンを使用して検索し、[**[作成]**] をクリックします。
4. LDAP オブジェクトが作成されたことを示す確認メッセージが表示されます。

図16-1 新しいLDAP オブジェクトの作成

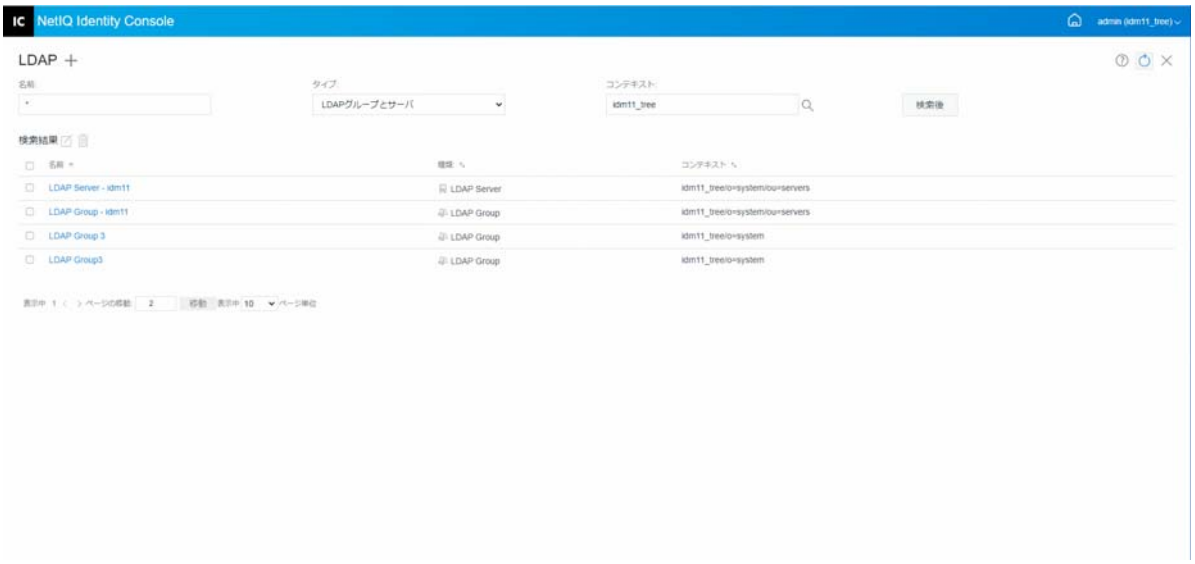


LDAP オブジェクトの削除

LDAP オブジェクトを削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[LDAP 環境設定]**] オプションをクリックします。
2. LDAP オブジェクトの名前、タイプ、およびコンテキストを指定し、検索後 ボタンをクリックします。
3. 検索リストから LDAP オブジェクトを選択し、アイコンをクリックします。
4. LDAP オブジェクトが削除されたことを示す確認画面が表示されます。

図 16-2 LDAP オブジェクトの削除

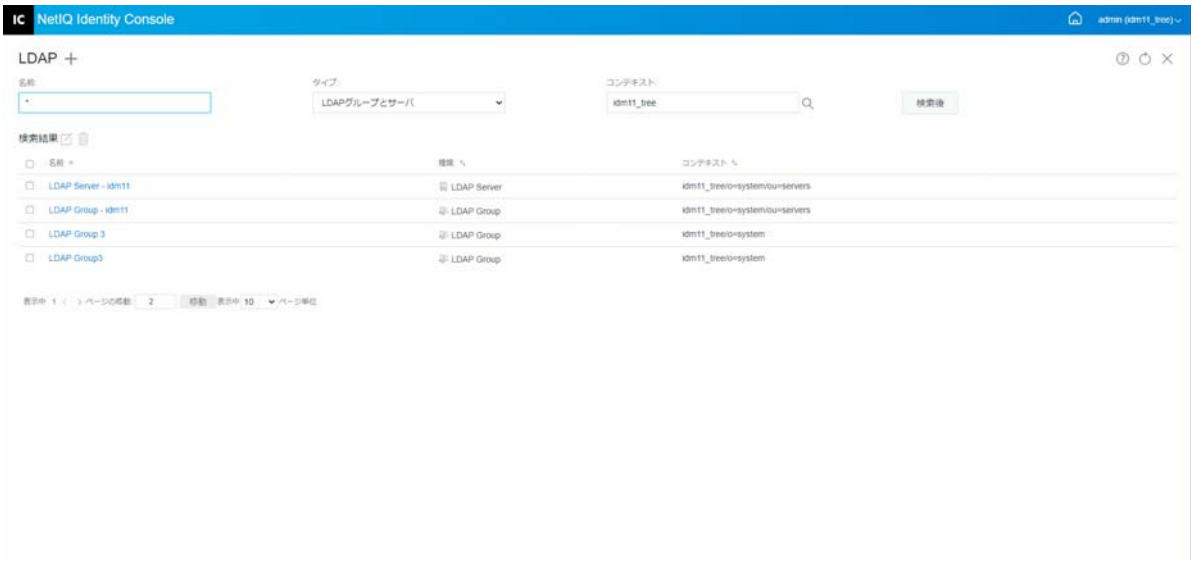


LDAP オブジェクトの変更

LDAP オブジェクトを変更するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[LDAP 環境設定]**] オプションをクリックします。
2. LDAP オブジェクトの名前、タイプ、およびコンテキストを入力し、検索後 ボタンをクリックします。
3. 検索リストから LDAP オブジェクトを選択し、アイコンをクリックします。
4. 必要に応じて特定の LDAP オブジェクトの属性および情報を変更し、保存 ボタンをクリックします。LDAP オブジェクトの属性の詳細については、NetIQ eDirectory 管理ガイドの「*Configuring LDAP Server and LDAP Group Objects on Linux (Linux での LDAP サーバおよび LDAP グループオブジェクトの設定)*」を参照してください。
5. LDAP オブジェクトが変更されたことを示す確認メッセージが表示されます。

図 16-3 LDAP オブジェクトの変更



17 証明書の管理

eDirectory をインストールすると、NetIQ Certificate Server が自動的にインストールされます。Certificate Server は、eDirectory にネイティブに統合された公開鍵暗号サービスを提供します。このサービスを使用すれば、ユーザとサーバの両方の証明書を作成、発行、および管理することができます。これらのサービスにより、インターネットなどのパブリック通信チャネルを介した機密データの伝送を保護できます。

注 : 証明書管理モジュールを Identity Console と一緒に使用する場合は、eDirectory サーバを 9.2.4 HF2 にアップグレードする必要があります。

Identity Console では、次のような証明書管理タスクが提供されます。

- 95 ページの 「認証局の管理」
- 99 ページの 「サーバ証明書の管理」
- 102 ページの 「ユーザ証明書の管理」
- 104 ページの 「ルート認証局とコンテナの管理」
- 107 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」
- 108 ページの 「公開鍵証明書の発行」
- 111 ページの 「SAS Service オブジェクトの管理」

認証局の管理

デフォルトでは、NetIQ Certificate Server のインストールプロセスで、組織認証局 (CA) が作成されます。組織認証局の名前を指定するように求められます。[終了] をクリックすると、組織認証局がデフォルトのパラメータで作成され、セキュリティコンテナに配置されます。組織認証局の作成をより詳細に制御する場合は、Identity Console ポータルを使用して手動で組織認証局を作成できます。また、組織認証局を削除した場合、それを再作成する必要があります。

認証局モジュールを使用して、次のタスクを実行できます。

- 96 ページの 「組織認証局オブジェクトの作成」
- 96 ページの 「組織認証局証明書のバックアップ」
- 97 ページの 「組織認証局の復元」
- 97 ページの 「組織認証局の証明書の検証」
- 98 ページの 「組織認証局証明書の置き換え」
- 98 ページの 「組織認証局証明書の取り消し」

組織認証局オブジェクトの作成

組織認証局オブジェクトを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[認証局の管理]**] オプションをクリックします。
2. 組織の認証局オブジェクトが存在しない場合、[Create an Organizational Certificate Authority Object] ダイアログボックスとオブジェクトを作成するウィザードが開きます。メッセージに従ってオブジェクトを作成します。

   注 : ここで指定する CRL ファイルパスが、eDirectory インストールパスと対応していることを確認します。
3. 認証局の作成を完了したら、認証局の公開鍵 / 秘密鍵のペアのバックアップを作成し、安全な場所に保存することをお勧めします。詳細については、96 ページの 「組織認証局証明書のバックアップ」 を参照してください。

組織認証局証明書のバックアップ

組織認証局のホストサーバで回復不能な障害が発生する場合に備え、組織認証局の秘密鍵と証明書をバックアップしておくことをお勧めします。障害が発生した場合、バックアップファイルを使用して、組織認証局をツリー内の任意のサーバに復元できます。

注 : 組織認証局をバックアップする機能は、NetIQ Certificate Server バージョン 9.0 以上で作成された組織認証局に対してのみ使用できます。証明書サーバの以前のバージョンでは、組織認証局の秘密鍵は、エクスポートできない方法で作成されていました。

バックアップファイルには、認証局の秘密鍵、自己署名証明書、公開鍵証明書、およびこの操作に必要とされるいくつかの他の証明書が含まれています。この情報は、PKCS #12 形式 (PFX とも呼ばれます) で保存されます。

組織認証局が正常に機能しているときに、組織認証局をバックアップする必要があります。

組織認証局をバックアップするには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[認証局の管理]**] オプションをクリックします。
2. [**[証明書]**] タブをクリックします。
3. [**[自己署名証明書]**] または [**[公開鍵証明書]**] のいずれかを選択します。証明書は両方とも、バックアップ操作中にファイルに書き込まれます。RSA と ECDSA 証明書の [自己署名証明書] を別個に選択することをお勧めします。
4. アイコンをクリックします。

5 秘密鍵のエクスポートを選択して、6 文字以上の英数字で PFX ファイルの暗号化に使用するパスワードを指定し、PKCS12 をエクスポートフォーマットとして選択し、[[OK]] をクリックします。

6 暗号化されたバックアップファイルは、指定した場所に書き込まれます。これで、緊急用に、ファイルを安全な場所に保存する準備ができました。

組織認証局の復元

組織認証局オブジェクトが削除されたまたは破損した場合、あるいは組織認証局のホストサーバに回復不能な障害が発生した場合、96 ページの 「組織認証局証明書のバックアップ」で作成したバックアップファイルを使用して、完全に復元することができます。

組織認証局を復元するには、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[認証局の管理]] オプションをクリックします。

2 画面の上部の↑↓([[認証局の管理]] の横) をクリックして、既存の組織認証局を削除します。

3 新しい組織認証局の設定が求められます。この操作により、[Create an Organizational Certificate Authority Object] ダイアログボックスと、オブジェクトを作成する対応するウィザードが開きます。

4 作成ダイアログボックスで、組織認証局をホストするサーバおよび組織認証局オブジェクトの名前を指定する必要があります。

5 [[インポート]] を選択します。

6 RSA と ECDSA の両方の証明書を選択します。証明書サーバでは、両方の証明書のサブジェクト名が同じである必要があります。ただし、証明書サーバでは、外部自己署名認証局証明書のインポートをサポートしません。ただし、従属認証局証明書をインポートすることはできます。

7 その後の画面で RSA と ECDSA のファイルの名前をブラウズし、選択します。

8 バックアップ実行時に、ファイルを暗号化するために使用したパスワードを入力し、[[OK]] をクリックします。

9 これで組織認証局の秘密鍵と証明書が復元され、認証局が完全に機能するようになります。将来の使用に備え、ここでファイルをもう一度保存できます。

組織認証局の証明書の検証

証明書に問題があることが疑われる場合、または失効していると思われる場合は、Identity Console を使用して簡単に証明書を検証できます。外部認証局によって発行された証明書を含め、eDirectory ツリー内のすべての証明書を検証できます。

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて 1 つ以上の中間認証局の証明書からなります。

証明書を検証するには、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[認証局の管理]] オプションをクリックします。
2 [[証明書]] タブをクリックします。
3 [[自己署名証明書]] または [[公開鍵証明書]] のいずれかを選択します。
4 選択した認証局証明書を検証するには、をクリックします。

組織認証局証明書の置き換え

証明書が何らかの理由で破損または無効になった場合、または既存の証明書を置き換える場合は、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[認証局の管理]] オプションをクリックします。
2 [[証明書]] タブをクリックします。
3 [[自己署名証明書]] または [[公開鍵証明書]] のいずれかを選択します。
4 選択した認証局証明書を置き換えるには、をクリックします。
5 認証局証明書を .pfx または .p12 形式でインポートし、秘密鍵を暗号化するためのパスワードを指定します。
6 [OK] をクリックします。

組織認証局証明書の取り消し

証明書を取り消すには、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[認証局の管理]] オプションをクリックします。
2 [[証明書]] タブをクリックします。
3 [[自己署名証明書]] または [[公開鍵証明書]] のいずれかを選択します。
4 アイコンをクリックします。
5 サーバ証明書の取り消しに伴うリスクを読み、理解をしてください。
6 ドロップダウンリストから取り消しの有効な理由を選択し、無効日を選択して、その他のコメントを指定します。
7 [[OK]] をクリックして取り消しを完了します。

図 17-1 認証局の管理

サーバ証明書の管理

サーバ証明書管理モジュールを使用すると、管理者は次のタスクを実行できます。

- 99 ページの 「サーバ証明書オブジェクトを作成する」
- 100 ページの 「サーバ証明書オブジェクトのエクスポート」
- 100 ページの 「サーバ証明書オブジェクトの検証」
- 100 ページの 「サーバ証明書オブジェクトの置き換え」
- 101 ページの 「サーバ証明書オブジェクトの取り消し」
- 101 ページの 「サーバ証明書オブジェクトの削除」

サーバ証明書オブジェクトを作成する

サーバ証明書オブジェクトを作成するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[サーバ証明書管理]**] オプションをクリックします。

2 ＋アイコンをクリックします。

3 [**[サーバ証明書の作成]**] ページで、**[ニックネーム]** とサーバを指定し、次のオプションのいずれかを選択します。

- **規格 (デフォルトパラメータ):** RSA または ECDSA タイプのデフォルトのサーバ証明書オブジェクトを作成できます。
- **カスタム (ユーザ指定パラメータ):** サーバ証明書オブジェクトのカスタムパラメータを指定できます。
- **インポート (PKCS12 ファイルのインポートを許可):** PKCS12 ファイルを .pfx または .p12 形式でインポートできます。

4 パラメータを指定した後、[[次へ]] をクリックし、証明書の概要を確認します。

5 [概要] 画面で、[[OK]] をクリックしてサーバ証明書オブジェクトを作成します。

サーバ証明書オブジェクトのエクスポート

サーバ証明書オブジェクトをエクスポートするには、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[サーバ証明書管理]] オプションをクリックします。

2 ドロップダウンリストから適切なサーバを選択します。

3 リストから適切なサーバ証明書を選択して、アイコンをクリックします。

4 次の画面で、[[Export Private key(秘密鍵のエクスポート)]] のチェックボックスをオンにして、秘密鍵を保護するためのパスワードを指定します。パスワードを確認し、エクスポート形式を選択します。

注 : サーバ証明書は PKCS12 形式でのみエクスポートできます。

5 [[OK]] をクリックして、サーバ証明書オブジェクトをエクスポートします。

サーバ証明書オブジェクトの検証

サーバ証明書オブジェクトを検証するには、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[サーバ証明書管理]] オプションをクリックします。

2 ドロップダウンリストから適切なサーバを選択します。

3 リストから適切なサーバ証明書を選択して、アイコンをクリックします。

4 サーバ証明書オブジェクトの検証が成功したことを示す確認メッセージが表示されます。

サーバ証明書オブジェクトの置き換え

サーバ証明書が何らかの理由で破損または無効になった場合、または既存のデフォルト証明書を置き換える場合は、次の手順を実行します。

1 Identity Console のランディングページから、[[証明書管理]] > [[サーバ証明書管理]] オプションをクリックします。

2 ドロップダウンリストから適切なサーバを選択します。

3 リストから適切なサーバ証明書を選択して、アイコンをクリックします。

4 サーバ証明書の置き換えに伴うリスクを読み、理解し、[[OK]] をクリックします。

5 次の画面で、.pfx または .p12 形式の新しいサーバ証明書を参照して選択し、パスワードを指定します。

6 サーバ証明書を置き換える場合は、[[OK]] をクリックします。

サーバ証明書オブジェクトの取り消し

サーバ証明書オブジェクトを取り消す場合は、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[サーバ証明書管理]**] オプションをクリックします。
2. ドロップダウンリストから適切なサーバを選択します。
3. リストから適切なサーバ証明書を選択して、⊘アイコンをクリックします。
4. サーバ証明書の取り消しに伴うリスクを読み、理解し、[**[OK]**] をクリックします。
5. 次の画面で、ドロップダウンリストから取り消しの有効な理由を選択し、無効日を選択して、その他のコメントを指定します。
6. [**[OK]**] をクリックして取り消しを完了します。

サーバ証明書オブジェクトの削除

サーバ証明書オブジェクトを削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[サーバ証明書管理]**] オプションをクリックします。
2. ドロップダウンリストから適切なサーバを選択します。
3. リストから適切なサーバ証明書を選択して、🗑アイコンをクリックします。
4. 次の画面で [**[OK]**] をクリックします。
5. サーバ証明書オブジェクトが正常に削除されたことを示す確認メッセージが表示されます。

図 17-2 サーバ証明書の管理

ユーザ証明書の管理

ユーザ証明書管理モジュールを使用して、次のタスクを実行できます。

ユーザ証明書オブジェクトの作成

ユーザ証明書オブジェクトを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[ユーザ証明書管理]**] オプションをクリックします。
2. ＋アイコンをクリックします。
3. [**[ユーザ証明書の作成]**] ページで、**[ニックネーム]** とサーバを指定し、次のオプションのいずれかを選択します。
   - **規格 (デフォルトパラメータ):** RSA または ECDSA タイプのデフォルトのユーザ証明書オブジェクトを作成できます。
   - **カスタム (ユーザ指定パラメータ):** ユーザ証明書オブジェクトのカスタムパラメータを指定できます。
   - **インポート :** 証明書ファイルを CERT または PKCS12 形式でインポートできます。
4. パラメータを指定した後、[**[次へ]**] をクリックし、証明書の概要を確認します。
5. **[概要]** 画面で、[**[OK]**] をクリックしてユーザ証明書オブジェクトを作成します。

ユーザ証明書オブジェクトのエクスポート

ユーザ証明書オブジェクトをエクスポートするには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[ユーザ証明書管理]**] オプションをクリックします。
2. ドロップダウンリストから適切なサーバを選択します。
3. リストから適切なユーザ証明書を選択し、アイコンをクリックします。
4. 次の画面で、[**[Export Private key(秘密鍵のエクスポート)]**] のチェックボックスをオンにして、秘密鍵を保護するためのパスワードを指定します。パスワードを確認し、エクスポート形式を選択します。

   注 : ユーザ証明書は、PKCS12 形式でのみエクスポートできます。

5. [**[OK]**] をクリックして、ユーザ証明書オブジェクトをエクスポートします。

ユーザ証明書オブジェクトの検証

ユーザ証明書オブジェクトを検証するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ユーザ証明書管理]**] オプションをクリックします。
2 ドロップダウンリストから適切なサーバを選択します。
3 リストから適切なユーザ証明書を選択し、アイコンをクリックします。
4 ユーザ証明書オブジェクトの検証が成功したことを示す確認メッセージが表示されます。

ユーザ証明書オブジェクトの取り消し

ユーザ証明書オブジェクトを取り消す場合は、次の手順を実行します。

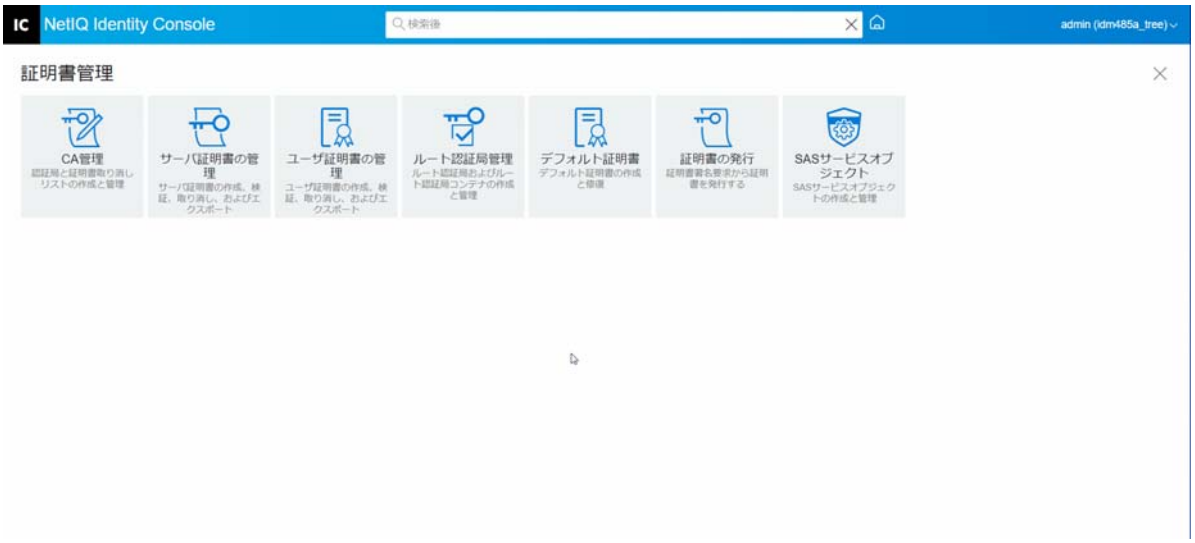
1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ユーザ証明書管理]**] オプションをクリックします。
2 ドロップダウンリストから適切なサーバを選択します。
3 リストから適切なユーザ証明書を選択し、アイコンをクリックします。
4 ユーザ証明書の取り消しに伴うリスクを読み、理解をしてください。
5 ドロップダウンリストから取り消しの有効な理由を選択し、無効日を選択して、その他のコメントを指定します。
6 [**[OK]**] をクリックして取り消しを完了します。

ユーザ証明書オブジェクトの削除

ユーザ証明書オブジェクトを削除するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ユーザ証明書管理]**] オプションをクリックします。
2 ドロップダウンリストから適切なサーバを選択します。
3 リストから適切なユーザ証明書を選択し、アイコンをクリックします。
4 次の画面で [**[OK]**] をクリックします。
5 ユーザ証明書オブジェクトが正常に削除されたことを示す確認メッセージが表示されます。

図 17-3 ユーザ証明書の管理



ルート認証局とコンテナの管理

ルート認証局は、公開鍵暗号の信頼の基盤です。ルート認証局は、他の CA によって署名された証明書の検証に使用されます。ルート認証局は、SSL、セキュリティで保護された電子メール、および証明書ベースの認証のセキュリティを有効にします。

ルート認証局管理モジュールを使用して、次のタスクを実行できます。

- 104 ページの 「ルート認証局コンテナの作成」
- 105 ページの 「ルート認証局証明書オブジェクトの作成」
- 105 ページの 「ルート認証局証明書オブジェクトのエクスポート」
- 105 ページの 「ルート認証局証明書オブジェクトの検証」
- 106 ページの 「ルート認証局証明書オブジェクトの削除」
- 106 ページの 「ルート認証局コンテナの削除」

ルート認証局コンテナの作成

ルート認証局コンテナを作成するには、次のタスクを実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。
2. 新しいルート認証局コンテナを作成するには、＋アイコンをクリックします。
3. ルート認証局コンテナの名前を指定します。
4. オブジェクトセレクタを使用して、適切なコンテナを参照します。
5. [**[OK]**] ボタンをクリックします。
6. ルート認証局コンテナが正常に作成されたことを示す確認メッセージが表示されます。

ルート認証局証明書オブジェクトの作成

ルート認証局オブジェクトを作成するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。[**[ルート認証局]**] チェックボックスを選択します。

2 新しいルート認証局オブジェクトを作成するには、＋アイコンをクリックします。

3 ルート認証局オブジェクトの名前を指定します。

4 ドロップダウンリストから適切なルート認証局コンテナを選択します。

5 .der または .b64 形式の適切な証明書ファイルを参照し、選択します。

注 : ルート認証局オブジェクトには、すべてのタイプの証明書を保存できます (認証局証明書、中間認証局証明書、またはユーザ証明書)。

---

6 [**[OK]**] ボタンをクリックします。

7 ルート認証局オブジェクトが正常に作成されたことを示す確認メッセージが表示されます。

ルート認証局証明書オブジェクトのエクスポート

ルート認証局証明書オブジェクトをエクスポートするには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。[**[ルート認証局]**] チェックボックスを選択します。

2 リストから適切なルート認証局証明書を選択し、アイコンをクリックします。

3 次の画面で、[**[Export Private key(秘密鍵のエクスポート)]**] のチェックボックスをオンにして、秘密鍵を保護するためのパスワードを指定します。パスワードを確認し、エクスポート形式を選択します。

注 : ルート認証局証明書は、DER または BASE64 形式でのみエクスポートできます。

---

4 [**[OK]**] をクリックして、ルート認証局証明書オブジェクトをエクスポートします。

ルート認証局証明書オブジェクトの検証

ルート認証局証明書オブジェクトを検証するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。[**[ルート認証局]**] チェックボックスを選択します。

2 リストから適切なルート認証局証明書を選択し、アイコンをクリックします。

3 ルート認証局証明書オブジェクトの検証が成功したことを示す確認メッセージが表示されます。

ルート認証局証明書オブジェクトの削除

ルート認証局証明書オブジェクトを削除するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。[**[ルート認証局]**] チェックボックスを選択します。

2 リストから適切なルート認証局証明書を選択し、アイコンをクリックします。

3 警告画面で［ **[OK]**］をクリックします。

4 ルート認証局証明書オブジェクトが正常に削除されたことを示す確認メッセージが表示されます。

ルート認証局コンテナの削除

ルート認証局コンテナを削除するには、次の手順を実行します。

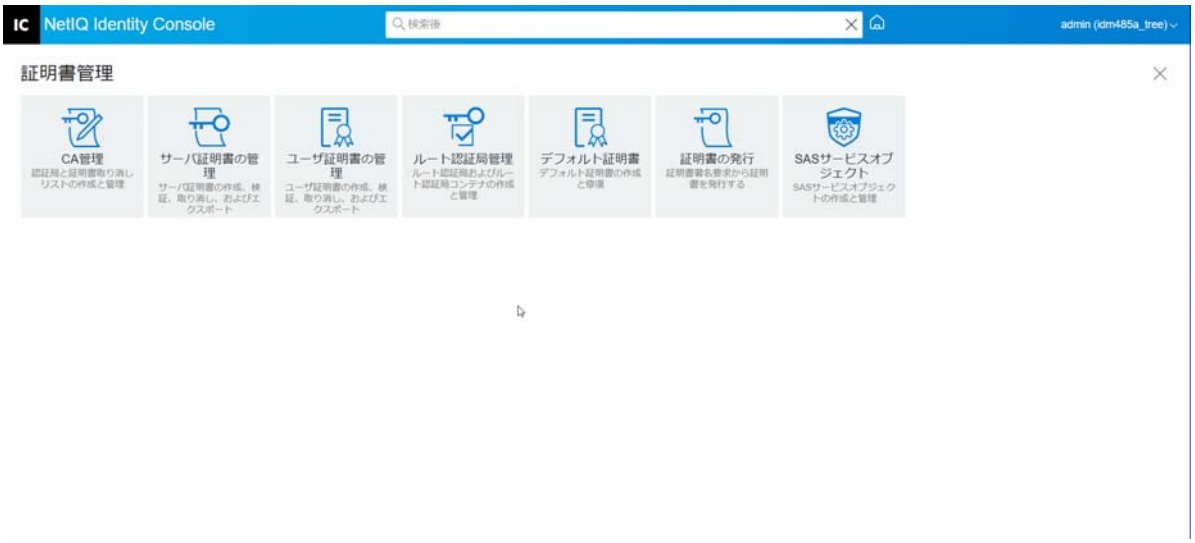
1 Identity Console のランディングページから、[**[証明書管理]**] > [**[ルート認証局管理]**] オプションをクリックします。デフォルトでは、[**[ルート認証局コンテナ]**] チェックボックスがオンです。

2 リストから適切なルート認証局コンテナを選択し、アイコンをクリックします。

3 警告画面で［ **[OK]**］をクリックします。

4 ルート認証局コンテナが正常に削除されたことを示す確認メッセージが表示されます。

図 17-4 *ルート認証局コンテナの管理*



デフォルトのサーバ証明書オブジェクトを作成する

証明書サーバをインストールすると、デフォルトのサーバ証明書オブジェクトが作成されます。

- SSL CertificateDNS - *server_name*
- サーバで設定した IP アドレスごとの証明書 (IPAG*xxx.xxx.xxx.xxx - server_name*)
- サーバで設定した DNS 名ごとの証明書 (DNSAG*www.example.com - server_name*)

注 : eDirectory では、SSL CertificateIP は自動的に作成されません。SSL 証明書 DNS には、[件名の代替名] にリストされているすべての IP が含まれます。Identity Console を使用してデフォルトの証明書を作成または修復しようとしても、デフォルトでは SSL CertificateIP 証明書は作成または修復されません。ただし、プラグインインタフェースに、デフォルトの動作を上書きして、強制的に SSL CertificateIP 証明書の作成 / 修復を実行することを選択できるチェックボックスがあります。

eDirectory 9.0 以降では、組織認証局に ECDSA 証明書があれば、ECDSA 証明書が自動的に作成されます。

何らかの理由でこれらの証明書が破損しているまたは無効になった場合、あるいは既存のデフォルト証明書を置換する場合は、次の手順に従って [Create Default Server Certificates] ウィザードを使用します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[デフォルト証明書]**] オプションをクリックします。
2. デフォルトの証明書を作成する 1 つまたは複数のサーバを選択し、[**[次へ]**] をクリックします。
3. 既存のデフォルトサーバ証明書を上書きする場合は [はい] を選択し、既存のデフォルトサーバ証明書が有効でないときにのみ上書きする場合は [いいえ] を選択します。
4. (単一サーバのみ) 既存の DNS アドレスを使用する場合は、そのオプションを選択します。別の DNS アドレスを使用する場合は、そのオプションを選択し新しい DNS アドレスを指定します。
5. (単一サーバのみ) 既存のデフォルト IP アドレスを使用する場合は、そのオプションを選択します。別の IP アドレスを使用する場合は、そのオプションを選択し新しい IP アドレスを指定します。
6. [**[次へ]**] をクリックします。
7. [概要] ページの内容を確認し、[**[終了]**] をクリックします。

サーバ証明書オブジェクトの作成をより細かく制御する場合は、サーバ証明書オブジェクトを手動で作成できます。詳細については、99 ページの 「サーバ証明書オブジェクトを作成する」を参照してください。

図 17-5 デフォルトのサーバ証明書オブジェクトを作成する

公開鍵証明書の発行

組織認証局は、外部認証局と同じ方法で機能します。つまり、証明書署名要求 (CSR) から証明書を発行する機能があります。ユーザが署名のために CSR を送信してきたら、組織認証局を使用して証明書を発行できます。証明書を要求したユーザは、発行された証明書を取得し、暗号化対応アプリケーションに直接インポートします。

このタスクでは、サーバ証明書オブジェクトを認識しない暗号化対応アプリケーション用の証明書を生成できます。

証明書を発行するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[証明書の発行]**] オプションをクリックします。
2. CSR ファイルをブラウズし、選択します。
3. キーの使用目的仕様で、適切なキータイプと対応するキーの使用目的を選択します。これらのオプションを使用してキータイプを選択できます。それぞれのキータイプには、キータイプに関連付けられた定義済みのキーの使用目的の値が設定されています。
   - **3a** **［指定なし］**: このオプションはデフォルトで選択されており、証明書のキーの使用目的のいずれもアクティブではありません。
   - **3b** **認証局** : このオプションでは、証明書署名と CRL 署名キーの使用目的がアクティブになります。
   - **3c** **暗号化** : このオプションを選択すると、キーの使用目的としてキー暗号化がアクティブになります。
   - **3d** **署名** : このオプションを選択すると、キーの使用目的としてデジタル署名がアクティブになります。
   - **3e** **SSL または TLS:** このオプションを選択すると、SSL または TLS トランザクションで使用できるようにキーが設定されます。

3f **カスタム**: このオプションを選択すると、キーの使用目的のいずれか、またはすべてを手動で選択できます。

3g **キーの使用目的拡張を重要に設定する**: [指定なし] 以外のキータイプが選択された状態で、そのキーの使用目的拡張を重要に設定することができます。証明書を使用するには、「重要」に設定された拡張が受信側のソフトウェアでサポートされている必要があります。したがって、アプリケーションは必ずしも証明書を使用できないことから、拡張を「重要」に設定することにはある程度のリスクが伴います。ただし、キーの使用目的のような既知の拡張の場合は、リスクは最小限に抑えられます。一般的に、キーの使用目的が指定されている場合は、拡張を重要に設定する必要があります。

4 証明書内の **[拡張キーの使用目的]** の拡張をエンコードできます。この機能をアクティブにするには、[**[拡張キーの使用目的を許可する]**] を選択します。

4a **サーバ**: このオプションは、サーバ認証による拡張キーの使用目的をアクティブにします。

4b **ユーザ**: このオプションは、ユーザ認証および電子メール保護による拡張キーの使用をアクティブにします。

4c **カスタム**: このオプションで、拡張キーの使用のいずれかまたはすべてを選択できます。

4d **任意**: 拡張キーのどの使用に対してもキーを使用できます。

4e **キーの拡張使用目的のエクステンションを「重要」に設定する**: 証明書を使用するには、「重要」に設定された拡張が受信側のソフトウェアでサポートされている必要があります。したがって、アプリケーションは必ずしも証明書を使用できないことから、拡張を「重要」に設定することにはある程度のリスクが伴います。多くのアプリケーションでは拡張キー使用目的の拡張を認識しないため、この拡張を「重要」とマークすると、特定のアプリケーションによって証明書が受諾されない大きなリスクが発生します。したがって、必要な場合以外は「重要」と設定しないでください。

5 適切な **[基本制約条件]** を選択します。

5a **証明書タイプ**:

5a1 **[指定なし]**: 証明書の基本制約条件を拡張しない場合は、このオプションを選択します。

5a2 **認証局**: 証明書の認証局基本制約条件を拡張する場合は、このオプションを選択します。認証局用の証明書の場合は、このオプションを選択する必要があります。

5a3 **エンドエンティティ**: 証明書に対して、(認証局でない) エンドエンティティ証明書であると指定する基本制約条件を拡張するには、このオプションを選択します。メモ : 証明書のタイプがエンドエンティティである場合は、パスの長さを [指定なし] に設定します。

5b **[パス長]**:

5b1 **[指定なし]**: この CA 下で作成できるサブオーディネート CA のレベル数を指定しない場合、このオプションを選択します。

注: 証明書のタイプがエンドエンティティである場合は、パスの長さを [指定なし] に設定します。

5b2 **［固有］**: この CA 下で作成できるサブオーディネート CA のレベル数を指定する場合、このオプションを選択します。上矢印と下矢印をクリックして、パスの長さを指定します。

注 : 作成された証明書が従属 CA である場合、パスの長さは上位の CA と一致していなければなりません。たとえば、上位の CA のパスの長さが 3 である場合、サブオーディネートのパスの長さは 2 以下でなければなりません。上位の CA のパスの長さが指定されていない場合、サブオーディネートのパスの長さも指定されないか、または任意の長さになります。

5c **［基本制約条件の拡張を「重要」に設定］**: 一般的に基本制約条件の拡張は、CA 証明書に対して「重要」に設定する必要があります。証明書を使用するには、「重要」に設定された拡張が受信側のソフトウェアでサポートされている必要があります。したがって、アプリケーションは必ずしも証明書を使用できないことから、拡張を「重要」に設定することにはある程度のリスクが伴います。ただし、基本制約条件のような既知の拡張の場合は、リスクは最小限に抑えられます。

6 次の証明書パラメータを指定します。

6a **サブジェクト名 :** eDirectory ツリーの完全識別名が表示されます。

6b **サブジェクト名 :** eDirectory ツリーの完全識別名が表示されます。

6c **有効期間 :** ドロップダウンリストを使用して、証明書が有効になる期間を指定します。範囲は最短で 6ヶ月から、最長で 2036 年 (32 ビット時刻値に基づく時間制限) まで指定できます。［日付の指定］オプションを選択する場合、［発効日］および［有効期限］フィールドを編集して、カスタムの有効期間を作成することができます。最長の日付は認証局の有効期限の範囲内で選択する必要があります。

6c1 **有効開始日 :** 証明書が有効になる日時を表示または編集できます。

6c2 **有効期限日 :** 証明書が無効になる日時を表示または編集できます。

6d **カスタム拡張 :** この機能により、作成する証明書に含める標準拡張またはカスタム拡張を、Certificate Server でサポートできるようになります。拡張は、あらかじめ作成してファイルに格納しておく必要があります (1 ファイルにつき 1 つの拡張)。拡張は、IETF RFC 2459/3280 セクション 4.2 の定義に従って、ASN.1 でエンコードされている必要があります。

作成中の証明書に 1 つ以上のカスタム拡張機能を含めるには、［新規］をクリックし、カスタム拡張機能を含むファイルをブラウズして、証明書に追加します。このプロセスを繰り返すことで、複数の拡張機能を追加できます。

カスタム拡張ファイルを削除するには、ファイルを選択して、  アイコンをクリックします。

7 次のオプションから適切な証明書形式を選択します。

7a **バイナリ DER 形式のファイル :** このオプションを使用すると、ファイル名フィールドに表示されるファイルに証明書を保存またはエクスポートできます。デフォルトでは、証明書ファイルには .DER 拡張子が付けられ、Windows ベースの

Identity Console ワークステーションでは C ドライブのルートに、また Linux ベースの Identity Console ワークステーションではホームディレクトリにエクスポートされます。

7b **Base64 形式のファイル :** このオプションを使用すると、CSR の保存やファイル名フィールドに表示されているファイルに証明書をエクスポートできます。デフォルトでは、証明書ファイルおよび CSR ファイルには .B64 拡張子が付けられ、Windows ベースの Identity Console ワークステーションでは C ドライブのルートに、また Linux ベースの Identity Console ワークステーションではホームディレクトリにエクスポートされます。

7c **CER 形式のファイル :** このオプションを使用すると、CSR の保存やファイル名フィールドに表示されているファイルに証明書をエクスポートできます。デフォルトでは、証明書ファイルおよび CSR ファイルには .CER の拡張子が付けられ、Windows ベースの Identity Console ワークステーションでは C ドライブのルートに、また Linux ベースの Identity Console ワークステーションではホームディレクトリにエクスポートされます。

8 次の画面で証明書の概要を確認し、[**[OK]**] をクリックします。

9 証明書が正常に発行されたことを示す確認メッセージが表示されます。

図 17-6 公開鍵証明書の発行

SAS Service オブジェクトの管理

SAS Service オブジェクトは、サーバとサーバ証明書間の通信を容易にします。サーバを eDirectory ツリーから削除する場合は、サーバに関連付けられた SAS Service オブジェクトを削除する必要があります。サーバをツリーに戻す場合は、そのサーバに属する SAS Service オブジェクトを作成する必要があります。ツリーに戻さない場合は、新しいサーバ証明書を作成することはできません。

SAS Service オブジェクトは、サーバヘルスチェックの一部として自動的に作成されます。このオブジェクトを手動で作成する必要はありません。

新しい SAS Service オブジェクトを作成できるのは、サーバオブジェクトと同じコンテナ内に、正しく名付けられた SAS Service オブジェクトが存在しない場合だけです。たとえば、「WAKE」と名付けられたサーバでは、「SAS Service- WAKE」と名付けられた SAS Service オブジェクトが作成されます。ユーティリティでは、サーバオブジェクトから SAS Service までの DS ポインタ、および SAS Service からサーバオブジェクトまでの DS ポインタが追加されます。また、SAS サービスオブジェクト上に正しい ACL エントリが設定されます。

SAS サービスオブジェクトがすでに正しい名前で存在する場合、新しい SAS サービスオブジェクトを作成することはできません。古い SAS サービスオブジェクトの DS ポインタは、誤っていたり見つからなかったりする場合があります。または、ACL が適切でない場合もあります。この場合、破損した SAS サービスオブジェクトを削除し、Identity Console ポータルを使用して新しい SAS サービスオブジェクトを作成できます。

SAS サービスオブジェクトの作成または削除

SAS サービスオブジェクトを作成または削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[証明書管理]**] > [**[SAS サービスオブジェクト]**] オプションをクリックします。
2. 既存のサーバに対して SAS サービスオブジェクトが作成されていない場合は、＋アイコンをクリックして新しい SAS サービスオブジェクトを作成します。
3. SAS サービスオブジェクトが正常に作成されたことを示す確認メッセージが表示されます。
4. SAS サービスオブジェクトを削除するには、🗑アイコンをクリックします。
5. 確認画面で［ **[OK]**］をクリックして、SAS サービスオブジェクトを正常に削除します。

図 17-7 *SAS サービスオブジェクトの管理*

18 認証フレームワークの管理

認証モジュールを使用して、次のタスクを実行できます。

ログインとポストログインのメソッドとシーケンスの管理

NMAS には、NetIQ とサードパーティ認証開発者による複数のログインメソッドとポストログインメソッドのサポートが含まれます。メソッドによっては、追加のハードウェアやソフトウェアが必要な場合があります。使用するメソッドに必要なすべてのハードウェアとソフトウェアが揃っていることを確認してください。

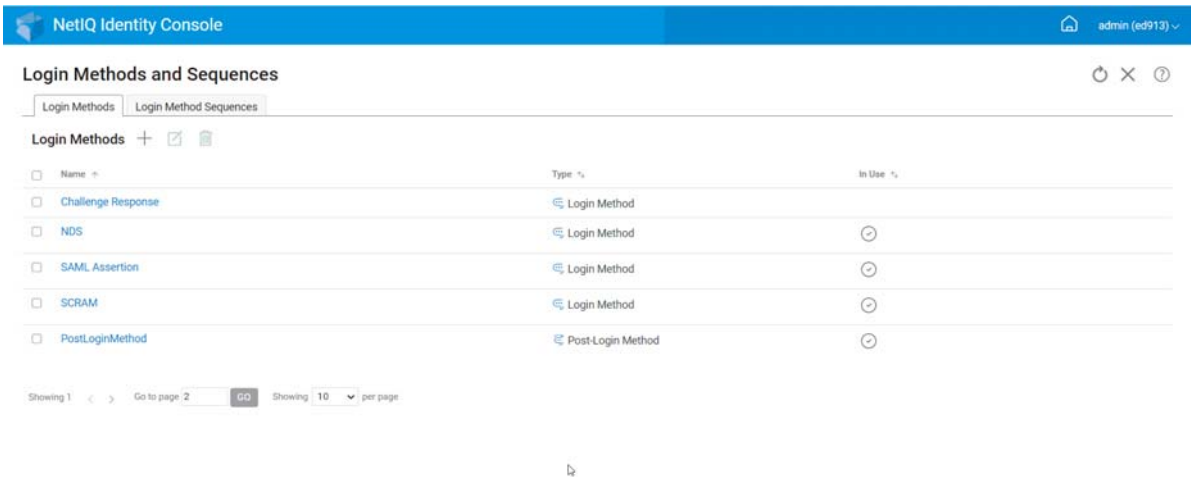
このセクションでは、NMAS 用のログインとポストログインのメソッドとシーケンスのインストール、セットアップ、および設定方法について説明します。

ログインメソッドまたはポストログインメソッドのインストール

ログインメソッドをインストールするには、次のタスクを実行します。

1. Identity Console のランディングページから、[**認証管理**] > [**ログインのメソッドとシーケンス**] オプションをクリックします。
2. ＋アイコンをクリックして、新しいログインメソッドをインストールします。
3. インストールするログインメソッド (.zip) ファイルをブラウズし、選択した後に [**次へ**] をクリックします。
4. インストールウィザードに従って、ログインメソッドのインストールプロセスを完了します。

図 18-1 新しいログインメソッドのインストール

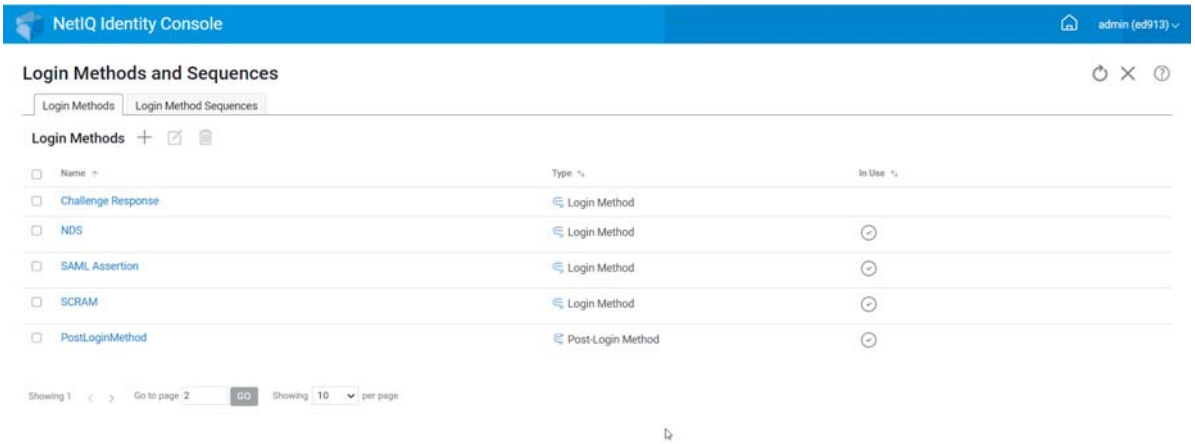


既存のログインメソッドまたはポストログインメソッドの更新

既存のログインメソッドを更新するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。
2. リストから更新するログインメソッドを選択し、アイコンをクリックします。
3. アップデートするログインメソッド (.zip) ファイルをブラウズし、選択した後に [**[次へ]**] をクリックします。
4. 更新ウィザードに従って、ログインメソッドの更新を完了します。

図 18-2 既存のログインメソッドの更新



ログインメソッドまたはポストログインメソッドのアンインストール

ログインメソッドまたはポストログインメソッドをアンインストールするには、次の手順を実行します。

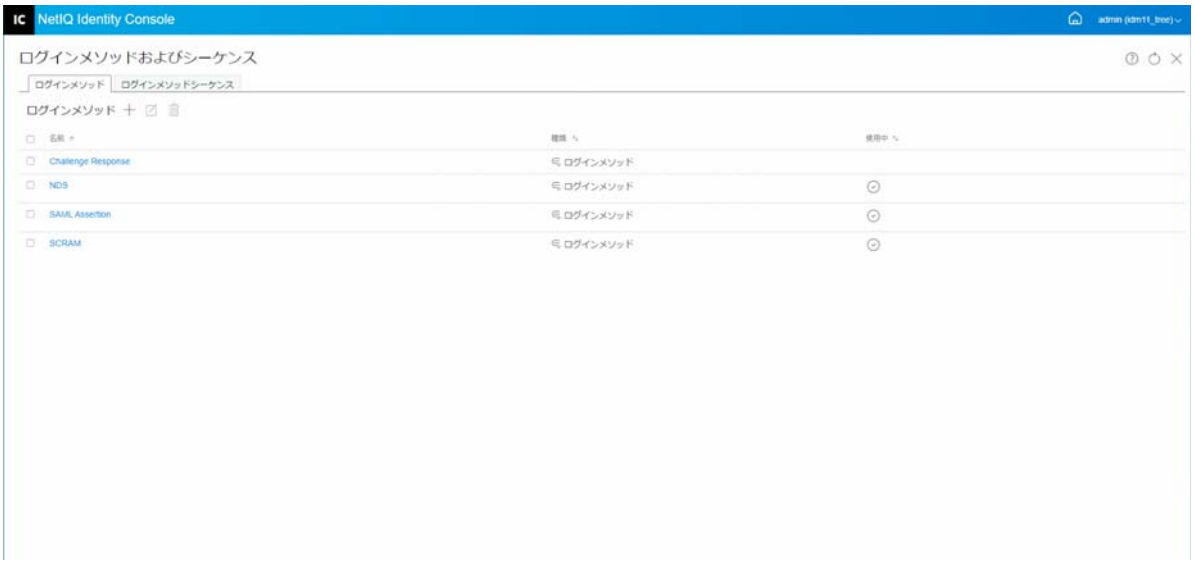
1 Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。

2 リストからアンインストールするログインメソッドを選択し、アイコンをクリックします。

3 次の画面で［ **[OK]**］をクリックします。

4 ログインメソッドがアンインストールされたことを示す確認メッセージが表示されます。

図 18-3 *ログインメソッドのアンインストール*



新しいログインメソッドシーケンスの作成

環境に合ったさまざまなログインメソッドを作成したら、これらのメソッドを使用する順序を決めることができます。新しいログインメソッドシーケンスを作成するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。

2 [**[ログインメソッドシーケンス]**] タブを選択します。

3 ＋アイコンをクリックして、新しいログインメソッドシーケンスを作成します。

4 **[名前]** を指定し、**[シーケンスタイプ]** を選択します。

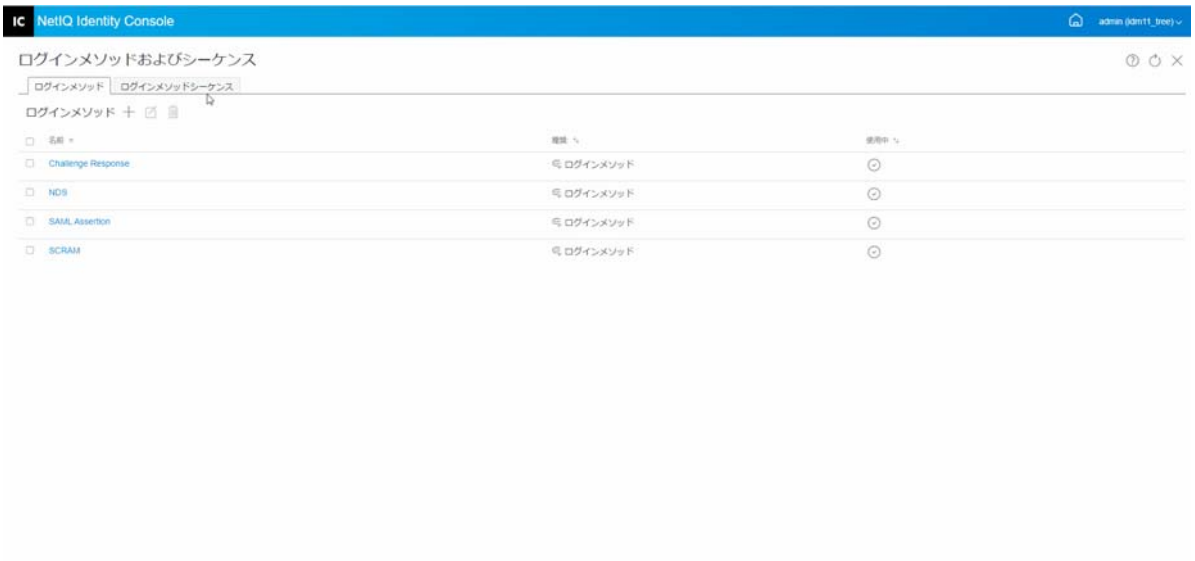
5 使用可能なログインメソッドとポストログインメソッドのリストから、必要なログインメソッドとポストログインメソッドを選択します。

注 : ログインメソッドオブジェクトに表示される上矢印と下矢印をクリックして、ログインメソッドの順序を決められます。

6 [**[作成]**] ボタンをクリックします。

7 新しいログインメソッドシーケンスが正常に作成されたことを示す確認メッセージが表示されます。

図 18-4 *ログインメソッドシーケンスの作成*



ログインメソッドシーケンスの変更

既存のログインメソッドシーケンスを変更するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。

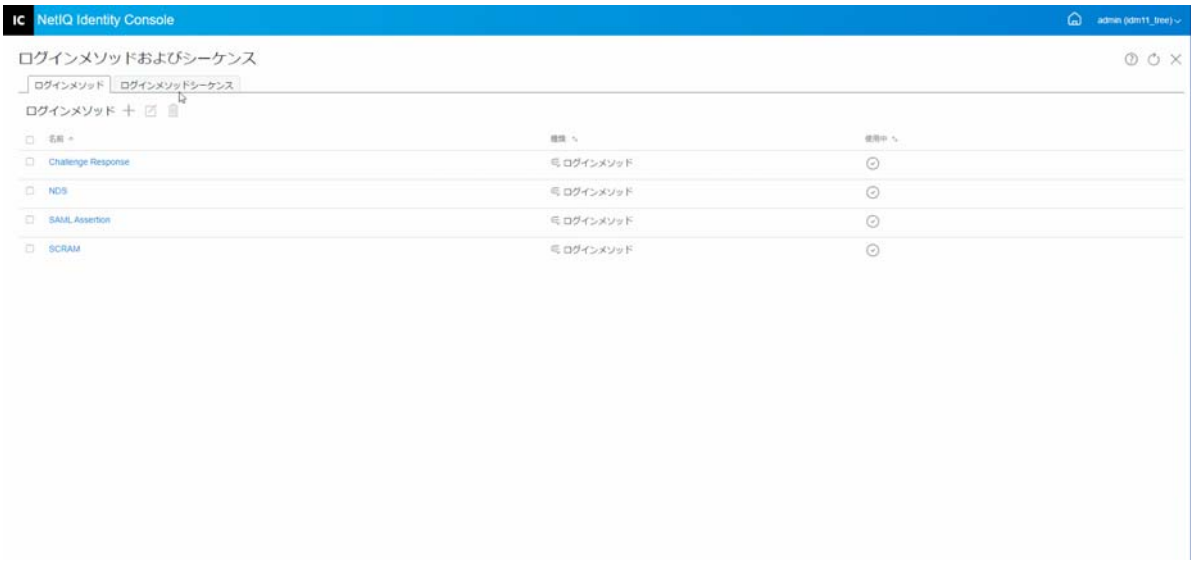
2 [**[ログインメソッドシーケンス]**] タブを選択します。

3 既存のログインメソッドシーケンスを変更するには、アイコンをクリックします。

4 [**[ログインメソッドシーケンスの変更]**] ページで必要な変更を行い、[**[保存]**] をクリックします。

5 ログインメソッドシーケンスが正常に変更されたことを示す確認メッセージが表示されます。

図 18-5 ログインメソッドシーケンスの変更



ログインメソッドシーケンスの認証または認証の解除

ログインメソッドシーケンスをユーザ、コンテナ、およびパーティションに関連付けるには、認証し、デフォルトに設定する必要があります。ログインメソッドシーケンスを認証するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。
2. [**[ログインメソッドシーケンス]**] タブを選択します。
3. リストから適切なログインメソッドシーケンスを選択し、⊘アイコンをクリックします。
4. ログインメソッドシーケンスの認証を取り消すには、ログインメソッドシーケンスを選択して、⊗アイコンをクリックします。
5. または、ログインメソッドシーケンスリストの [**[承認済み]**] 列の下にあるドロップダウンメニューから、ログインメソッドシーケンスの認証または認証の取り消しをすることもできます。

図 18-6 ログインメソッドシーケンスの認証または認証の解除

デフォルトログインメソッドシーケンスの設定

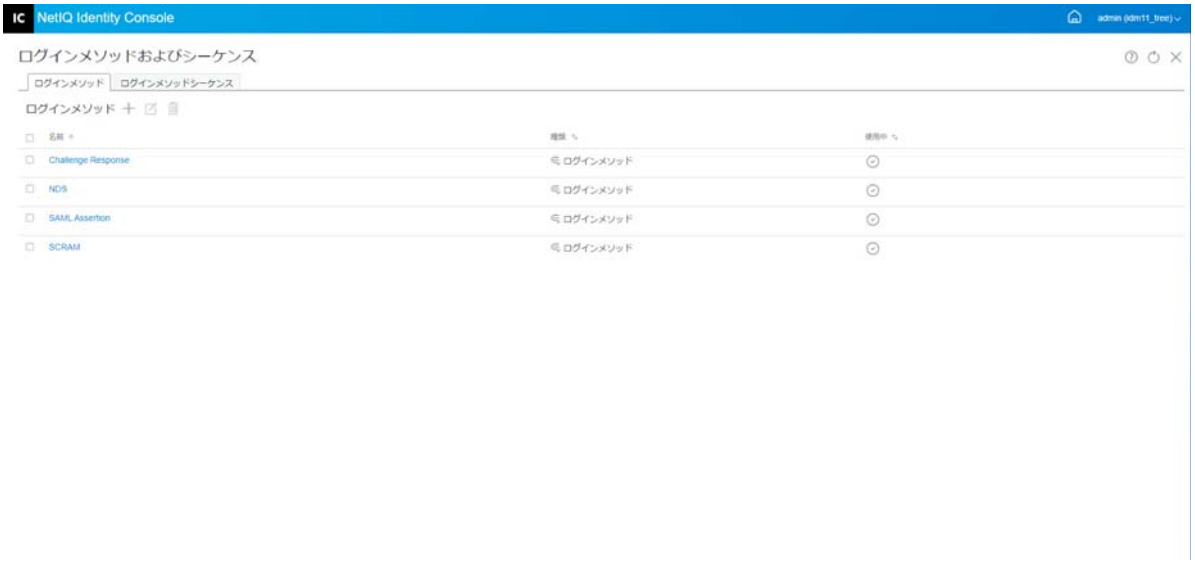
ユーザがログイン時にログインシーケンスを指定する必要がないようにデフォルトログインシーケンスを設定するには :

1 Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。

2 [**[ログインメソッドシーケンス]**] タブを選択します。

3 認証されたログインメソッドシーケンスをデフォルトに設定するには、アイコンを有効にしてください。

図 18-7 デフォルトログインメソッドシーケンスの設定

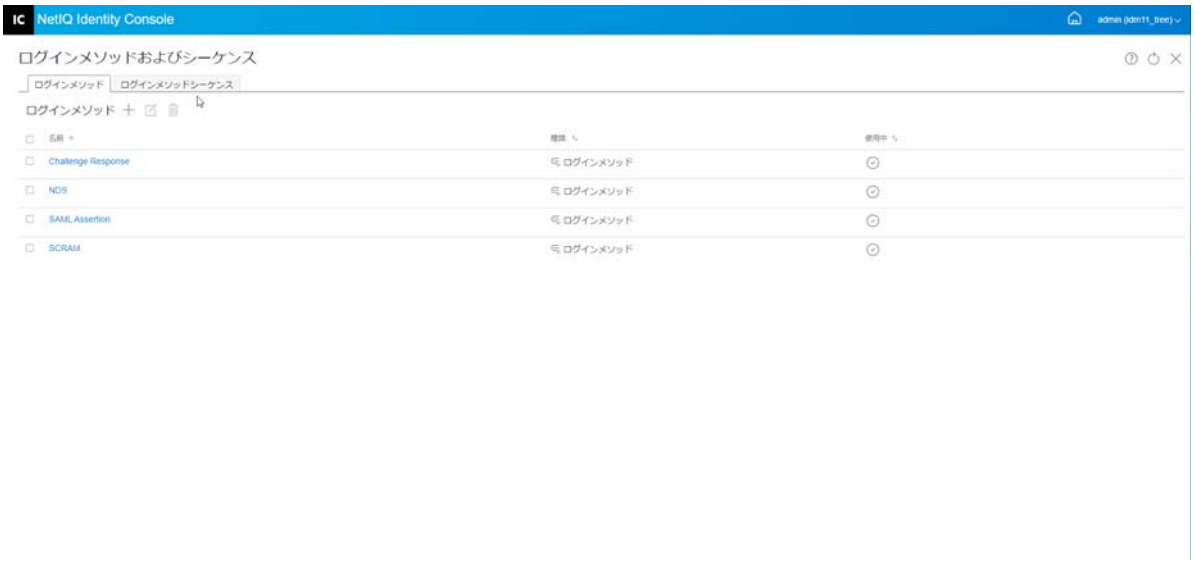


ログインメソッドシーケンスの削除

ログインメソッドシーケンスを削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[ログインのメソッドとシーケンス]**] オプションをクリックします。
2. [**[ログインメソッドシーケンス]**] タブを選択します。
3. リストから適切なログインメソッドシーケンスを選択し、アイコンをクリックします。
4. 次の確認画面で [**[OK]**] をクリックします。

図 18-8 *ログインメソッドシーケンスの削除*



パスワードポリシーの管理

Password Policy (パスワードポリシー) は、エンドユーザパスワードの作成および交換に関する基準を指定した管理者定義ルールの集まりです。NMAS を使用すると、eDirectory のユーザに割り当てるパスワードポリシーを強制できます。パスワードポリシーには [パスワードを忘れた場合] セルフサービス機能を含めて、パスワードを忘れた場合のヘルプデスクへの呼び出しを減らすこともできます。セルフサービス機能としては、パスワードリセットセルフサービスもあります。パスワードリセットセルフサービスでは、ユーザが管理者によってパスワードポリシーに指定されたルールを確認しながら、自分のパスワードを変更することができます。ユーザはこれらの機能に、Identity Manager ユーザアプリケーションまたは Identity Console からアクセスします。

パスワードポリシーモジュールを使用して、次のタスクを実行できます。

- 120 ページの 「デフォルト設定を使用したパスワードポリシーの作成」
- 120 ページの 「カスタム設定値を使用したパスワードポリシーの作成」

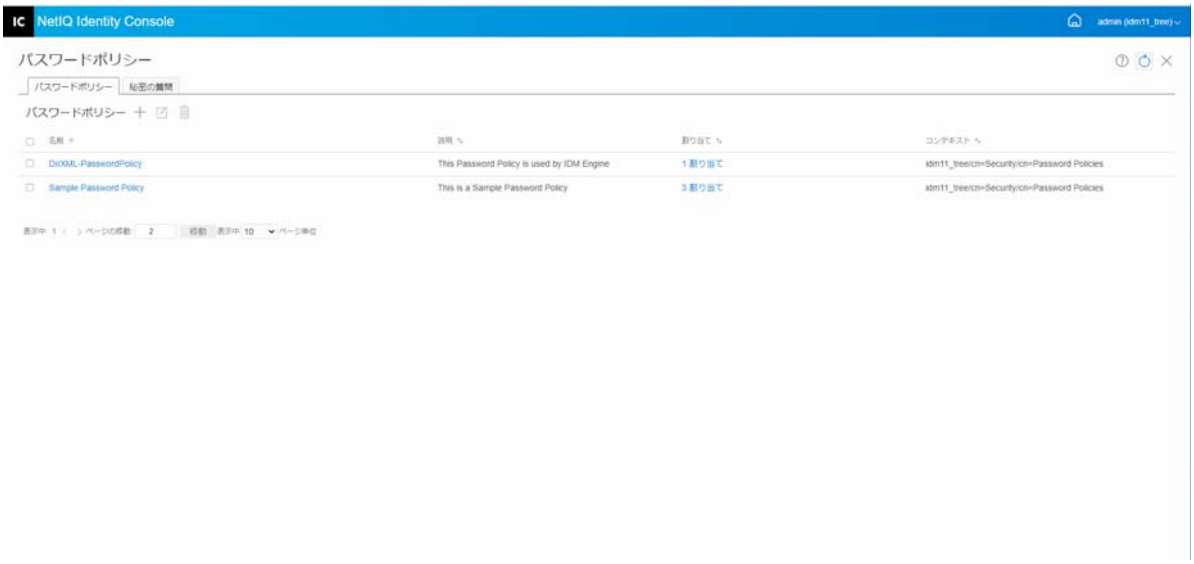
- 124 ページの 「パスワードポリシーの変更」
- 125 ページの 「パスワードポリシーの削除」

デフォルト設定を使用したパスワードポリシーの作成

新しいパスワードポリシーを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] オプションをクリックします。
2. ＋アイコンをクリックして、新しいパスワードポリシーを作成します。
3. 次の画面で、名前、コンテキスト、説明、およびパスワード変更メッセージを指定します。
4. デフォルト設定でパスワードポリシーを作成する場合は、[**[Create a new Password Policy based on default settings（デフォルト設定に基づいて新しいパスワードポリシーを作成する）]**] チェックボックスをオンにし、[**[次へ]**] をクリックして [**[概要]**] ページを表示します。
5. [**[概要]**] ページで詳細を確認し、[**[作成]**] をクリックします。
6. パスワードポリシーが正常に作成されたことを示す確認メッセージが表示されます。

図 18-9 *デフォルト設定を使用したパスワードポリシーの作成*



カスタム設定値を使用したパスワードポリシーの作成

カスタム設定値でパスワードポリシーを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] オプションをクリックします。
2. ＋アイコンをクリックして、新しいパスワードポリシーを作成します。
3. 次の画面で、名前、コンテキスト、説明、およびパスワード変更メッセージを指定します。

4 カスタム設定値でパスワードポリシーを作成する場合は、[**[次へ]**] をクリックします。

5 [**[環境設定]**] ページで次のアクションを実行します。

5a ユニバーサルパスワードを有効にする : ポリシーにユニバーサルパスワードを有効にすることで、[パスワードポリシー] 機能のオプションを使用できるようになります。ただし、ポリシーでユニバーサルパスワードを有効にする前に、使用環境でユニバーサルパスワードの前提条件を満たしている必要があります。

5b 高度なパスワードルールを有効にする : このオプションにより、[高度なパスワードルール] にあるパスワードルールが有効になります。これらのルールは、パスワードの有効期間や文字、数字、大文字または小文字、特殊文字の組み合わせなどのパスワードの内容を制御することで、環境のセキュリティを確保するのに役立ちます。会社名などの、安全でないと思われるパスワードを除外することができます。

5c パスワード同期 : これらのオプションでは、eDirectory 内で、ユニバーサルパスワードが他のタイプのアイデンティティボールトパスワードと同期する方法を指定します。パスワード同期には、次のオプションが含まれます。

5c1 Remove NDS password when setting Password(パスワードを設定するときに NDS パスワードを削除する): このオプションを選択すると、ユニバーサルパスワードが設定されるときに NDS パスワードが無効になります。ユーザは、NMAS と通信する代わりに、NDS パスワードで直接ログインする古いメソッドやユーティリティを使用できなくなります。このオプションを設定すると、次のオプション [**[パスワードの設定時に NDS パスワードを同期する]**] がデフォルトで無効になります。

5c2 Synchronize NDS password when setting Password(パスワードを設定するときに NDS パスワードを同期する): このオプションを選択すると、Identity Console などのアプリケーションにおいても、ユニバーサルパスワードの設定を NDS パスワードに変更できます。

5c3 Synchronize Simple Password when setting Password(パスワードを設定するときに単純パスワードを同期する): このオプションは、単純パスワードおよびユーザプロビジョニングを使用する NetIQ クライアントおよびサードパーティクライアントとの互換性を提供します。

5c4 Synchronize Distribution Password when setting Password(パスワードを設定するときに配布パスワードを同期する): このオプションにより、メタディレクトリエンジンが eDirectory 内でユーザのユニバーサルパスワードを取得または設定できるかどうかが決まります。

5d Universal Password Retrieval: 次のオプションを指定できます。

5d1 Allow user to retrieve password: ユーザエージェントにパスワードの取得を許可します。このオプションにより、パスワードを電子メールでユーザに送信できるようにするため、[パスワードを忘れた場合] セルフサービス機能がユー

ザに代わってパスワードを取得するかどうかを指定します。このオプションを選択しない場合、パスワードポリシーの［パスワードを忘れた場合］タブにある、対応する機能は選択できなくなります。

5d2 **管理者にパスワードの取得を許可する :** この機能を必要とする特定のサービスがある場合、このボックスを選択します。Identity Manager の場合、管理者がパスワードを取得する必要はありません。ただし、一部のサードパーティサービスはこのオプションを利用する場合があります。

5d3 **パスワードの取得を次のユーザに許可する :** ＋アイコンをクリックして、パスワードを取得することになっている適切なユーザを選択します。

5e **認証 :**

5e1 **既存のパスワードがパスワードポリシーに準拠するかどうかを確認します (検証はログイン時に実行されます):** このオプションでは、新しいパスワードポリシーを導入するときや、既存のポリシーの［高度なパスワードルール］を変更する場合に、既存のパスワードが新しいルールや変更済みのルールに準拠していることを確認できます。

このオプションを選択すると、ユーザがログインするときに、既存のパスワードが分析されることで、新しいまたは変更済みの［高度なパスワードルール］に準拠していることを確認できます。既存のパスワードがルールに準拠していない場合、ユーザはそのパスワードを変更するように求められます。

完了したら、［**[次へ]**］をクリックします。

6 **[高度なパスワードルール]** は、パスワードの有効期間、パスワードの変更頻度、パスワードに含まれる内容などのパスワードの詳細を制御することで、環境のセキュリティを確保するのに役立ちます。

特殊文字とは、数字 (0-9) でもなく、アルファベット文字でもない文字を指します。

［高度なパスワードルール］ページで次のアクションを実行します。

6a Microsoft Complexity Policy (Microsoft Windows Server 2008 より前)、Microsoft Server 2008 パスワードポリシー、または Novell 構文を使用して、パスワード構文の設定を管理できます。

6b ウィザードでパスワード変更、パスワード有効期間、パスワードの長さと構成、およびパスワードの除外に必要なオプションを指定し、［**[次へ]**］をクリックします。

7 ユーザがパスワードを忘れたときの［**[パスワードを忘れた場合]**］セルフサービスを有効にすることで、ヘルプデスクのコストを削減できます。ユーザは、Identity Console ポータルからこれらのセルフサービス機能にアクセスできます。［パスワードを忘れた場合］ページで次のアクションを実行します。

注 : [パスワードを忘れた場合] を有効にする場合は、ユーザのログインを支援する [秘密の質問] が必要かどうかを指定する必要があります。

7a **秘密の質問 :** 秘密の質問を使用する場合、ユーザは秘密の質問に答えるまで [パスワードを忘れた場合] セルフサービスを使用できません。ユーザに Identity Console ポータルからこの情報を入力するように求めるようにするには、[**[秘密の質問を要求する]**] オプションを選択します。

7b **アクション :** このタブで使用できるオプションを使用すると、ユーザは秘密の質問とユニバーサルパスワードを使用してパスワードをリセットしたり、現在のパスワードやパスワードヒントを電子メールで送信したり、パスワードヒントオプションを表示したりできます。

7c **認証 :** [**[認証時にユーザにセキュリティクエスチョンやヒントの設定を強制する]**] ボックスを選択すると、秘密の質問またはパスワードヒントの指定がユーザに求められます。

完了したら、[**[次へ]**] をクリックします。

8 ポリシーは、1 つ以上のオブジェクトに割り当てるまでは有効になりません。管理を簡素化するには、ツリー内のできるだけ高い位置にポリシーを割り当てることをお勧めします。パスワードポリシーは、次のオブジェクトに割り当てることができます。

8a **ログインポリシーオブジェクト :** ツリー内のすべてのユーザに対してデフォルトのパスワードポリシーを作成し、セキュリティコンテナにあるログインポリシーオブジェクトに割り当てることをお勧めします。

8b **パーティションのルートであるコンテナ :** パーティションルートのコンテナにポリシーを割り当てる場合、そのパーティション内のすべてのユーザ (サブコンテナを含む) は、そのポリシーの割り当てを継承します。

8c **パーティションのルートではないコンテナ :** パーティションのルートではないコンテナにポリシーを割り当てる場合、その特定のコンテナに保存されたユーザのみがポリシーの割り当てを継承します。サブコンテナ内のユーザはポリシーを継承しません。

パーティションルートでないコンテナ内のすべてのユーザにポリシーを適用するには、ポリシーを各サブコンテナにそれぞれ割り当てます。

8d **ユーザ :** ポリシーは、1 人以上のユーザに割り当てることができます。

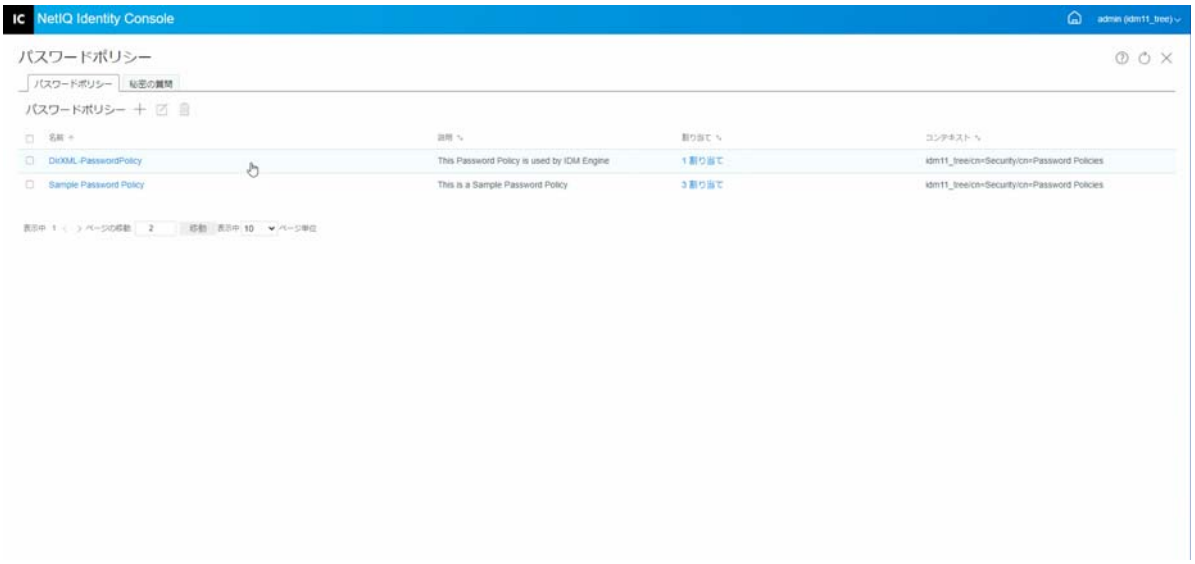
ポリシーを割り当てるには、+ アイコンをクリックします。次に、パスワードポリシーを割り当てる適切なオブジェクトをブラウズし、選択します。

ポリシーの関連付けを削除する場合は、リストからポリシーを選択し、🗑 アイコンをクリックします。

9 [**[概要]**] ページで詳細を確認し、[**[作成]**] をクリックします。

10 パスワードポリシーが正常に作成されたことを示す確認メッセージが表示されます。

図 18-10 カスタム設定値を使用したパスワードポリシーの作成

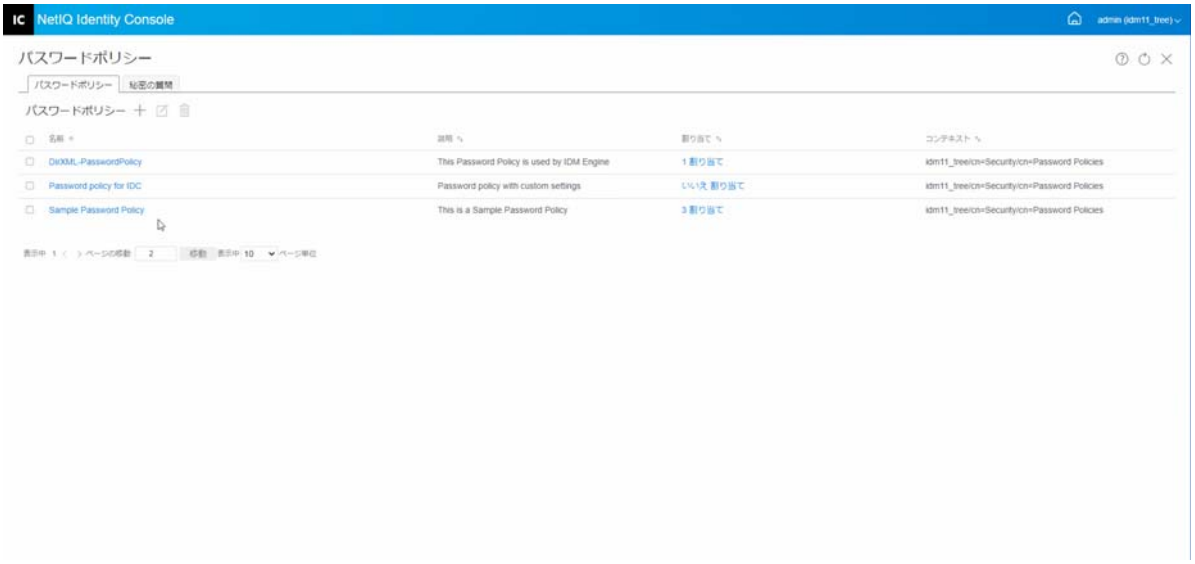


パスワードポリシーの変更

既存のパスワードポリシーを変更するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] オプションをクリックします。
2. リストから適切なパスワードポリシーを選択して、アイコンをクリックします。
3. [**[パスワードポリシーの変更]**] ページで必要な変更を行い、[**[保存]**] をクリックします。

図 18-11 パスワードポリシーの変更



パスワードポリシーの削除

パスワードポリシーを削除するには、次の手順を実行します。

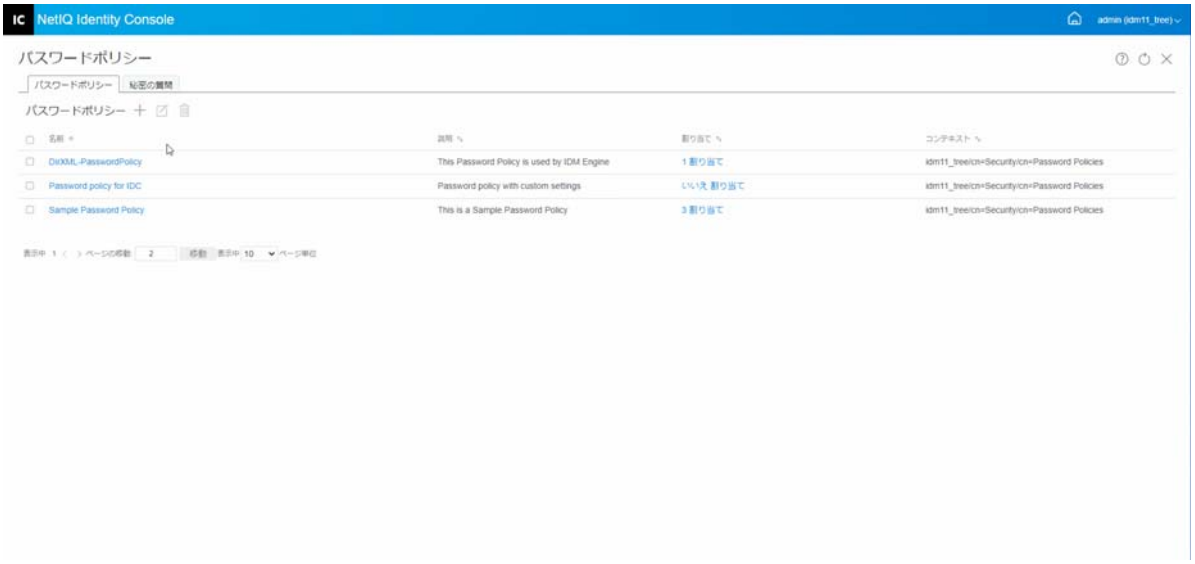
1 Identity Console のランディングページから、[[認証管理]] > [[パスワードポリシー]] オプションをクリックします。

2 リストから適切なパスワードポリシーを選択して、アイコンをクリックします。

3 次の警告画面で、[[OK]] をクリックします。

4 パスワードポリシーが削除されたことを示す確認メッセージが表示されます。

図 18-12 パスワードポリシーの削除



秘密の質問の管理

[秘密の質問] は、ユーザが自分の識別情報を検証するために回答する 1 つ以上の質問です。秘密の質問は、パスワードセルフサービスの一部です。

パスワードを思い出せない場合や、パスワードを使用できない場合は、ヘルプデスクに問い合わせる代わりに、パスワードセルフサービスを使用できます。[秘密の質問] により、ユーザは、識別情報の妥当性を確認してから、電子メールでヒントまたはパスワードを受け取ったり、Web ブラウザを使用してパスワードをリセットしたりできます。

ユーザに固有の質問を作成させて回答させたり、管理者が作成した質問に回答させたりできます。

[秘密の質問] ページでは、既存の秘密の質問の検索、新しい秘密の質問の作成、および既存の秘密の質問の編集を行うことができます。

- 126 ページの 「新しい秘密の質問の作成」
- 126 ページの 「秘密の質問の変更」
- 127 ページの 「秘密の質問の削除」

新しい秘密の質問の作成

新しい秘密の質問を作成するには、次の手順を実行します。

1 Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] > [**[秘密の質問]**] の順にクリックします。

2 ＋アイコンをクリックして、新しい秘密の質問を作成します。

3 秘密の質問オブジェクトの名前を指定し、秘密の質問を作成するコンテナまたはサブコンテナを選択します。

4 ユーザのパスワードを取得するために尋ねられる新しい一連の質問を作成します。また、既存のランダムな質問のセットから選択できます。

5 質問する質問数を設定し、[**[作成]**] をクリックします。

6 秘密の質問が正常に作成されたことを示す確認メッセージが表示されます。

図 18-13 *秘密の質問の作成*

秘密の質問の変更

既存の秘密の質問を変更するには、次の手順を実行します。

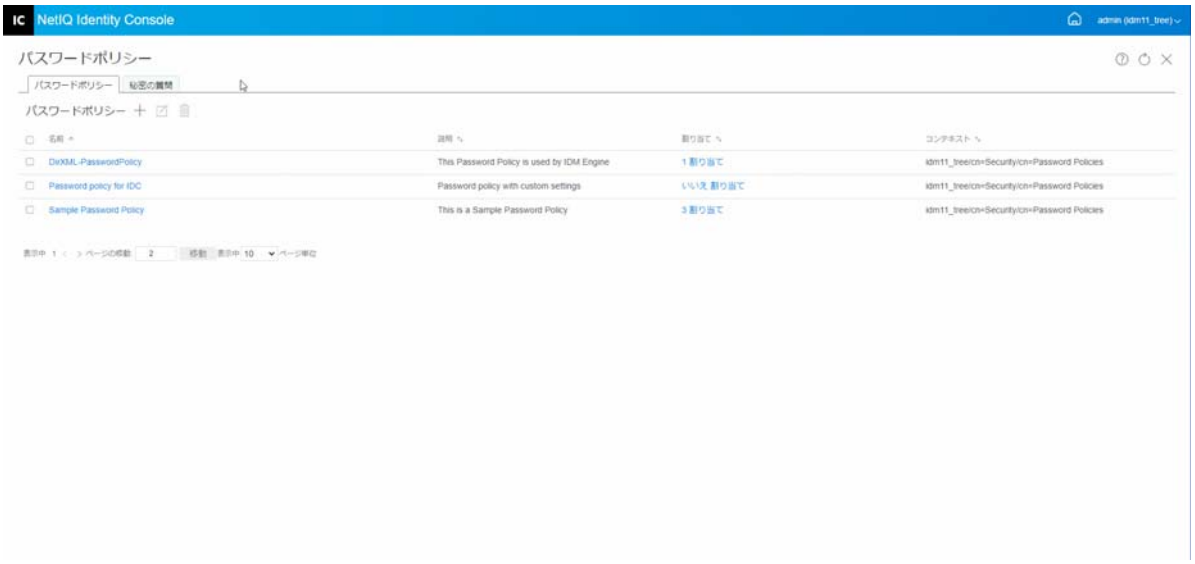
1 Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] > [**[秘密の質問]**] の順にクリックします。

2 リストから適切な秘密の質問を選択して、アイコンをクリックします。

3 [秘密の質問の変更] ページで必要な変更を行い、[**[保存]**] をクリックします。

4 秘密の質問が正常に変更されたことを示す確認メッセージが表示されます。

図 18-14 秘密の質問の変更

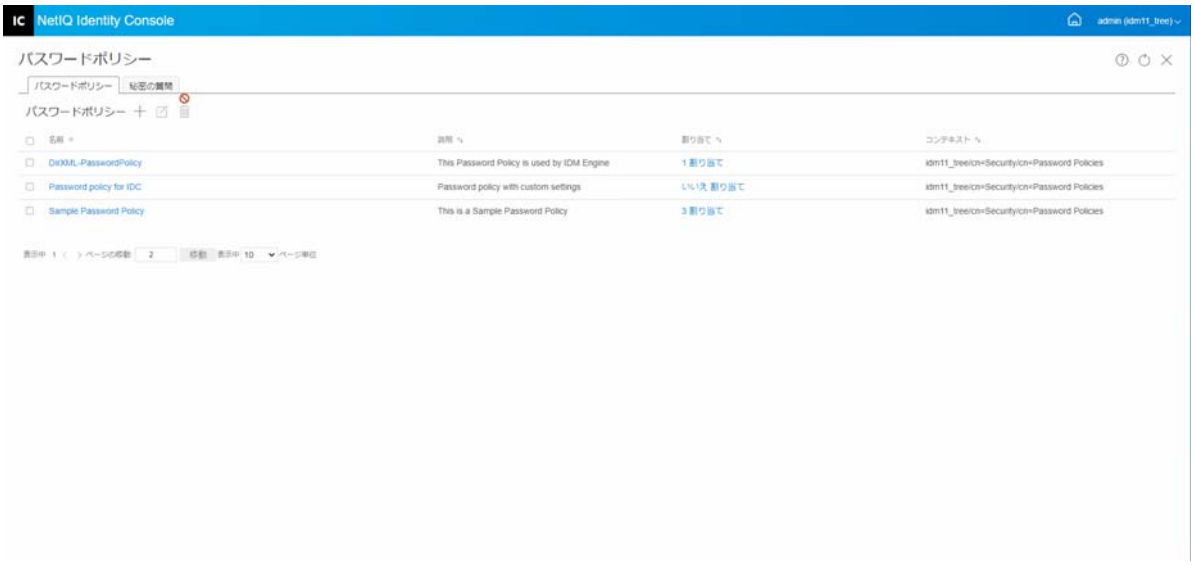


秘密の質問の削除

秘密の質問を削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[認証管理]**] > [**[パスワードポリシー]**] > [**[秘密の質問]**] の順にクリックします。
2. リストから必要な秘密の質問を選択して、🗑アイコンをクリックします。
3. 確認画面で [**[OK]** をクリックします。
4. 秘密の質問が正常に削除されたことを示す確認メッセージが表示されます。

図 18-15 秘密の質問の削除



19 SNMP グループオブジェクトの管理

SNMP(Simple Network Management Protocol) は、インターネットを介してデバイスを操作および保守するための標準的なプロトコルです。管理コンソールアプリケーションと管理対象デバイスは、このプロトコルに従って管理情報をやり取りします。

SNMP モジュールを使用して、次のタスクを実行できます。

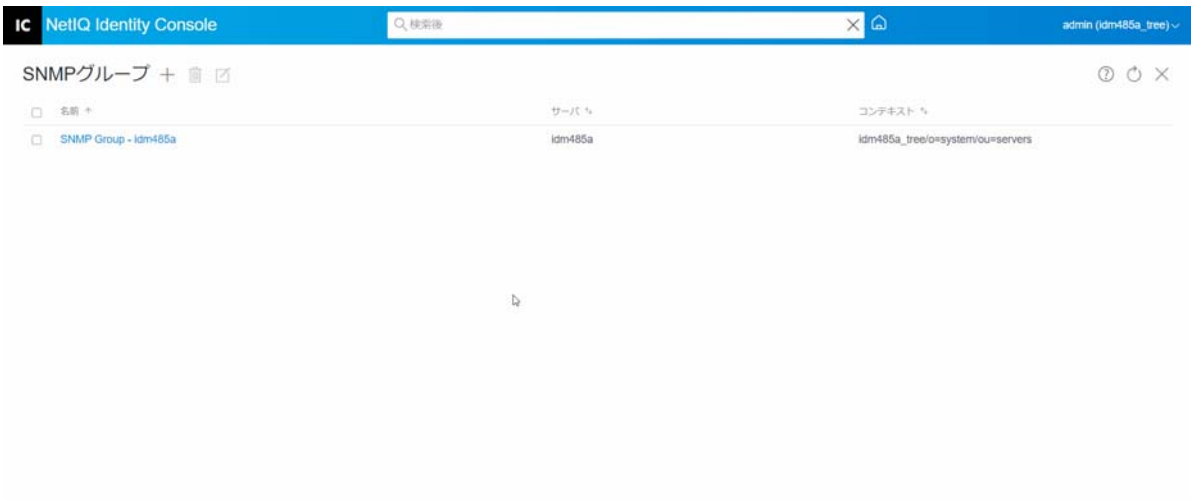
- 129 ページの 「SNMP グループオブジェクトの作成」
- 130 ページの 「SNMP グループオブジェクトの変更」
- 130 ページの 「SNMP グループオブジェクトの削除」

SNMP グループオブジェクトの作成

SNMP グループオブジェクトを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[SNMP]**] モジュールをクリックします。
2. ＋アイコンをクリックして、新しい SNMP グループオブジェクトを作成します。
3. 名前を指定し、新しい SNMP グループオブジェクトを作成するコンテキストを選択します。
4. [**[作成]**] ボタンをクリックします。
5. SNMP グループオブジェクトが正常に作成されたことを確認するメッセージが画面に表示されます。

図 19-1 *SNMP グループオブジェクトの作成*

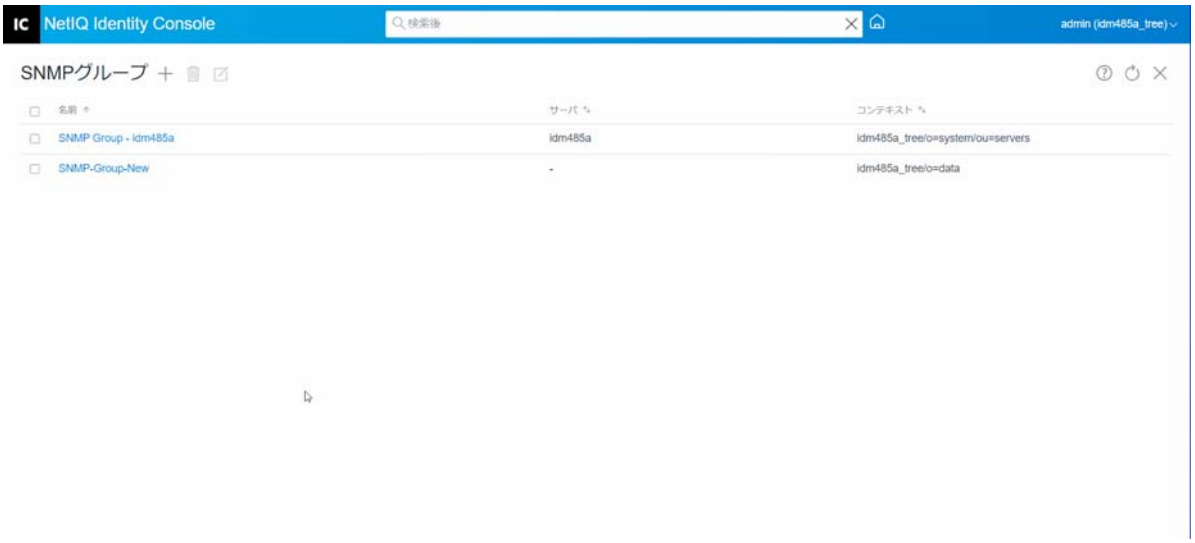


SNMP グループオブジェクトの変更

SNMP グループオブジェクトを変更するには、次の手順を実行します。

1. Identity Console のランディングページから、[[SNMP]] モジュールをクリックします。
2. 変更する SNMP グループオブジェクトを選択し、アイコンをクリックします。
3. [[一般]/ [トラップ]] ページで、構成可能なパラメータを変更します。
4. 完了したら、[[保存]] ボタンをクリックします。
5. SNMP グループオブジェクトが正常に変更されたことを確認するメッセージが画面に表示されます。

図 19-2 SNMP グループオブジェクトの変更

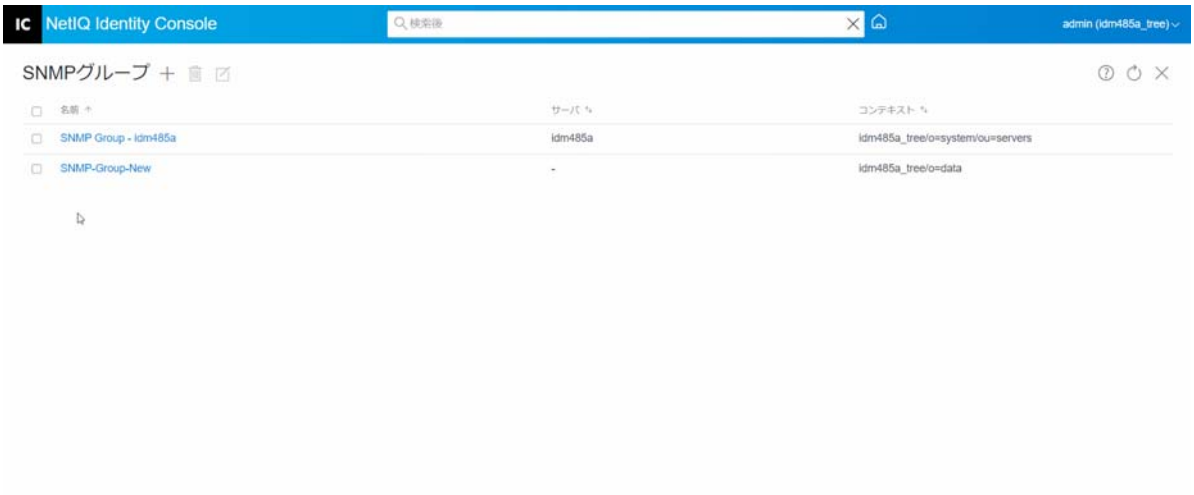


SNMP グループオブジェクトの削除

SNMP グループオブジェクトを削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[[SNMP]] モジュールをクリックします。
2. 変更する SNMP グループオブジェクトを選択し、アイコンをクリックします。
3. 次の画面で [[OK]] をクリックします。
4. SNMP グループオブジェクトが正常に削除されたことを確認するメッセージが画面に表示されます。

図 19-3 SNMP グループオブジェクトの削除



20 拡張バックグラウンド認証の管理

Identity Console の EBA プラグインから eDirectory にアクセスするには、ツリー内に有効な eba.p12 ファイルを持つ EBA 対応サーバが必要です。eDirectory ツリーで EBA を有効にする方法の詳細については、『NetIQ eDirectory 管理ガイド』の「*eDirectory ツリー上での EBA の有効化*」を参照してください。

注 : EBA モジュールを Identity Console と一緒に使用する場合は、eDirectory サーバを 9.2.4 HF2 にアップグレードする必要があります。

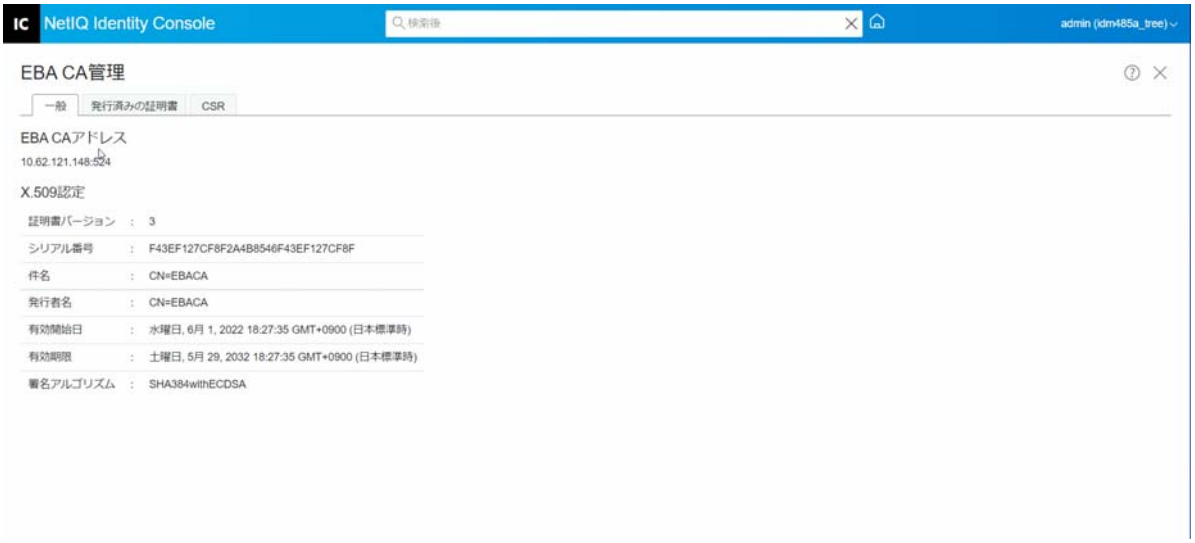
EBA CA 管理ページを開くには、Identity Console ポータルにログインし、[**[EBA]**] モジュールをクリックします。

[EBA CA 管理] ページには、EBA CA のさまざまな側面を管理するための以下のタブが表示されます。

- **一般 :** EBA CA の IP アドレスとその証明書を表示します。
- **発行された証明書 :** NCP CA 証明書を IP アドレスおよびポートとともに表示します。

  証明書を取り消すには、証明書を選択して、⊘をクリックします。証明書を無効にすると、NCP CA 証明書を所有しているサーバが機能しなくなるため、このオプションは異常な状況以外は使用しないでください。証明書を無効にする必要があるのはサーバが侵害された場合などです。
- **CSR:** 管理者の承認が保留になっている証明書署名要求を列挙します。証明書署名要求を承認するには、リストから証明書を選択して、[**[承認]**] をクリックします。

図 20-1 *拡張バックグラウンド認証の管理*



II Identity Console を使用した Identity Manager の管理

このセクションでは、Identity Console ポータルを使用して、Identity Manager サーバを管理するために実行できるさまざまなタスクについて説明します。

21 ドライバおよびドライバセットの管理

ドライバセットは、複数の Identity Manager ドライバを格納するコンテナです。1 つのサーバで一度にアクティブにできるドライバセットは 1 つだけです。このため、アクティブなドライバはすべて同じドライバセットにグループ化する必要があります。ドライバセットは、Designer ツールを使用して作成できます。詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の Configuring Driver Sets を参照してください。

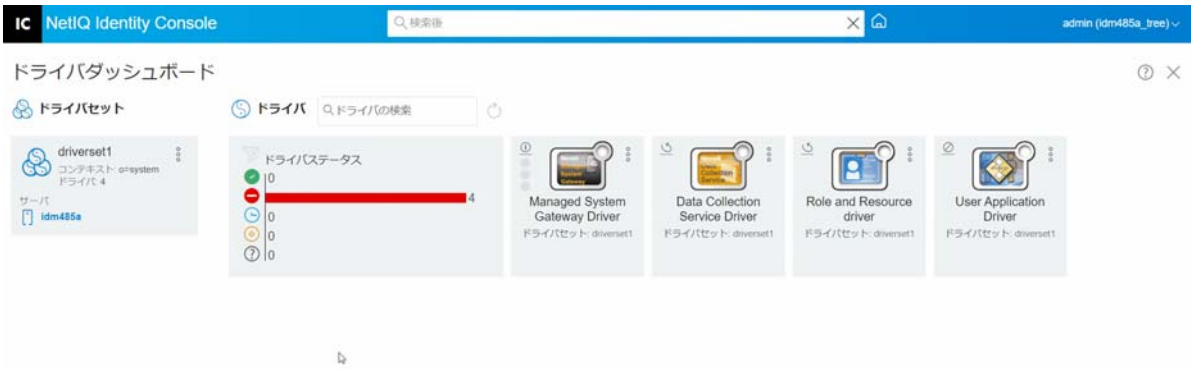
サーバの追加または削除

1 つのドライバセットを一度に 1 つまたは複数のサーバに関連付けることができます。ただし、要件によっては、別のドライバセットオブジェクトを使用可能なサーバに関連付けることができます。

新しいサーバを追加するには、特定のドライバセットオブジェクトの  アイコンをクリックし、[**[サーバの追加]**] を選択し、コンテキストブラウザから適切なサーバを選択します。

既存のサーバを削除するには、[**[サーバの削除]**] オプションを選択します。

図 21-1 ドライバセットへのサーバの追加



プロダクトアクティベーションキーを使用したドライバセットのアクティベーション

ドライバセットおよびドライバセット内にあるドライバを使用する前に、電子メール ID で受け取ったアクティベーションコードを使用して、アクティブにする必要があります。ライセンスを購入すると、NetIQ からアクティベーションキーを受け取ります。アクティベーションキーを使用してドライバセットをアクティブにするには、次の手順を実行します。

1. Identity Console のホーム画面から［ **[IDM 管理]**］タブをクリックします。
2. アクティブにする特定のドライバセットボックスのアクションアイコン をクリックし、［ **[アクティベーションのインストール]**］をクリックします。

   アクティベーションの適用時に、[IDM 管理] タイルの各ドライバセットタブには、そのドライバセットに関連付けられているすべてのサーバのアクティベーション情報が表示されます。この情報は、アクティベーションの有効期限を特定するのに役立ちます。
3. コンピュータにアクティベーションファイルがダウンロードされている場合は、［ **[資格情報を含むファイルを選択します]**］チェックボックスをオンにします。
4. アクティベーションファイルをブラウズして選択し、［ **[送信]**］をクリックします。

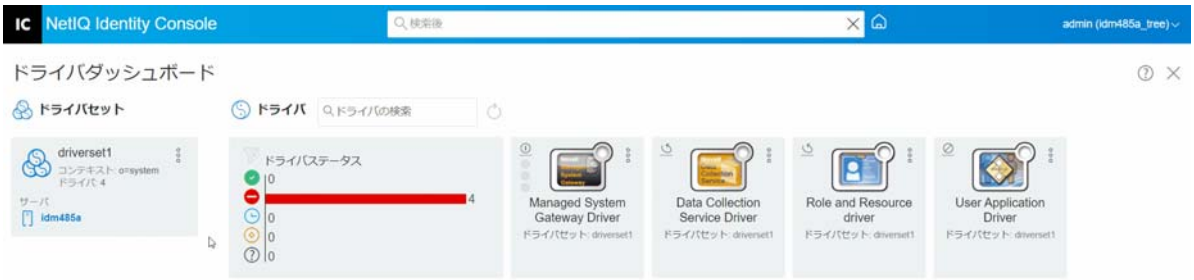
5 または、アクティベーションファイルの内容を使用してドライバセットをアクティブにできます。[[資格情報を入力]] のチェックボックスをオンにします。

5a プロダクトアクティベーションキーファイルを開き、プロダクトアクティベーションキーの内容をクリップボードにコピーします。

5b 内容をコピーする方法を選択する場合、不要な行やスペースが含まれないようにしてください。資格情報の最初のダッシュ (-) から (----BEGIN PRODUCT ACTIVATION CREDENTIAL) 資格情報の最後のダッシュ (-) まで (END PRODUCT ACTIVATION CREDENTIAL-----) をコピーし、[[終了]] をクリックします。

6 ドライバセットが正常にアクティブになったことを示す確認メッセージが表示されます。

図 21-2 ドライバセットのアクティベーション



ドライバセットのアクティベーション情報の表示

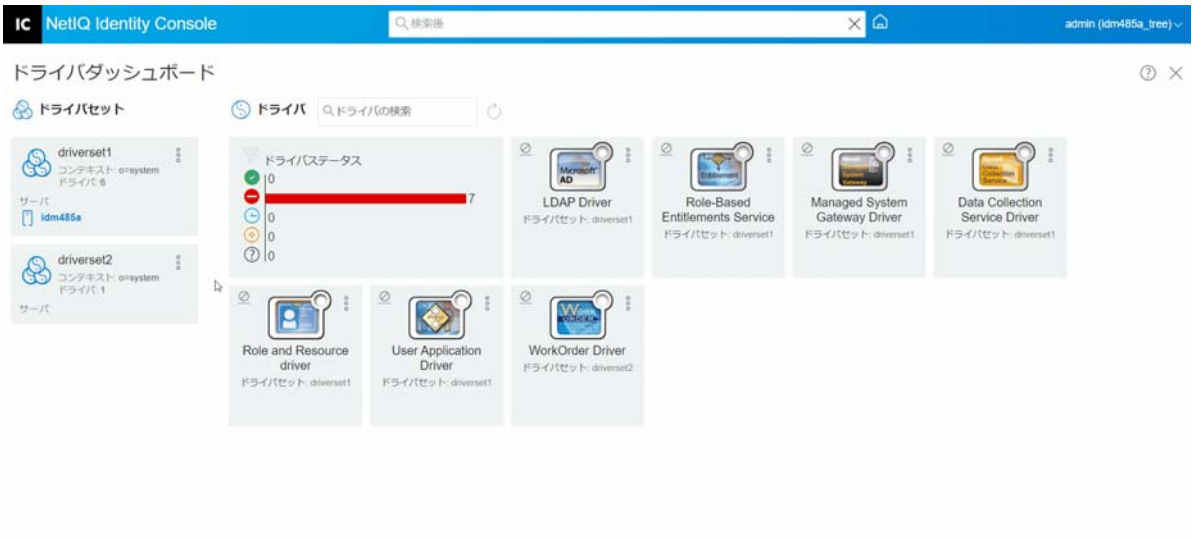
ドライバセットをアクティブにした後、ドライバセットが正常にアクティブになったことを確認する必要があります。確認を行うには、次の手順を実行します。

1 Identity Console のホーム画面から [[IDM 管理]] タブをクリックします。

2 アクティベーション情報を確認する特定のドライバセットオブジェクトのアクションアイコン をクリックし、[[アクティベーション情報]] をクリックします。

3 アクティベーション関連の情報ウィンドウがコンピュータにポップアップ表示されます。このページでは、特定のドライバセットのアクティベーションの詳細を確認できます。

図 21-3 ドライバセットのアクティベーション情報の表示

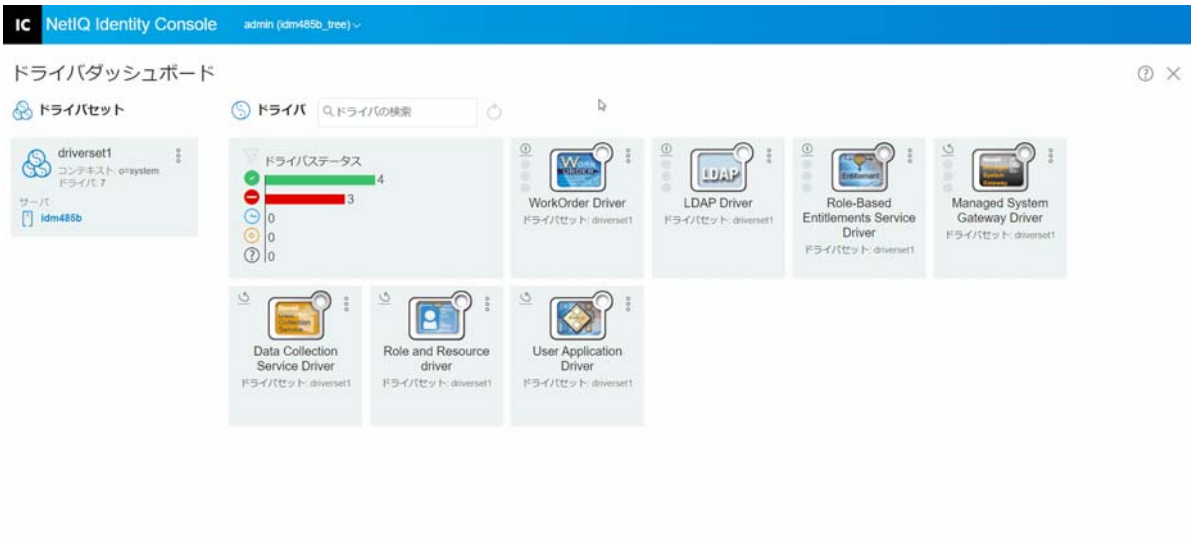


ドライバの起動および停止

ドライバが作成されると、デフォルトで停止されます。ドライバを動作させるには、ドライバを起動する必要があります。Identity Manager はイベントドリブンシステムであるため、ドライバが起動した後も、イベントが発生するまでアイドル状態が維持されます。次の手順を実行して、ドライバを起動 / 停止します。

1. Identity Console のホーム画面から［ **[IDM 管理]**］タブをクリックします。
2. コンピュータ画面の右側にある特定のドライバセットオブジェクトをクリックして、関連付けられているすべてのドライバを表示します。
3. 特定のドライバのアクションアイコン をクリックし、［ **[ドライバの起動]**］を選択します。
4. ドライバオブジェクトを停止するには、特定のドライバのアクションアイコン をクリックし、［ **[ドライバの停止]**］を選択します。
5. (オプション) または、同じドライバセットオブジェクト内のすべてのドライバを同時に起動または停止することもできます。ドライバセットオブジェクトのアクションアイコン をクリックして、［ **[すべてのドライバを起動する]**］または［ **[すべてのドライバを停止する]**］を選択します。

図 21-4 ドライバの起動および停止



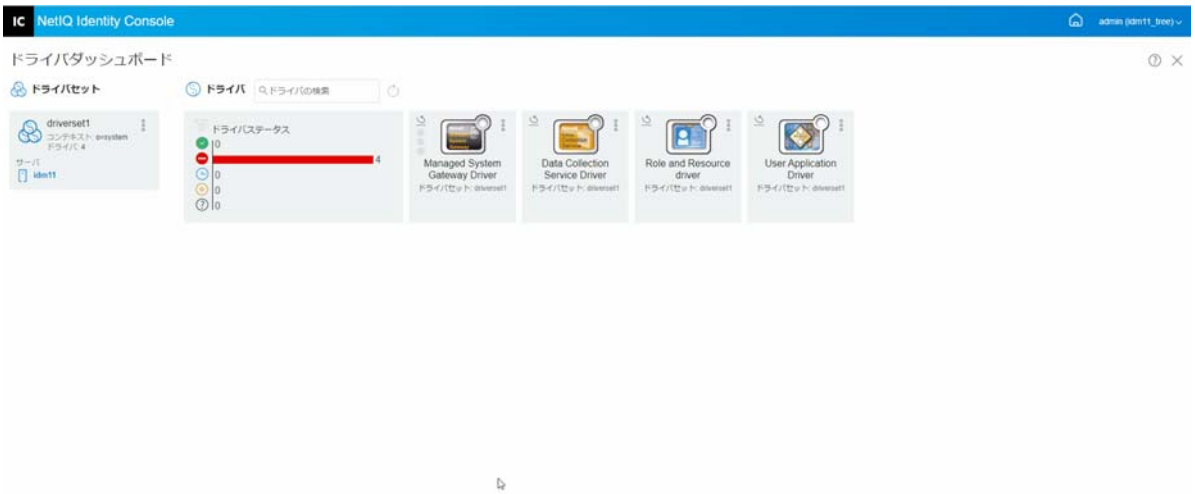
ドライバの検索

Identity Console には、サーバ内の特定のドライバを検索するオプションがあります。ドライバを検索するには、次の手順を実行します。

1 Identity Console のホーム画面から［ **[IDM 管理]**］タブをクリックします。

2 **[検索]** ボックスにドライバの名前を指定します。特定のドライバオブジェクトがコンピュータの画面に表示されます。アイコンをクリックして、ドライバのリストを更新することもできます。

図 21-5 ドライバの検索



ドライバとドライバセットのフィルタリング

ドライバは、[[IDM 管理]] ページからそれらのステータスに基づいてフィルタできます。ドライバをフィルタするには、次の手順を実行します。

1 Identity Console のホーム画面から［ [IDM 管理]］タブをクリックします。

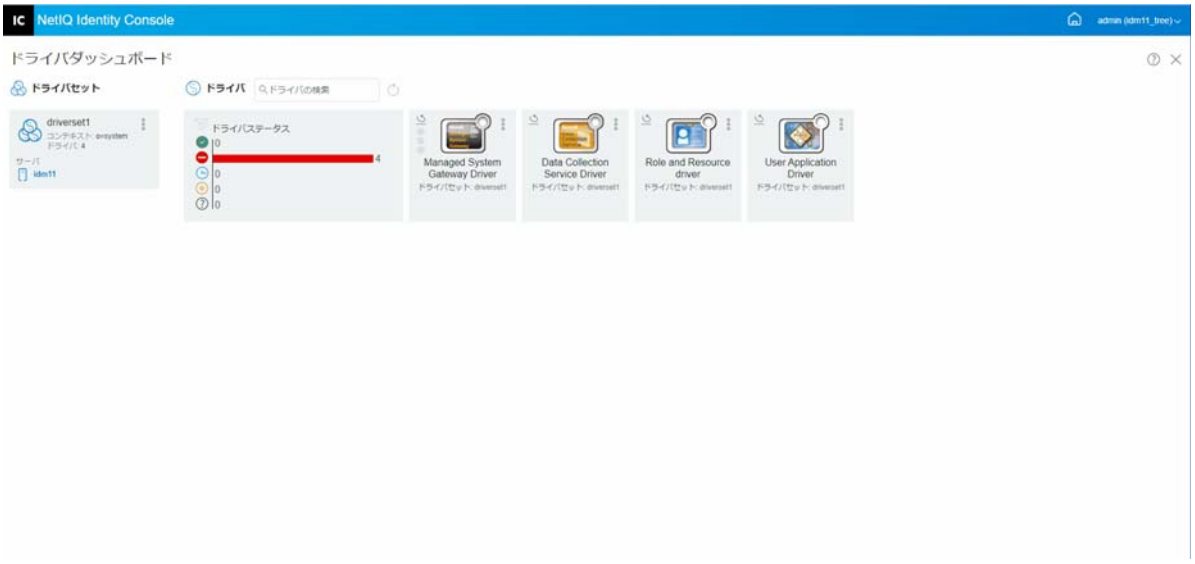
2 [Drivers' Status(ドライバのステータス)] タイルの次のアイコンをクリックして、ドライバステータスに基づいてドライバをフィルタします。

- アイコンをクリックして、サーバで実行中のすべてのドライバをフィルタします。
- アイコンをクリックして、サーバで停止しているすべてのドライバをフィルタします。
- アイコンをクリックして、起動しているすべてのドライバをフィルタします。
- アイコンをクリックして、停止しているすべてのドライバをフィルタします。
- アイコンをクリックして、ステータスが関連付けされていないドライバをフィルタします。ドライバセットにサーバが関連付けられていない場合、そのドライバセットに存在するドライバには [不明] ステータスが表示されます。

ドライバに適用されているフィルタをクリアするには、[Drivers' Status(ドライバのステータス)] タイルに表示されている アイコンをクリックします。

3 ドライバセットは、Identity Console ポータルを使用してフィルタすることも可能です。デフォルトでは、Identity Console ポータルには、サーバ内のすべてのドライバセットに関連付けられているすべてのドライバが表示されます。特定のドライバセットの下にあるドライバを表示する場合は、Identity Console ポータルの左側にあるドライバセットのリストから適切なドライバセットを選択する必要があります。ドライバセットの選択を解除するには、選択したドライバセットを再度クリックします。

図 21-6 ドライバとドライバセットのフィルタリング



ドライバセットの削除

ドライバセットを削除するには、次の手順を実行します。

1 Identity Console のホーム画面から［ **[IDM 管理]**］タブをクリックします。

2 削除する適切なドライバセットのアクションボタン  をクリックします。

3 **[削除]** を選択します。

ドライバのアクション

個々のドライバのタイル上でアクションアイコン  をクリックすると、次のアクションがサポートされます。

- **ドライバの起動** : ドライバを起動する
- **ドライバの停止** : ドライバを停止する
- **ドライバの再起動** : 停止したドライバを再起動する
- **ドライバの削除** : ドライバを削除する
- **統計** : ドライバのパフォーマンス統計を表示する
- **データのコピー** : ドライバのデータを 1 つのサーバから別のサーバにコピーします。このオプションは、マルチサーバ環境でのみ使用できます。

22 ドライバセットのプロパティの管理

このセクションでは、すべてのドライバセットに共通するプロパティについて説明します。これには、すべてのプロパティ (名前付きパスワード、ログレベル、ドライバセットインスペクタなど) が含まれます。

このセクションは、次のカテゴリで構成されています。

ドライバセットの設定

ドライバセットの設定を変更するには、次の手順を実行します。

1 [[IDM 管理]] > [[Click on the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]] > [[ドライバセットのプロパティ]] をクリックします。

2 デフォルトでは、[[ドライバセット環境設定]] ページが表示されます。ドライバセット環境設定オプションは、次のカテゴリに分かれています。

名前付きパスワード

Identity Manager では、ドライバセットの複数のパスワードを安全に保存できます。この機能は、名前付きパスワードと呼ばれます。それぞれのパスワードはキー、または名前でアクセスできます。

名前付きパスワードは、ドライバセットまたは個々のドライバに追加できます。ドライバセットの名前付きパスワードは、セット内のすべてのドライバで使用できます。

ドライバポリシーで名前付きパスワードを使用するには、実際のパスワードではなくパスワードの名前を使用してパスワードを参照します。その後、Identity Manager エンジンからドライバにパスワードが送信されます。この節で説明する名前付きパスワードの保存と復元の方法は、ドライバシムを変更することなく、どのドライバでも使用できます。

名前付きパスワードにアクセスするには、[ドライバセット環境設定] の下の［ [IDM 管理]］>［ [Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]］>［ [ドライバセットのプロパティ]］>［ [名前付きパスワード]］を選択します。

新しい名前付きパスワードを追加するには、＋アイコンをクリックします。既存の名前付きパスワードを削除するには、適切なパスワードを選択し、🗑アイコンをクリックします。

グローバル構成値

グローバル環境設定オブジェクトの順序付きリストを表示します。オブジェクトには、ドライバの起動時に Identity Manager がロードするドライバの拡張 GCV 定義が含まれています。グローバル環境設定オブジェクトを追加または削除したり、オブジェクトの実行順序を変更することができます。アイコンをクリックして、GCV を保存します。GCV のリストを更新するには、アイコンをクリックします。

Java 環境パラメータの設定

Java 環境パラメータを設定するには、次の手順を実行します。

1 Identity Console で、［ [IDM 管理]］>［ [Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]］>［ [ドライバセットのプロパティ]］を選択します。

2 ［ [ドライバセットの環境設定]］の下にある［ [Java 環境パラメータ]］をクリックして、Java 環境パラメータを含むプロパティページを表示します。

3 必要に応じて次の設定を変更します。

クラスパスの追加 : JVM がパッケージ (.jar) およびクラス (.class) ファイルを検索する、追加のパスを指定します。このパラメータを使用することは、java -classpath コマンドを使用することと同じです。複数のクラスパスを入力するには、Windows JVM の場合にはセミコロン (;)、UNIX または Linux JVM の場合にはコロン (:) で区切ります。

JVM オプション : JVM で使用する付加的なオプションを指定します。有効なオプションは、使用している JVM のマニュアルを参照してください。

DHOST_JVM_OPTIONS は、対応する環境変数です。JVM1.2 の引数を指定します。例えば :

-Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000

各オプション文字列は空白で区切られます。オプション文字列に空白が含まれている場合は、二重引用符で囲む必要があります。

ドライバセット属性オプションは、環境変数 DHOST_JVM_OPTIONS よりも優先されます。この環境変数は、ドライバセット属性オプションの末尾に付加されます。

初期ヒープサイズ : JVM が利用できる初期 (最小) ヒープサイズを指定します。初期ヒープサイズを大きくすれば、起動時間とスループットのパフォーマンスが改善される場合があります。数値の後に G、M、または K を使用します。文字サイズが指定されていない場合、サイズはデフォルトでバイトに設定されます。このパラメータを使用することは、java -Xms コマンドを使用することと同じです。

DHOST_JVM_INITIAL_HEAP は、対応する環境変数です。これは、JVM の初期ヒープサイズを 10 進数のバイト単位で指定します。これは、ドライバセット属性オプションよりも優先されます。

JVM のデフォルトの初期ヒープサイズの詳細については、使用している JVM のマニュアルを参照してください。

最大ヒープサイズ : JVM が利用できる最大ヒープサイズを指定します。数値の後に G、M、または K を使用します。文字サイズが指定されていない場合、サイズはデフォルトでバイトに設定されます。このパラメータを使用することは、java -Xmx コマンドを使用することと同じです。

DHOST_JVM_MAX_HEAP は、対応する環境変数です。これは、JVM の最大ヒープサイズを 10 進数のバイト単位で指定します。これは、ドライバセット属性オプションよりも優先されます。

JVM のデフォルトの最大ヒープサイズの詳細については、使用している JVM のマニュアルを参照してください。

4 をクリックして変更内容を保存します。

5 アイデンティティボールトを再起動して、変更を適用します。

値がある属性のリストの管理

特定のドライバセットについて、値がある属性のリストに属性を追加するには、次の手順を実行します。

1 Identity Console で、[**[オブジェクト管理]**] モジュールを選択します。

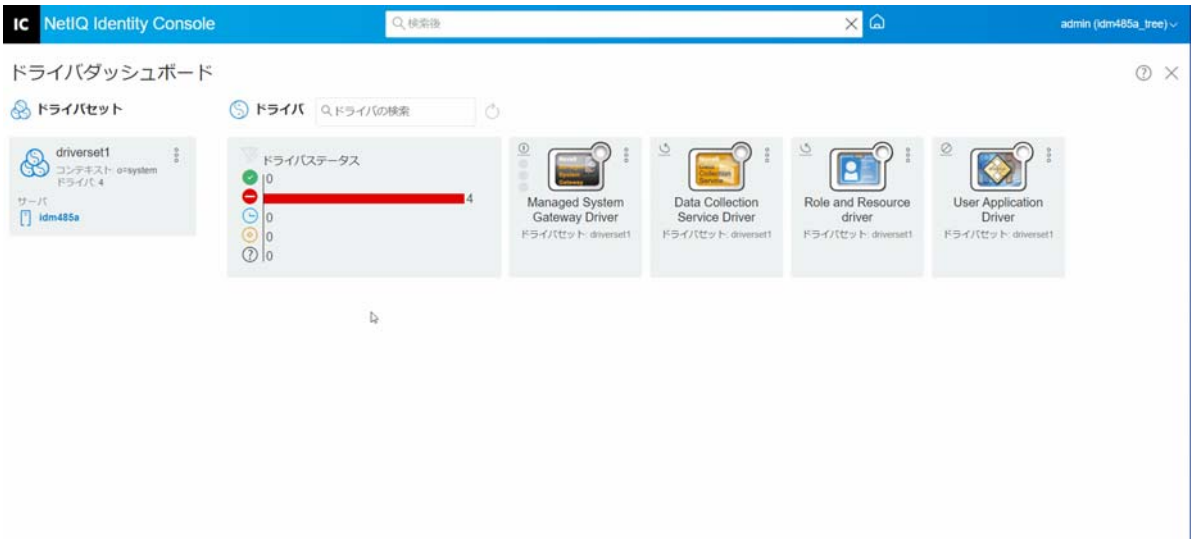
2 ドロップダウンリストから **[DirXML-DriverSet]** タイプを選択し、[検索] ボタンをクリックします。

3 検索リストから適切なドライバセットをクリックします。

4 値のない属性を値のある属性のリストに追加するには、[**[値がある属性]**] の横の アイコンをクリックし、リストから適切な値のない属性を選択します。

5 完了したら、[**[OK]**] をクリックします。

図 22-1 ドライバセット環境設定パラメータの管理



ドライバセットのジョブの管理

Identity Console では、それぞれのドライバセットに存在するすべてのドライバについて、ジョブオプションを使用してイベントをスケジュールできます。

［ジョブスケジューラ］ページには、ジョブの名前、ジョブが有効か無効か、実行スケジュール、およびジョブの説明が含まれています。ジョブ名をクリックして、［ジョブ］ページを表示します。ジョブを有効または無効にするには、［有効］列の下で［有効 / 無効］アイコンをクリックします。ジョブの詳細を表示するには、ジョブの説明をクリックします。

［ジョブ］ページにアクセスするには、Identity Console のメインページから、[**[IDM 管理]**] > [**[Click on the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[詳細]**] タブを選択します。［ジョブ］タブには、選択したドライバの既存のジョブオブジェクトが表示される表が含まれています。選択したドライバは、［ドライバ］エントリに完全識別名で一覧されます。

［ジョブスケジューラ］ページでは、次のタスクを実行できます。

- **ジョブの作成** : ＋アイコンをクリックして新しいジョブを作成します。

  [**新規ジョブ**] ポップアップで新しいジョブを作成するには、次の手順を実行します。

  1. ジョブ名を指定します。
  2. ジョブタイプを選択します。
  3. ﹀アイコンをクリックし、使用可能なサーバのリストからジョブを実行するサーバを選択します。それ以外の場合は、サーバ名を指定してからサーバを選択します。
  4. [**[作成]**] ボタンをクリックします。

- **ジョブの開始** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。
- **ジョブの停止** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。
- **ジョブの有効化** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。
- **ジョブの無効化** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。
- **ステータスの取得** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。
- **ジョブの削除** : ジョブの左側にあるボックスをオンにしてジョブを選択してから、  アイコンをクリックします。

ジョブをクリックして［**Job Property(ジョブプロパティ)**］ページにアクセスします。このページで、ジョブの実行方法を設定できます。

一般 : ジョブの Java クラス名が表示されます。このページを使用して、ジョブを有効または無効にする、実行後にジョブを削除する、このジョブを実行するサーバ (1 つまたは複数) を選択する、電子メールサーバを指定する、ジョブに別の表示名と説明を付けることができます。

スケジュール : ジョブの実行時期を設定できます。ジョブ開始時間を指定して時刻を設定し、ジョブを毎日、毎週、毎月、毎年実行するかどうかを指定します。ジョブを実行する時間をカスタマイズしたり、トグルを有効にしてジョブを手動で実行したりすることもできます。

スコープ : このジョブを適用するオブジェクトを定義できます。オブジェクトはコンテナ、動的グループ、グループ、またはリーフオブジェクトです。［追加］をクリックして、このジョブを適用するオブジェクトを選択します。［参照］ボタンを使用してオブジェクトを選択して、［OK］をクリックすることもできます。オブジェクトをスコープリストから削除するには、DN オブジェクトの左側にあるボックスをオンにしてスコープオブジェクトを選択してから、［削除］をクリックします。

オブジェクトが追加されたら、それを選択してさらにオプションを表示します。グループオブジェクトを選択すると、ジョブをグループのメンバーまたはグループのみに適用するオプションが表示されます。コンテナオブジェクトを選択した場合は、ジョブをそのコンテナのすべての子孫に適用するか、そのコンテナのすべての子に適用するか、それともそのコンテナのみに適用するかを選択できます。

パラメータ : 追加パラメータをジョブに追加して、現在設定されているパラメータを確認できます。これらのパラメータは、選択したジョブのタイプに応じて異なります。

結果 : ジョブの結果で行うことを定義できます。結果ページは［中間結果］と［最終結果］の 2 つの部分に分かれており、次の結果が表示されます。「成功」、「警告」、「エラー」、および「中止」。［結果］列の右側は［アクション］列です。［アクション］列をクリックすると、各結果の通知方法を設定できます。アクションには、「監査結果の送信」、または「結果が出た際に電信メールで送信する」が含まれます。オプションを選択しないと、結果に対するアクションは行われません。

[**トレース**] タブでは、特定のドライバのトレースを設定できます。詳細については、179 ページの 「トレースレベルの設定」を参照してください。

特定のドライバセットのライブラリの管理

ライブラリオブジェクトは、複数のポリシーおよび 1 つまたは複数のドライバによって共有されているその他のリソースを保存します。ライブラリオブジェクトは、ドライバセットオブジェクトまたは任意の eDirectory コンテナ内で作成できます。eDirectory ツリーには複数のライブラリが存在できます。ドライバは、そのドライバが動作しているサーバがライブラリオブジェクトの読み書き可能レプリカまたはマスタレプリカを保持している限り、ツリー内のどのライブラリでも参照できます。

ライブラリにスタイルシート、ポリシー、ルール、その他のリソースオブジェクトを保存して、これを 1 つ以上のドライバに参照させることができます。

ライブラリ管理モジュールを使用して、次のタスクを実行できます。

- 150 ページの 「既存のライブラリの表示と削除」
- 150 ページの 「ライブラリからのオブジェクトの表示と削除」

既存のライブラリの表示と削除

既存のライブラリを表示および削除するには、次の手順を実行します。

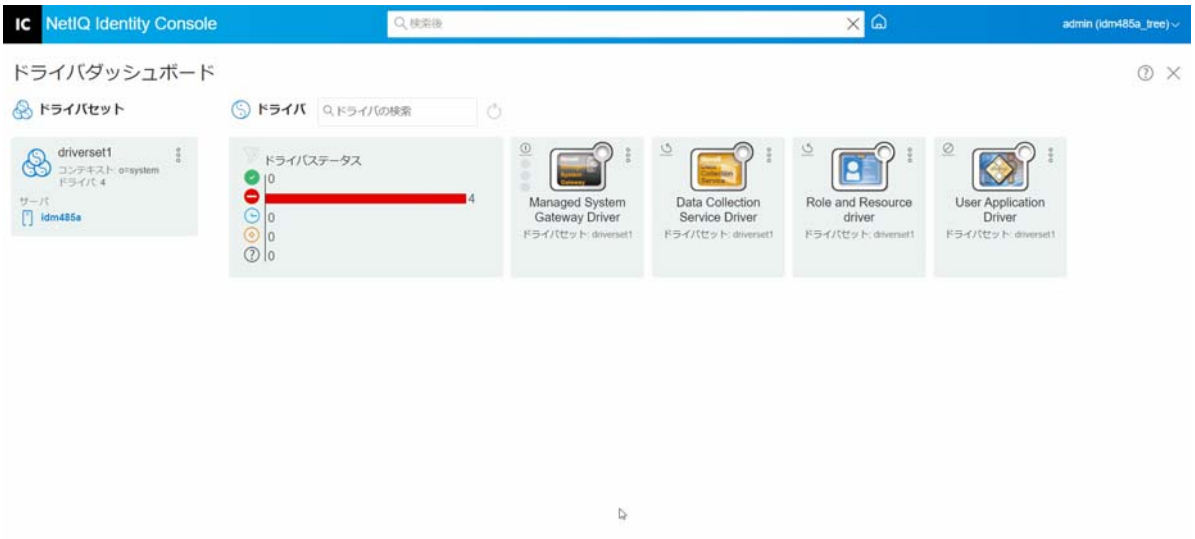
1. Identity Console で、[**[IDM 管理]**] > [**[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[詳細]**] > [**[ライブラリ]**] を選択します。
2. 適切なライブラリをリストから選択します。
3. アイコンをクリックします。**[OK]** をクリックして、確認します。

ライブラリからのオブジェクトの表示と削除

ライブラリオブジェクトからポリシーおよびマッピングテーブルを表示および削除できます。オブジェクトを削除するには、次の手順を実行します。

1. Identity Console で、[**[IDM 管理]**] > [**[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[詳細]**] > [**[ライブラリ]**] を選択します。
2. リストから適切なライブラリをクリックします。
3. ポリシーを削除するには、[**[ポリシー]**] タブを選択します。
4. リストから適切なポリシーを選択して、アイコンをクリックします。
5. マッピングテーブルを削除するには、[**[マッピングテーブル]**] タブを選択します。
6. リストから適切なマッピングテーブルを選択して、アイコンをクリックします。
7. **[OK]** をクリックして、確認します。

図 22-2 ドライバセットのジョブとライブラリの管理



ドライバセットのログレベルとトレースレベルの設定

ドライバセットのログとトレースを設定するには、Identity Console のメインページから、[[IDM 管理]] > [[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]] > [[ドライバセットのプロパティ]] > [[ログとトレースの環境設定]] タブを選択します。このセクションは、次のカテゴリで構成されています。

- 151 ページの 「ログレベルの設定」
- 152 ページの 「トレースレベルの設定」
- 153 ページの 「DirXML スクリプトのトレース」

ログレベルの設定

各ドライバセットにはログレベルフィールドがあります。このフィールドで、追跡するエラーレベルを定義できます。ここで指定するレベルによって、ログに記録されるメッセージの種類が決まります。デフォルトでは、ログレベルはエラーメッセージを追跡するように設定されています。(これには致命的エラーも含まれます。) 追加のメッセージタイプを追跡するには、ログレベルを変更します。ログレベルを設定するには、Identity Console 内で [[IDM 管理]] > [[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]] > [[ドライバセットのプロパティ]] > [[ログとトレースの環境設定]] > [[ログレベル]] を選択します。次のテーブルは、ログレベルの設定を示します。

オプション	説明
[[Turn off logging to DriverSet, Subscriber and Publisher logs]]	ドライバセットオブジェクト、購読者チャネル、および発行者チャネルのすべてのドライバのログ記録をオフにします。

オプション	説明
[ログ内のエントリの最大数 (50-500)]	ログ内のエントリ数。デフォルト値は「50」です。
[ログレベル]	次のログレベルを選択できます。 ◆ [エラーをログに記録]: エラーをログに記録します。 ◆ エラーと警告をログに記録 : エラーと警告のログを記録します。 ◆ [特定のイベントをログに記録]: 選択したイベントをログに記録します。このオプションを選択すると、次のイベントのリストが有効になります。 ◆ [Metadirectory Engine Events (メタディレクトリエンジンイベント)] ◆ [ステータスイベント] ◆ [操作イベント] ◆ [変換イベント] ◆ [資格情報プロビジョニングイベント] ◆ [最終ログ時刻のみを更新]: 最後のログ時刻を更新します。 ◆ [ログ記録のオフ]: ドライバのログ記録をオフにします。

トレースレベルの設定

特定のドライバセットのトレースを設定できます。ドライバセットに指定されたトレースレベルに応じて、エンジンがイベントを処理するときに、ドライバ関連のイベントがトレースに表示されます。ドライバトレースレベルは、トレースが設定されているドライバまたはドライバセットにのみ影響します。リモートローダを使用している場合は、リモートローダのトレースファイルは直接リモートローダに設定され、ドライバシムトレースのみが含まれます。

ドライバセットのトレースを設定するには、[[IDM 管理]] > [[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]] > [[ドライバセットのプロパティ]] > [[ログとトレースの環境設定]] > [[トレース]] タブを選択します。次のテーブルは、トレース設定を示します。

パラメータ	ドライバ
トレースレベル	ドライバのトレースレベルを上げると、トレースに表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因にはなりません。パスワード同期の情報を表示するには、トレースレベルを 5 に設定します。 [[ドライバセットの設定を使用する]] を選択した場合、値はドライバセットから取得されます。

パラメータ	ドライバ
XSL のトレースレベル	トレースは XSL イベントを表示します。このトレースレベルは、XSL スタイルシートのトラブルシューティング時にのみ設定します。XSL 情報を表示しない場合は、レベルをゼロに設定します。
Java デバッグポート	開発者は Java デバッガをアタッチできます。Java デバッガを接続した後、アイデンティティボールトを再起動します。
トレースファイル	選択したドライバに対して、ファイル名および Identity Manager 情報を書き込む場所を指定します。 [**[ドライバセットの設定を使用する]**] を選択した場合、値はドライバセットから取得されます。
トレースファイルのエンコーディング	トレースファイルはシステムのデフォルトのエンコーディングを使用します。必要な場合には、他のエンコーディングを指定できます。 [**[ドライバセットの設定を使用する]**] を選択した場合、値はドライバセットから取得されます。
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズが増加します。 **注 :** ファイルサイズの制限が指定されている場合、トレースファイルは複数のファイルに作成されます。Identity Manager により自動的に最大のファイルサイズが 10 で割られ、10 個のファイルが作成されます。これらのファイルを組み合わせたサイズが、トレースファイルの最大サイズと等しくなります。 [**[ドライバセットの設定を使用する]**] を選択した場合、値はドライバセットから取得されます。

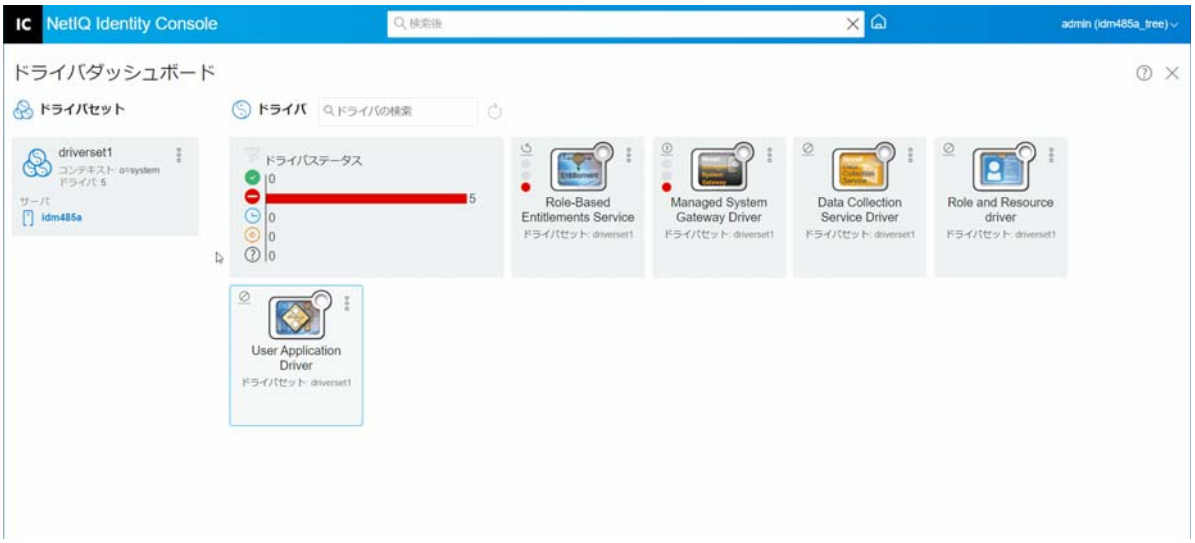
DirXML スクリプトのトレース

[DirXML Script Tracing (DirXML スクリプトのトレース)] オプションを使用すると、ドライバセットのトレースレベルを選択できます。選択した内容は、ドライバセット内のすべてのポリシーに適用されます。次の DirXML スクリプトトレースオプションを選択できます。

- すべての DirXML スクリプトトレースをオンにする
- すべての DirXML スクリプトトレースをオフにする
- DirXML スクリプトルールのトレースオン
- DirXML スクリプトルールのトレースオフ

をクリックして変更内容を保存します。

図 22-3 ドライバセットのログレベルとトレースレベルの管理



ドライバセットインスペクタと統計の管理

ドライバセットインスペクタを使用して、ドライバセットに関連付けられているオブジェクトに関する詳細情報を表示できます。このセクションは、次のカテゴリで構成されています。

- 154 ページの 「ドライバセット統計の表示」
- 155 ページの 「バージョン情報を表示する」
- 156 ページの 「関連付け統計の表示」

ドライバセット統計の表示

Identity Console ポータルを使用して、単一のドライバまたはドライバセット全体に関するさまざまな統計情報を表示できます。これには、キャッシュファイルのサイズ、キャッシュファイル内の未処理トランザクションのサイズ、最も古いトランザクションと最新のトランザクション、およびカテゴリ別の未処理トランザクションの総数 (追加、削除、変更など) などの統計情報が含まれます。ドライバセットの統計を表示するには、次の手順を実行します。

1 Identity Console で、[**[IDM 管理]**] > [**[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[インスペクタと統計]**] > [**[統計]**] を選択します。

2 ドロップダウンから適切なサーバを選択します。

ドライバセットに含まれるすべてのドライバの統計を表示できるページが表示されます。

- 統計情報を更新するには、アイコンをクリックします。

- ドライバの統計情報を閉じるには、ドライバの統計情報ウィンドウの右上隅にあるボタンをクリックします。
- すべてのドライバの統計情報を開く場合は、[**[アクション]**] > [**[すべてを表示]**] をクリックします。
- ドライバの未処理トランザクションのリストを折りたたむには、リストの上にあるボタンをクリックします。すべてのドライバの未処理トランザクションのリストを折りたたむには、[**[アクション]**] > [**[すべてのトランザクションを折りたたむ]**] をクリックします。
- トランザクションのリストを開くには、ボタンをクリックします。すべてのドライバの未処理トランザクションのリストを開くには、[**[アクション]**] > [**[すべてのトランザクションを開く]**] をクリックします。
- 無効になっているドライバの統計ダッシュボードを閉じるには、[**[アクション]**] をクリックして、[**[無効なドライバを閉じる]**] を選択します。

バージョン情報を表示する

Identity Manager エンジン、ドライバシム、およびドライバ環境設定ファイルにはそれぞれ個別のバージョン番号が含まれています。Identity Console のバージョンディスカバリオプションは、Identity Manager エンジンのバージョンとドライバシムのバージョンを確認するのに役立ちます。ドライバ環境設定ファイルには、独自の命名規則が含まれています。バージョン情報を表示するには、次の手順を実行します。

1 Identity Console で、[**[IDM 管理]**] > [**[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[インスペクタと統計]**] > [**[バージョンの検出]**] を選択します。

2 トップレベルディスプレイでのバージョン情報の表示 :

- 認証されている eDirectory ツリー

  注 : eDirectory は、Identity Manager 環境で使用される場合、アイデンティティボールトと呼ばれます。

- 選択したドライバセット
- ドライバセットに関連付けられているサーバ

  ドライバセットが 2 つ以上のサーバに関連付けられている場合、各サーバの Identity Manager 情報を表示できます。
- ドライバ

3 [**[表示]**] アイコンをクリックすると、トップレベルに表示されるのと同じ情報がテキスト形式で表示されます。

4 [エクスポート] ボタン をクリックして、テキストをエクスポートし、ローカルドライブまたはネットワークドライブ上のファイルに保存します。

関連付け統計の表示

Identity Manager の関連付け統計機能を使用すると、Identity Manager が管理する識別情報の関連付けの詳細を検索できます。Identity Manager は関連付け統計を使用して、Identity Manager ドライバの関連付け数を取得します。

ドライバのアクティブオブジェクト、非アクティブオブジェクト、およびシステム管理オブジェクトを取得するには、関連付け統計ジョブを実行します。関連付け統計ジョブは、日単位、週単位、月単位、または年単位でスケジュールできます。デフォルトでは、ジョブは毎週実行されるようにスケジュールされます。

関連付け統計ダッシュボードには、関連付け詳細が表示されます。または、関連付けをファイルにエクスポートして詳細を表示することもできます。

注

- ドライバの関連付け数はサーバ単位です。オブジェクトが複数のドライバに関連付けられている場合、関連付け数は各ドライバに対して固有に計算されます。
- 関連付け数が 200,000 を超える場合は、ドライバセットの最大ヒープサイズを 2GB 以上に設定することをお勧めします。ヒープサイズの設定については、146 ページの「Java 環境パラメータの設定」を参照してください。

関連付け統計を表示するには、次の手順を実行します。

1. Identity Console で、[**[IDM 管理]**] > [**[Click the context menu (three dots) of the appropriate Driver Set（適切なドライバセットのコンテキストメニュー (3 つの点) をクリックする）]**] > [**[ドライバセットのプロパティ]**] > [**[インスペクタと統計]**] > [**[関連性統計]**] を選択します。
2. 関連付け統計を実行するサーバを選択します。
3. 関連付け数には、以前に計算された結果が表示されます。

   Identity Console には、ドライバセットに関連付けられているすべてのドライバのアクティブオブジェクト、非アクティブオブジェクト、およびシステム管理オブジェクトの関連付け数が表示されます。

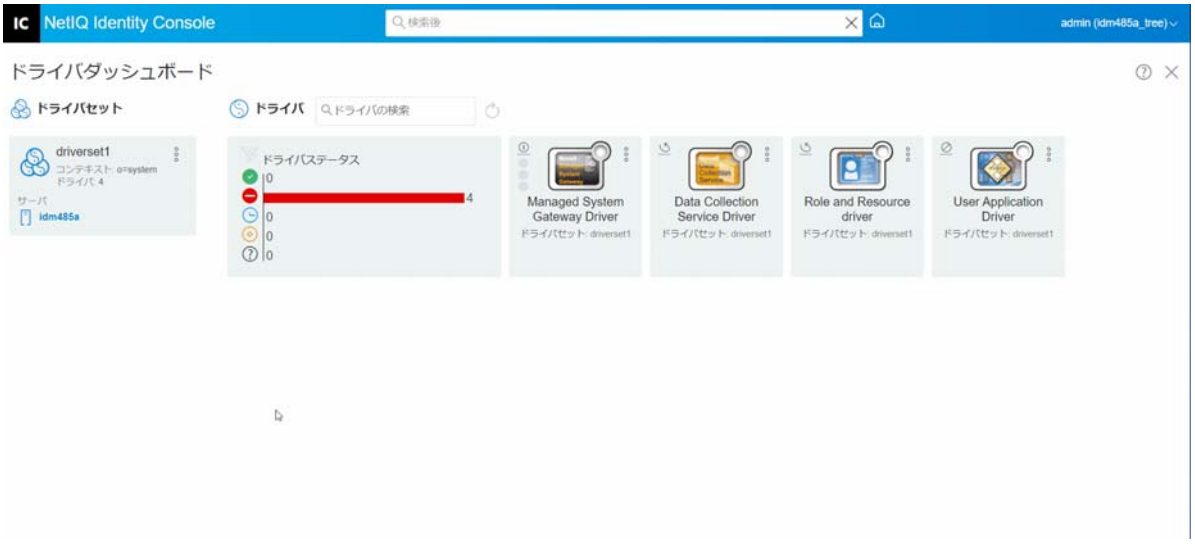
   Identity Console は、グループと組織単位をシステム管理オブジェクトと見なします。Identity Console では、オブジェクトの［ログインが無効］属性が true に設定され、オブジェクトが過去 120 日以内に変更されていない場合、オブジェクトは非アクティブと見なされます。残りのオブジェクトはすべてアクティブな管理オブジェクトと見なされます。
4. 更新された結果を取得するには、アイコンをクリックします。

   ドライバがサーバ上で無効になっている場合、Identity Console はダッシュボードにドライバを表示しません。
5. サーバに関連付けられているドライバのシステム詳細および関連付け数の詳細をエクスポートするには、アイコンをクリックします。
6. 特定のドライバに関連付けられているオブジェクトをエクスポートするには、必要なオブジェクトの隣の をクリックしてファイルを保存します。

注 : Fan-Out ドライバの場合は、固有のオブジェクトのみがエクスポートされます。オブジェクトが Fan-Out ドライバの複数のインスタンスに関連付けられている場合、Identity Console はダッシュボード内のすべての関連付け数を表示します。ただし、ファイル内のオブジェクトをエクスポートする場合、Identity Console は固有のオブジェクトのみをエクスポートします。

7 [**[アクション]**] をクリックし、関連付け数ダッシュボードを整理するために必要なオプションを選択します。

図 22-4 *ドライバセット統計の管理*



23 ドライバプロパティの管理

このセクションでは、すべてのドライバに共通するプロパティについて説明します。これには、すべてのプロパティ (名前付きパスワード、エンジン制御値、ログレベルなど) が含まれます。

ドライバのアクティベーション情報が表示され、有効期限が切れたドライバを有効にするアクションが通知されます。

ドライバの環境設定を変更するには、次の手順を実行します。

1 Identity Console のホーム画面から［[ドライバ]］タブをクリックします。

2 各ドライバのタイルをクリックして、ドライバの環境設定ページを表示します。

デフォルトでは、［[接続パラメータ]］ページが表示されます。ドライバ環境設定オプションは、次のカテゴリに分かれています。

接続パラメータ

接続パラメータは、ドライバをローカルで実行するか、リモートで実行するかを制御します。

- **Java:** このオプションを使用して、ドライバのシムコンポーネントに対してインスタンス化される Java クラスの名前を指定します。このファイルはクラスディレクトリ内のクラスファイルとして、または LIB ディレクトリ内の .jar ファイルとして見つけることができます。ドライバをローカルで実行する場合、このオプションを選択します。また、ドライバオブジェクトパスワードおよびドライバキャッシュ制限も指定する必要があります。［[パスワードの設定]］リンクをクリックすると、新しいパスワードを設定できます。

  たとえば、com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim

- **ネイティブ :** このオプションは、ドライバのネイティブ言語 (C++ など) で開発された .dll の名前を指定するために使用されます。また、ドライバオブジェクトパスワードおよびドライバキャッシュ制限も指定する必要があります。［[パスワードの設定]］リンクをクリックすると、新しいパスワードを設定できます。

  たとえば、addriver.dll

- **リモートローダに接続** : このオプションは、ドライバが接続システムにリモートで接続している場合に使用されます。このオプションを選択した場合は、次のサブオプションを指定する必要があります。
  - [リモートローダ接続パラメータ]: ホスト名、接続ポートなどのリモートローダ環境の詳細に関する情報が含まれます。
  - [リモートローダパスワード]: リモートローダ用のパスワード。
  - [ドライバオブジェクトパスワード]: ドライバオブジェクトのパスワードを指定します。リモートローダを使用している場合は、このページにパスワードを入力する必要があります。リモートローダは、このパスワードを使用してリモートドライバシムに対して自身を認証します。
- **認証** : 認証パラメータは、Identity Manager エンジンおよびリモートローダサーバの認証に使用されます。次のパラメータを指定します。
  - [認証 ID]: ユーザアプリケーション ID を指定します。この ID は、アプリケーションにアイデンティティボールト購読情報を渡す際に使用されます。
  - [認証コンテキスト]: アプリケーションシムが通信する IP アドレスまたはサーバの名前を指定します。
  - [アプリケーションパスワード]: アプリケーション認証パスワードを設定するオプション。

完了したら、アイコンをクリックして設定を保存します。

図 23-1 *接続パラメータの管理*

ドライバ環境設定

ドライバ環境設定セクションでは、ドライバ固有のパラメータ、エンジン制御値、グローバル構成値などを設定できます。ドライバパラメータを変更する場合は、ネットワーク環境と協調するようにドライバの振る舞いを調整します。このセクションは、次のカテゴリで構成されています。

ドライバパラメータ

ドライバパラメータは、ドライバ設定、購読者設定、および発行者設定に分かれています。これらの設定は、ドライバの環境設定に基づいて入力されます。ドライバパラメータの詳細については、「Identity Manager ドライバマニュアル」の特定のドライバガイドを参照してください。

完了したら、をクリックしてパラメータを保存できます。パラメータをデフォルト値に設定する場合は、アイコンをクリックします。XML ファイルを使用してドライバ環境設定を変更するには、アイコンをクリックします。

グローバル構成値

グローバル環境設定オブジェクトの順序付きリストを表示します。オブジェクトには、ドライバの起動時に Identity Manager がロードするドライバの拡張 GCV 定義が含まれています。XML エディタを使用して、[[グローバル構成値]] タブのオブジェクトを表示または変更できます。アイコンをクリックして、GCV を保存します。GCV のリストを更新するには、アイコンをクリックします。GCV を削除するには、適切な GCV オブジェクトを選択し、アイコンをクリックします。

エンジン制御値

エンジン制御値は、Identity Manager エンジンのデフォルトの特定の振る舞いを変更できる方法です。これらの値には、サーバがドライバセットオブジェクトと関連付けられている場合のみアクセスできます。

オプション	説明
[購読者チャネル再試行間隔 (秒単位)]	購読者チャネル再試行間隔では、アプリケーションシムの購読者オブジェクトから再試行ステータスが戻された後で、Identity Manager エンジンがキャッシュ済みトランザクションの処理を再試行する頻度を制御します。
[DN 構文属性値の完全修飾フォーム]	DN 構文属性値の修飾指定では、DN 構文属性値を非修飾スラッシュ形式で表すか、完全修飾スラッシュ形式で表すかを制御します。True の設定は、値が修飾形式で表わされていることを意味します。
[名前変更イベント用の修飾形式]	名前変更イベント用の修飾形式では、名前変更イベントのアイデンティティボールトから取得する新しい名前の部分をタイプ識別子とともに購読者チャネルに表示するかどうかを制御します。たとえば、「CN=」というようになります。True の設定は、名前が修飾形式で表わされていることを意味します。
[最大 eDirectory 複製待機時間 (秒単位):]	この設定は、ローカルレプリカとリモートレプリカの間で複製される特定の変更を Identity Manager エンジンが待機する最大時間を制御します。これは、操作を実行するために同じツリーにあるリモート eDirectory 得サーバに、Identity Manager エンジンが接続する必要があり、操作 (Identity Manager サーバが移動オブジェクトのマスタレプリカを保持していないときのオブジェクト移動、テンプレートから作成されたユーザのファイルシステムの権利操作など) が完了する前にリモートサーバとの間で変更が複製されるのを待機する必要がある場合にのみ作用します。
[XSLT 未準拠バックワード互換モードの使用]	このコントロールは、Identity Manager エンジンが使用する XSLT プロセッサをバックワード互換モードに設定します。バックワード互換モードにより、XPath 1.0 および XSLT 1.0 標準に準拠しない 1 つまたは複数の動作が XSLT プロセッサで使用されます。これは、非規格の振る舞いに依存する既存の DirXML スタイルシートとの後方互換性のために行われます。 たとえば、1 つのオペランドがノードセットであり、もう一方のオペランドがノードセット以外であるときの XPath "!=" 演算子の動作は Identity Manager 2.0 までの DirXML リリースでは不正です。この振る舞いは修正されましたが、修正された振る舞いは、既存の DirXML スタイルシートとの後方互換性を確保するために、この制御により無効に設定されています。
[一度に移行するアプリケーションオブジェクトの最大数]	このコントロールは、アプリケーションからのオブジェクトの移行操作の一部として実行される 1 回のクエリの間に、Identity Manager エンジンがアプリケーションから要求するアプリケーションオブジェクトの数を制限するために使用します。 アプリケーションからの移行操作中に、java.lang.OutOfMemoryError エラーが発生する場合、この数はデフォルト値より少なくする必要があります。デフォルトは 50 です。 **注 :** このコントロールによって移行できるアプリケーションオブジェクト数は制限されません。バッチサイズが制限されるだけです。

オプション	説明
[アイデンティティボールトに作成されたオブジェクトに creatorsName を設定する]	このコントロールは、このドライバによりアイデンティティボールトに作成されたすべてのオブジェクトのこのドライバの DN に creatorsName 属性を設定するかどうかを決定するために、Identity Manager エンジンによって使用されます。 creatorsName 属性を設定すると、このドライバによってされたオブジェクトを容易に識別できるようになりますが、パフォーマンス上のペナルティも発生します。この属性を設定しない場合、creatorsName 属性は、デフォルトで、ドライバをホストする NCP サーバオブジェクトの DN に設定されます。
[保留中の関連付けの書き込み]	このコントロールは、購読者チャネルでの処理中に Identity Manager で保留中の関連付けをオブジェクトに書き込むかどうかを判断します。 保留中の関連付けを書き込むメリットはほとんど (またはまったく) ないにもかかわらず、パフォーマンスには悪影響を与えてしまいます。それにもかかわらず、後方互換性のためにこれをオンにするオプションが存在しています。
[パスワードイベント値の使用]	このコントロールは、購読者チャネルの追加および変更イベント用に nspmDistributionPassword 属性に対して報告された値のソースを判断します。 このコントロールを False に設定すると、nspmDistributionPassword の現在の値が取得され、属性イベントの値として報告されます。つまり、現在のパスワード値のみが利用可能です。これはデフォルトの動作です。 このコントロールを True に設定すると、eDirectory イベントとともに記録された値が復号化され、属性イベントの値として報告されます。つまり、イベントの際に、古いパスワード値 (存在する場合) と置換用パスワード値の両方が利用可能です。これは、新しいパスワードを設定できるようにするために古いパスワードが必要な特定のアプリケーションとパスワードを同期する場合に便利です。
[Retry Out of Band events（アウトオブバンドイベントの再試行）]	このコントロールは、アウトオブバンド同期イベントの [再試行] ステータスを受信した場合に、アウトオブバンド同期イベントを再試行するかどうかを決定します。 コントロールが False に設定されている場合、アウトオブバンド同期は再試行されません。この値が true に設定されている場合、アウトオブバンド同期は正常に試行されるまで再試行されます。
[Use Rhino ECMAScript engine（Rhino ECMAScript エンジンの使用）]	Identity Manager エンジンが Rhino ECMAScript エンジンを使用するかどうかを決定します。エンジンは、デフォルトの ECMAScript エンジンとして Rhino を使用します。 このコントロールを [False] エンジンに設定した場合、このコントロールはデフォルトで [True] になります。この場合、このコントロールは Nashorm スクリプトを使用します。

オプション	説明
[購読者サービスチャネルの有効化]	Identity Manager エンジンが、ドライバの購読者サービスチャネルでアウトオブバンドクエリを処理するかどうかを決定します。これらのクエリの一般的な例としては、コードマップの更新、データ収集、dxcmd からトリガされたクエリがあります。 このコントロールが true に設定されている場合、チャネルはイベントの通常の処理を中断することなく、これらのクエリを個別に処理します。 現在、このコントロールは JDBC Fan-Out ドライバ (デフォルトで有効) でのみ使用できます。
[パスワード同期ステータス報告の有効化]	このコントロールは、購読者チャネルパスワードの変更イベントのステータスを Identity Manager エンジンが報告するか動かを判断します。 購読者チャネルのパスワード変更イベントのステータスを報告すると、Identity Manager ユーザアプリケーションなどのアプリケーションは、接続アプリケーションと同期する必要があるパスワード変更の同期の進行状況を監視することができます。
[Combine values from template object with those from add operation（テンプレートオブジェクトの値を追加操作の値と結合する）]	この値は、追加操作を実行するときに、Identity Manager エンジンが作成テンプレートと追加操作と同様の値を組み合わせるかどうかを決定します。この値を［True］に設定すると、テンプレートの複数値属性の値のほかに、追加操作で指定されている同じ属性の値も使用されます。この値を False に設定すると、追加操作で指定されている同じ属性の値が存在する場合、テンプレートの値は無視されます。
[Allow event loopback from publisher to subscriber channel（発行者チャネルから購読者チャネルへのイベントループバックを許可）]	この値は、Identity Manager エンジンがドライバの発行者チャネルから購読者チャネルにイベントをループできるかどうかを決定します。この値を［False］に設定すると、Identity Manager エンジンはイベントをループバックできなくなります。この値を［True］に設定すると、Identity Manager エンジンは発行者チャネルから購読者チャネルへイベントをループできるようになります。

オプション	説明
[Revert to calculated membership value behavior（計算されたメンバーシップ値の振る舞いに戻す）]	この値は、Identity Manager エンジンがグループメンバーシップに関連する読み込みおよび検索アクションを実行する際に使用する方法を決定します。 この値を［False］(デフォルト設定) に設定すると、Identity Manager エンジンは、アイデンティティボールトオブジェクトのメンバーおよびグループメンバー属性を読み込みまたは検索する際に、「静的」な値のみを返します。静的な値とは、ネストされたグループによる継承された割り当てではなく、グループに対する直接割り当てによってグループメンバーシップを受信したオブジェクトです。 この値を［True］に設定すると、Identity Manager エンジンは、Identity Manager 3.6 より前で使用されていた方法に戻ります。3.6 より前のバージョンでは、Identity Manager エンジンでメンバーおよびグループメンバー属性を検索すると、「計算された」値すべてが取得されていました。計算された値には、1) 静的に割り当てられたメンバーシップまたは 2) eDirectory で使用するネストされたグループ階層計算によって動的に割り当てられたメンバーシップのいずれかであるオブジェクトが含まれています。グループメンバー属性を検索すると、グループに直接割り当てられているオブジェクト、またはネストされたグループによってメンバーシップを割り当てられているオブジェクトがすべて返されます。
[Maximum time to wait for driver shutdown in seconds（ドライバのシャットダウンを待機する最大時間 (秒)）]	この設定は、Identity Manager エンジンがドライバの発行者チャネルのシャットダウンを待機する最大時間を制御します。指定した時間間隔内にドライバがシャットダウンされない場合、Identity Manager エンジンはドライバを終了します。
[Regular Expression escape meta-characters（正規表現エスケープメタ文字）]	このコントロールは、正規表現コンテキストで使用する場合に、ローカル変数を開くときにエスケープされるメタ文字を決定します。エスケープする必要があるすべての文字は、この制御値のカンマ区切りリストとして追加する必要があります。 制御値にメタ文字が存在しない場合、正規表現を含むローカル変数の拡張中にエスケープされません。 このコントロールを使用する場合は、次の条件を満たしてください。 ◆ 値は空のままにしないこと。デフォルトでは、***$*** が入力されています。この文字は、ローカル変数の拡張に必要です。 ◆ 値は、有効なカンマ (,) で区切られたリストである必要があります。そうでない場合、ポリシーの評価中にエラーが発生します。 ◆ すべてのメタ文字をエスケープするには、「\,$,^,.,?,*,+,［,］,(,),|」を値として指定します。 ◆ メタ文字をエスケープする必要がない場合は、その文字を値から削除します。 ◆ メタ文字をエスケープするには、メタ文字の後にバックスラッシュ (\) を指定します。

オプション	説明
[Ignore Entitlement Changes of other drivers（他のドライバのエンタイトルメントの変更を無視する）]	このコントロールは、Identity Manager エンジンが他のドライバのエンタイトルメントの変更を無視するか処理するか決定します。デフォルト値は「True」です。これは、ドライバが他のドライバのエンタイトルメントの変更を自動的に無視することを意味します。このコントロールが［False］に設定されている場合、他のドライバのエンタイトルメントの変更はキャッシュされ、このドライバによって処理されます。
[Allow Entitlement event loopback from cprs to subscriber channel（CPRS から購読者チャネルへのエンタイトルメントイベントのループバックを許可）]	このコントロールは、Identity Manager エンジンが CPRS 割り当てによって生成されたエンタイトルメントイベントがドライバの購読者チャネルにループバックすることを許可するかどうかを決定します。デフォルト値は「False」です。これは、イベントが購読者チャネルにループバックされないことを意味します。このコントロールが［True］に設定されている場合、イベントはドライバの購読者チャネルに流れます。

起動オプション

起動オプションでは、Identity Manager サーバの起動時のドライバ状態を設定できます。

- **オートスタート**：ドライバは、Identity Manager サーバが起動するたびに起動します。
- **手動**：Identity Manager サーバの起動時にドライバは起動しません。ドライバは、Identity Console ポータルを使用して起動する必要があります。
- **無効**：ドライバには、すべてのイベントを格納するキャッシュファイルがあります。ドライバを［無効］に設定すると、このファイルは削除され、ドライバの状態が［手動］または［オートスタート］に変更されるまで、新しいイベントはファイルに保存されません。

希望する起動オプションを設定した後、アイコンをクリックして保存します。起動オプションをリセットするには、アイコンをクリックします。

名前付きパスワード

Identity Manager では、ドライバで使用される複数のパスワードを安全に保存できます。この機能は、名前付きパスワードと呼ばれます。それぞれのパスワードはキー、または名前でアクセスできます。

名前付きパスワードは、ドライバセットまたは個々のドライバに追加できます。ドライバセットの名前付きパスワードは、セット内のすべてのドライバで使用できます。個々のドライバの名前付きパスワードは、そのドライバでのみ使用できます。

ドライバポリシーで名前付きパスワードを使用するには、実際のパスワードではなくパスワードの名前を使用してパスワードを参照します。その後、Identity Manager エンジンからドライバにパスワードが送信されます。この節で説明する名前付きパスワードの保存と復元の方法は、ドライバシムを変更することなく、どのドライバでも使用できます。

新しい名前付きパスワードを追加するには、アイコンをクリックします。既存の名前付きパスワードを削除するには、アイコンをクリックします。リストを保存するには、アイコンをクリックします。

Security Equals (同等セキュリティ)

［同等セキュリティ］ページを使用して、ドライバが明示的に同等セキュリティになっているオブジェクトのリストの表示または変更ができます。このオブジェクトは、実質、リスト内のオブジェクトのすべての権利を持っていることになります。

［同等セキュリティ］リストに新しいオブジェクトを追加するには、アイコンをクリックします。リストにオブジェクトを追加したり、リストからオブジェクトを削除したりすると、システムは自動的に、そのオブジェクトの「同等セキュリティ保有者」プロパティに対してこのオブジェクトが追加されたり削除されたりします。このオブジェクトの［Public］トラスティまたは親コンテナは、リストに追加する必要はありません。これは、このオブジェクトが、暗黙的に［Public］トラスティまたは親コンテナに対して同等セキュリティを持つためです。

このリストから既存のオブジェクトを削除するには、アイコンをクリックします。リストを保存するには、アイコンをクリックします。

除外オブジェクト

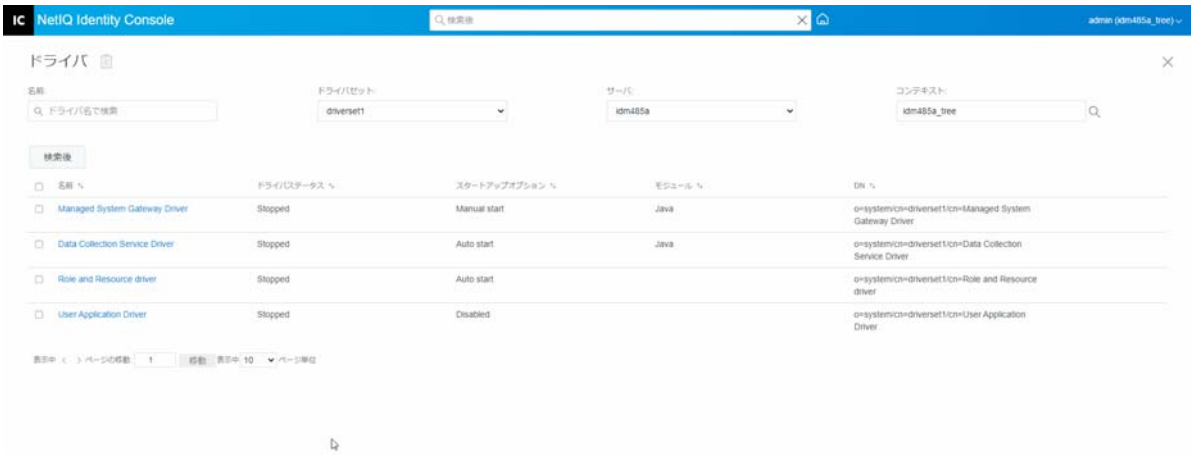
このオプションでは、アプリケーションに複製しないオブジェクトのリストを作成できます。管理者の役割を表すオブジェクト (Admin オブジェクトなど) はすべてこのリストに追加しておくことをお勧めします。このリストに新しいオブジェクトを追加するには、アイコンをクリックします。このリストから既存のオブジェクトを削除するには、アイコンをクリックします。リストを保存するには、アイコンをクリックします。

値がある属性のリストの管理

特定のドライバについて値がある属性のリストに属性を追加するには、次の手順を実行します。

1. Identity Console で、［**[オブジェクト管理]**］モジュールを選択します。
2. ドロップダウンリストから **[Dir-XML-Driver]** タイプを選択し、［検索］ボタンをクリックします。
3. 検索リストから適切なドライバをクリックします。
4. 値のない属性を値のある属性のリストに追加するには、［**[値がある属性]**］の横のアイコンをクリックし、リストから適切な値のない属性を選択します。
5. 完了したら、［**[OK]**］をクリックします。

図 23-2 ドライバ環境設定の管理



データ変換と同期

このセクションは、次のカテゴリで構成されています。

- 168 ページの 「データ同期ビュー」
- 171 ページの 「クラス属性フィルタ」
- 172 ページの 「ECMA Script」
- 172 ページの 「相互属性マッピング」

データ同期ビュー

[ドライバの概要] ページは、次のカテゴリに分かれています。

- 169 ページの 「フィルタ」
- 169 ページの 「すべてのポリシー」
- 169 ページの 「アイデンティティボールトへのデータの移行」
- 170 ページの 「アイデンティティボールトからのデータの移行」
- 170 ページの 「オブジェクトの同期」
- 170 ページの 「DirXML スクリプトのトレース」

フィルタ

フィルタはドライバに存在します。フィルタを使用すると、アプリケーションがアイデンティティボールトに送ったり、アイデンティティボールトから受け取ったりできるクラスおよび属性を指定できます。メタディレクトリエンジンで処理する特定のクラスを使用する場合は、該当するチャネルのフィルタにそのクラスを追加する必要があります。定義した特定の属性値でオブジェクトをフィルタすることもできます。

同期に含めるクラスと属性を追加し、ドライバフィルタを変更するには、発行者チャネルまたは購読者チャネルで [**[フィルタ]**] をクリックします。

注 : [概要] のグラフィックでは、発行者チャネルと購買者チャネル上のドライバフィルタに対して 2 つのオブジェクトが表示されていますが、これらは、両方のチャネルで使用される同じフィルタです。

すべてのポリシー

デフォルトでは、[すべてのポリシー] ページが表示されます。コンテナ内に既存のポリシーをインポートするには、  アイコンをクリックします。不要なポリシーを削除することもできます。ドライバのトレースレベルを選択するには、  アイコンをクリックします。リスト内でポリシーを上下に移動するには、  およびアイコンを使用します。

注 : ドライバの新しいポリシーの追加と展開は、Identity Console ではサポートされていません。新しいポリシーを追加および展開するには、iManager および Identity Designer を使用することをお勧めします。

アイデンティティボールトへのデータの移行

このタスクを使用すると、アプリケーションからアイデンティティボールトにオブジェクトを移行する際に Identity Manager が使用する条件を定義できます。オブジェクトを移行すると、メタディレクトリエンジンによって、「一致」、「配置」、および「作成」のすべてのポリシーと、購読者フィルタがそのオブジェクトに適用されます。オブジェクトは、クラスリストで指定した順序で、アイデンティティボールトに移行されます。このオプションを使用して、次のタスクを実行できます。

1. **クラスと属性の追加** : 移行するクラスおよび属性を追加または削除するには、  アイコンをクリックします。次に、追加するクラスとその属性を選択します。クラスと属性を選択した後、[**[追加]**] をクリックして変更を保存します。
2. **属性値の編集** : リストの編集時に指定した移行属性値を変更する場合は、属性の編集  アイコンをクリックします。
3. **クラスリストの順序を変更する** : リスト内のクラスの順序を変更するには、  ボタンとボタンを使用します。オブジェクトは、クラスリストで指定した順序で、アイデンティティボールトに移行されます。
4. **更新 :**  アイコンをクリックすると、リストが更新されます。

アイデンティティボールトからのデータの移行

[**[エクスポート]**]タブを使用すると、アイデンティティボールトからアプリケーションに移行するコンテナまたはオブジェクトを選択できます。オブジェクトを移行すると、メタディレクトリエンジンが一致ポリシー、作成ポリシー、および配置ポリシーのすべてと、購読者フィルタをオブジェクトに適用します。

アイデンティティボールトから別のアプリケーションにオブジェクトまたはコンテナを移行する場合は、  アイコンをクリックします。移行するオブジェクトをブラウズして選択し、[**[OK]**]をクリックすると、選択したオブジェクトが移行リストに追加されます。移行リストからオブジェクトを削除する場合は、  アイコンをクリックします。

移行するオブジェクトの選択が終わったら、  をクリックしてマイグレーションを開始します。マイグレーションの進行状況が画面に表示されます。マイグレーションを停止する場合は、  ボタンをクリックします。

オブジェクトの同期

同期処理は、変更されたオブジェクトを検索し、それらを同期します。[**[すべてのオブジェクトを調べる]**]を選択して、同期をすぐに開始することもできます。または、同期を開始する日付 / 時刻を設定できます。

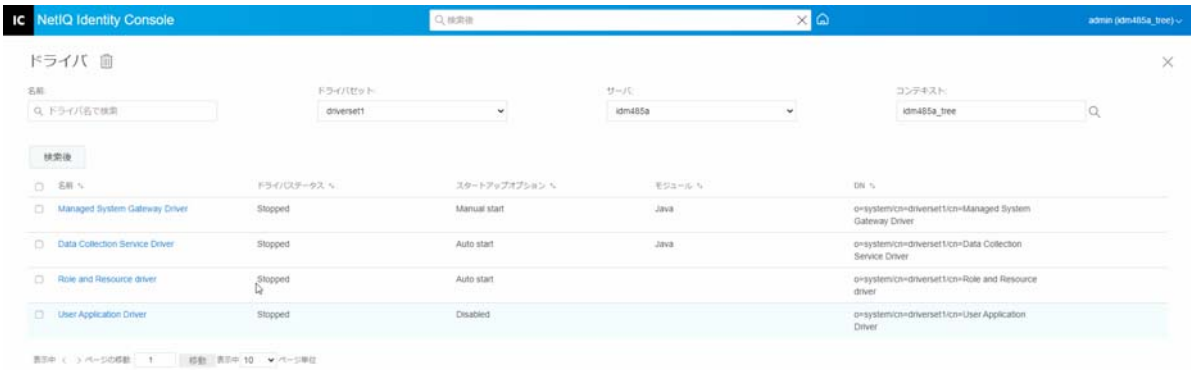
DirXML スクリプトのトレース

[Tracing DirXML Scripts (DirXML スクリプトのトレース)]オプションを使用すると、ドライバのトレースレベルを選択できます。さらに、すべての発行者チャネルおよび購読者チャネルにトレース設定が適用されます。次の DirXML スクリプトトレースオプションを選択できます。

- すべての DirXML スクリプトトレースをオンにする
- すべての DirXML スクリプトトレースをオフにする
- DirXML スクリプトルールのトレースオン
- DirXML スクリプトルールのトレースオフ

 をクリックして変更内容を保存します。

図 23-3 ドライバのデータ同期の管理



クラス属性フィルタ

クラス属性フィルタを使用すると、アプリケーションがアイデンティティボールトに送ったり、アイデンティティボールトから受け取ったりできるクラスおよび属性を指定できます。メタディレクトリエンジンで処理する特定のクラスを使用する場合は、該当するチャネルのフィルタにそのクラスを追加する必要があります。また、定義した属性値でオブジェクトをフィルタリングすることもできます。このオプションを使用して、次のアクションを実行することができます。

- **Set Template (テンプレートの設定)**: このオプションを使用して、フィルタに追加されるすべての属性のデフォルトオプションを設定します。［クラス属性フィルタ］ラベルの横のアイコンをクリックします。
- **新しいクラスの追加** : アイコンをクリックして新しいクラスを追加します。
- **新しい属性の追加** : アイコンをクリックして新しい属性を追加します。
- **フィルタのコピー元** : このオプションを使用すると、別のドライバからフィルタをコピーできます。アイコンをクリックしてフィルタをコピーします。
- **XML の編集** : XML ファイルの編集アイコンを使用して、クラスおよび属性のフィルタ設定を編集します。
- **Delete Class or Attributes（クラスまたは属性の削除）**: それぞれのクラスまたは属性の横にあるアイコンをクリックして、任意のクラスまたは属性を削除します。

発行者チャネルと購読者チャネルの両方で、クラスと属性値に次のオプションを設定できます。

- 同期
- 無視

- お知らせ君
- リセット

マージ権限

属性がどちらのチャネルでも同期されていない場合、マージは行われません。

属性が一方のチャネルだけで同期されている場合は、そのチャネルのターゲットの既存の値がすべて削除され、そのチャネルのソースの値と置き換えられます。ソースに複数の値があるが、ターゲットでは値を 1 つしか受け取れない場合は、値のうち 1 つだけがターゲット側で使用されます。

属性が両方のチャネルと両方のサイドで同期化されている場合、1 つの値のみ設定できます。接続されたアプリケーションは、アイデンティティボールトに値がない場合を除き、アイデンティティボールトに格納されている値を取得します。このシナリオでは、アイデンティティボールトは接続されたアプリケーションから値を取得します。

属性が両方のチャネルで同期され、一方だけが複数の値を受け入れられる場合は、単一値チャネルからの値しか受入れられない方の値が複数値側に存在していない場合に限り、複数値側に追加されます。単一の側に値がない場合は、単一の側に追加する値を選択できます。マージ権限には、以下のオプションを設定できます。

- デフォルト
- アイデンティティボールト
- アプリケーション
- なし

をクリックして変更内容を保存します。

ECMA Script

ECMAScript リソースファイルの順序付きリストを表示します。ファイルには、ドライバの起動時に Identity Manager がロードするドライバの拡張機能が含まれています。追加のファイルをインポートするには、をクリックします。既存のファイルを削除するには、をクリックします。または、実行するファイルの順序を変更します。リスト内でスクリプトを上下に移動することもできます。ECMA スクリプトリストを保存するには、アイコンをクリックします。

相互属性マッピング

相互属性マッピングでは、オブジェクト間のバックリンク、つまり参照を作成および管理できます。たとえば、グループオブジェクトには、そのグループに属するユーザオブジェクトすべてを参照するメンバー属性が含まれています。同様に、各ユーザオブジェクトには、そのユーザがメンバーであるグループオブジェクトを参照するグループメンバーシップ属性が含まれています。メタディレクトリエンジンで、アイデンティティボールト内にある [グループオブジェクト] > [Members attribute synchronized with the User object(ユーザオブジェクトと同期されているメンバー属性)] > [Group Membership attribute for all Group

objects and User objects(すべてのグループオブジェクトおよびユーザオブジェクトのグループメンバーシップ属性)] を保つには、これらの属性がリンクされている必要があります。このオブジェクト属性間のリンクを相互属性マッピングと呼びます。

このモジュールを使用して、次のアクションを実行することができます。

- 173 ページの 「カスタム相互属性マッピングの作成」
- 173 ページの 「新しい相互属性マッピングの追加」
- 174 ページの 「相互属性マッピングの削除」
- 174 ページの 「相互マッピングリストからの属性の削除」
- 174 ページの 「マップ済み属性の並べ替え」
- 174 ページの 「カスタム相互属性マッピングの削除」
- 174 ページの 「相互属性 XML の編集」

カスタム相互属性マッピングの作成

このセクションは、[相互属性マッピング] ページに、[**[ドライバにカスタム相互属性マッピングが含まれていません。上の [+] アイコンをクリックして、基本的な相互属性マッピングを作成してください]**] というプロンプトが表示された場合にのみ該当します。

1 新しいカスタム相互属性マッピングリストを作成するには、＋アイコンをクリックします。

2 ドライバのデフォルトの属性マッピングが表示されます。マッピングを追加するか、既存のマッピングを変更するか、またはマッピングを削除することができます。

新しい相互属性マッピングの追加

相互属性マッピングを作成する場合は、まず相互マッピングリストに属性の 1 つを追加する必要があります。

1 [アクション] のドロップダウンメニューの横にある＋アイコンをクリックします。

2 新しい属性エントリで、ドロップダウンリストから目的の属性を選択します。

3 相互マッピングの詳細を指定します。

3a **ソースクラス** : マッピングリスト内の属性が関連付けられているクラス名を指定します。たとえば、相互マッピングリストにグループメンバーシップ属性を配置した場合、関連付けられたソースクラスはユーザになります。

3b **宛先クラス** : 相互マッピングを作成する属性に関連付けられたクラス名を指定します。たとえば、相互マッピングリストにグループメンバーシップ属性を配置した場合、関連付けられた宛先クラスはグループになります。

3c **相互属性** : 相互マッピングを作成する属性名を指定します。

4 属性を別の相互属性にマップする場合は、属性名の右側にある＋アイコンをクリックします。

属性の新しいセクションが属性リストの末尾に追加されます。ソースクラス、宛先クラス、および相互属性を選択します。

相互属性マッピングの削除

相互属性マッピングを削除するには、次の手順を実行します。

1 [ソースクラス] の前で削除する相互属性マッピングのチェックボックスをオンにします。

2 属性ドロップダウンリストの横にあるアイコンをクリックします。

相互マッピングリストからの属性の削除

相互マッピングリストから属性を削除するには、次の手順を実行します。

1 削除する属性の前にあるチェックボックスをオンにして、削除する属性を選択します。

2 ［ [アクション]］のドロップダウンリストの横にあるアイコンをクリックします。

マップ済み属性の並べ替え

属性マッピングは、リストの順番に従って上から下に解決されます。リスト内でマップ済み属性を上下に移動して、正しい順序で解決されるようにすることができます。一般的には、詳細なマッピングをリストの最初に配置し、その後により一般的なマッピングを配置することをお勧めします。たとえば、グループオブジェクトのメンバー属性のマッピングは、すべてのオブジェクトのメンバー属性のマッピング (［< 任意のクラス >］オプション) より前に一覧にする必要があります。

移動するマップ済み属性の前にあるチェックボックスをオンにし、属性を上へ移動する場合は↑、下へ移動する場合は↓をそれぞれクリックします。

カスタム相互属性マッピングの削除

作成したカスタム属性マッピングを削除することができます。カスタム属性マッピングを削除すると、メタディレクトリエンジンは、ドライバのデフォルトの属性マッピングを使用するようになります。

カスタム相互属性マッピングを削除するには、画面上部のアイコンをクリックします。

相互属性 XML の編集

必要に応じて、相互属性の XML を直接編集できます。これを行うには、［カスタム相互属性マッピング］ページの［XML の編集］アイコンをクリックします。これにより、XML を変更できる基本的な XML エディタが開きます。終了したら、［OK］または［キャンセル］をクリックして XML エディタを閉じます。

詳細設定

詳細設定は、次のカテゴリに分かれています。

- 175 ページの 「エンタイトルメントの管理」
- 175 ページの 「オブジェクトマッピングテーブルの管理」
- 176 ページの 「ドライバのジョブの管理」

エンタイトルメントの管理

[エンタイトルメント] ページには、選択したドライバで現在定義されているすべてのエンタイトルメントの表があります (完全識別名でリストされています)。このページでは、次のアクションが許可されています。

- **Edit in XML（XML で編集）**: XML ファイルのエンタイトルメントを編集するには、リストからエンタイトルメントを選択し、アイコンをクリックします。次に、[**[Enable XML Editing（XML 編集を有効にする）]**] ボックスをオンにします。
- **削除** : エンタイトルメントを削除するには、エンタイトルメント名の左側にあるボックスをオンにし、アイコンをクリックします。操作は元に戻せないことを示すメッセージと、選択したエンタイトルメントの削除確認メッセージが表示されます。エンタイトルメントを削除する場合は [**[OK]**] をクリックし、操作を中断する場合は [**[キャンセル]**] をクリックします。複数のエンタイトルメントを削除するには、複数のボックスをクリックします。すべてのエンタイトルメントを削除するには、左上のボックスをクリックします。

オブジェクトマッピングテーブルの管理

Identity Manager ポリシーは、マッピングテーブルを使用して、1 組の値を対応する他の 1 組の値にマップします。エンタイトルメントパッケージをインストールすると、このパッケージのポリシーがドライバ起動ポリシーセットに追加されます。ドライバは、ドライバの起動時にこれらのポリシーを一度だけ実行します。詳細については、『NetIQ Identity Manager ドライバ管理ガイド』の *Mapping Table Objects（テーブルオブジェクトのマッピング）* を参照してください。

オブジェクトマッピングテーブルを使用して、次のアクションを実行できます。

- **Modify an existing Mapping（既存のマッピングの変更）**: 既存のオブジェクトマッピングテーブルを変更するには、リストからマッピングをクリックして、次の画面で次のアクションを実行します。
  - 新しい列の追加。

    列の値を指定してから、値が「大文字と小文字の区別あり」、「大文字と小文字の区別なし」、または数値なのかを指定します。
  - 新しい行を追加し、その行の値を指定します。
  - アイコンをクリックします。

- **Delete Mapping（マッピングの削除）**：リストからマッピングを削除するには、リストから適切なマッピングを選択し、アイコンをクリックします。
- **Edit in XML（XML で編集）**：XML ファイルでマッピングを編集するには、リストからマッピングをクリックしてアイコンを選択します。次に、[**[Enable XML Editing（XML 編集を有効にする）]**] ボックスをオンにします。

ドライバのジョブの管理

Identity Console では、すべての個々のドライバの［ジョブ］オプションを使用してイベントをスケジュールできます。

［ジョブスケジューラ］ページには、ジョブの名前、ジョブが有効か無効か、実行スケジュール、およびジョブの説明が含まれています。［ジョブ］ページを表示するには、ジョブ名をクリックします。ジョブを有効または無効にするには、［有効］列の下で［有効 / 無効］アイコンをクリックします。ジョブの詳細を表示するには、ジョブの説明をクリックします。

［ジョブ］タブには、選択したドライバの既存のジョブオブジェクトが表示される表が含まれています。選択したドライバは、［ドライバ］エントリに完全識別名で一覧されます。

［ジョブスケジューラ］ページでは、次のタスクを実行できます。

- **ジョブの作成**：アイコンをクリックして新しいジョブを作成します。

  [**新規ジョブ**] ポップアップで新しいジョブを作成するには、次の手順を実行します。

  1. ジョブ名を指定します。
  2. ジョブタイプを選択します。
  3. アイコンをクリックし、使用可能なサーバのリストからジョブを実行するサーバを選択します。それ以外の場合は、サーバ名を指定してからサーバを選択します。
  4. [**[作成]**] ボタンをクリックします。
- **ジョブの開始**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。
- **ジョブの停止**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。
- **ジョブの有効化**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。
- **ジョブの無効化**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。
- **ステータスの取得**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。
- **ジョブの削除**：ジョブの左側にあるボックスをオンにしてジョブを選択してから、アイコンをクリックします。

ジョブをクリックして［**Job Property(ジョブプロパティ)**］ページにアクセスします。このページで、ジョブの実行方法を設定できます。

一般 : ジョブの Java クラス名が表示されます。このページを使用して、ジョブを有効または無効にする、実行後にジョブを削除する、このジョブを実行するサーバ (1 つまたは複数) を選択する、電子メールサーバを指定する、ジョブに別の表示名と説明を付けることができます。

スケジュール : ジョブの実行時期を設定できます。ジョブ開始時間を指定して時刻を設定し、ジョブを毎日、毎週、毎月、毎年実行するかどうかを指定します。ジョブを実行する時間をカスタマイズしたり、トグルを有効にしてジョブを手動で実行したりすることもできます。

スコープ : このジョブを適用するオブジェクトを定義できます。オブジェクトはコンテナ、動的グループ、グループ、またはリーフオブジェクトです。［追加］をクリックして、このジョブを適用するオブジェクトを選択します。［参照］ボタンを使用してオブジェクトを選択して、［OK］をクリックすることもできます。オブジェクトをスコープリストから削除するには、DN オブジェクトの左側にあるボックスをオンにしてスコープオブジェクトを選択してから、［削除］をクリックします。

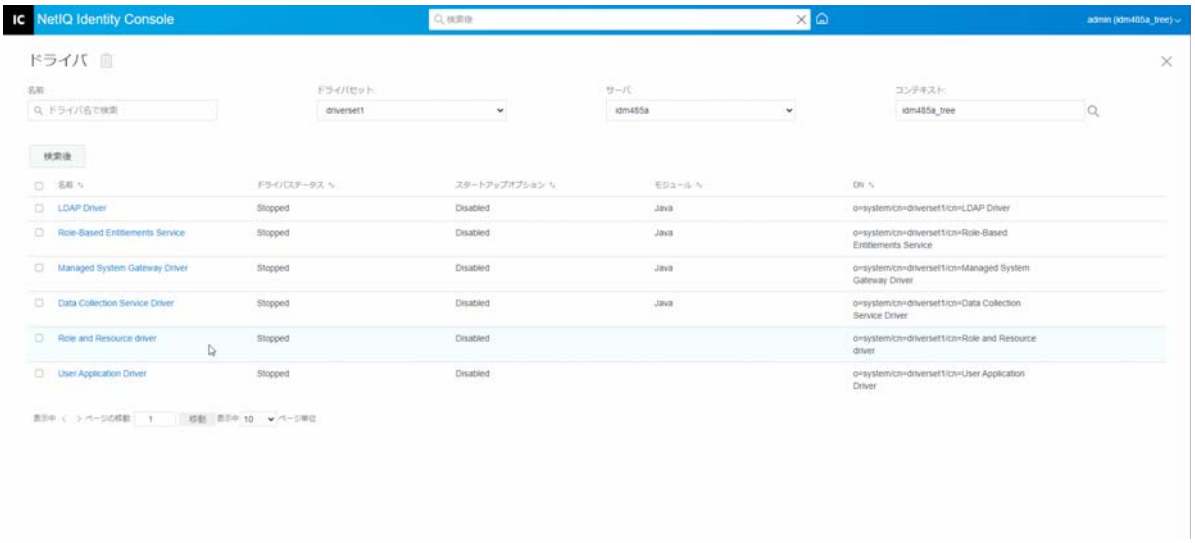
オブジェクトが追加されたら、それを選択してさらにオプションを表示します。グループオブジェクトを選択すると、ジョブをグループのメンバーまたはグループのみに適用するオプションが表示されます。コンテナオブジェクトを選択した場合は、ジョブをそのコンテナのすべての子孫に適用するか、そのコンテナのすべての子に適用するか、それともそのコンテナのみに適用するかを選択できます。

パラメータ : 追加パラメータをジョブに追加して、現在設定されているパラメータを確認できます。これらのパラメータは、選択したジョブのタイプに応じて異なります。

結果 : ジョブの結果で行うことを定義できます。結果ページは［中間結果］と［最終結果］の 2 つの部分に分かれており、次の結果が表示されます。「成功」、「警告」、「エラー」、および「中止」。［結果］列の右側は［アクション］列です。［アクション］列をクリックすると、各結果の通知方法を設定できます。アクションには、「監査結果の送信」、または「結果が出た際に電信メールで送信する」が含まれます。オプションを選択しないと、結果に対するアクションは行われません。

[**トレース**] タブでは、特定のドライバのトレースを設定できます。詳細については、179 ページの 「トレースレベルの設定」を参照してください。

図 23-4 詳細設定の管理



ドライバのログレベルとトレースレベルの設定

ドライバのログとトレースを設定するには、Identity Console のメインページから、[[ドライバ]] > [[ログとトレースの環境設定]] タブを選択します。このセクションは、次のカテゴリで構成されています。

- 178 ページの 「ログレベルの設定」
- 179 ページの 「トレースレベルの設定」

ログレベルの設定

各ドライバにはログレベルフィールドがあります。このフィールドで、追跡するエラーレベルを定義できます。ここで指定するレベルによって、ログに記録されるメッセージの種類が決まります。デフォルトでは、ログレベルはエラーメッセージを追跡するように設定されています。(これには致命的エラーも含まれます。) 追加のメッセージタイプを追跡するには、ログレベルを変更します。ログレベルを設定するには、[[ログとトレースの環境設定]] > [[ログレベル]] タブを選択します。次のテーブルは、ログレベルの設定を示します。

オプション	説明
[Use log settings from the Driver Set（ドライバセットのログ設定を使用する）]	このオプションを選択すると、ドライバはドライバセットオブジェクトのログ設定に基づいてイベントを記録します。
[Turn off logging to Driver Set, Subscriber and Publisher logs（ドライバセット、購読者および発行者ログへのログ記録をオフにする）]	ドライバセットオブジェクト、購読者チャネル、および発行者チャネルで、このドライバのすべてのログ記録をオフにします。
[ログ内のエントリの最大数 (50-500)]	ログ内のエントリ数。デフォルト値は「50」です。

オプション	説明
[ログレベル]	次のログレベルを選択できます。 ◆ [エラーをログに記録]: エラーをログに記録します。 ◆ エラーと警告をログに記録 : エラーと警告のログを記録します。 ◆ [特定のイベントをログに記録]: 選択したイベントをログに記録します。このオプションを選択すると、次のイベントのリストが有効になります。 ◆ [Metadirectory Engine Events (メタディレクトリエンジンイベント)] ◆ [ステータスイベント] ◆ [操作イベント] ◆ [変換イベント] ◆ [資格情報プロビジョニングイベント] ◆ [最終ログ時刻のみを更新]: 最後のログ時刻を更新します。 ◆ [ログ記録のオフ]: ドライバのログ記録をオフにします。

トレースレベルの設定

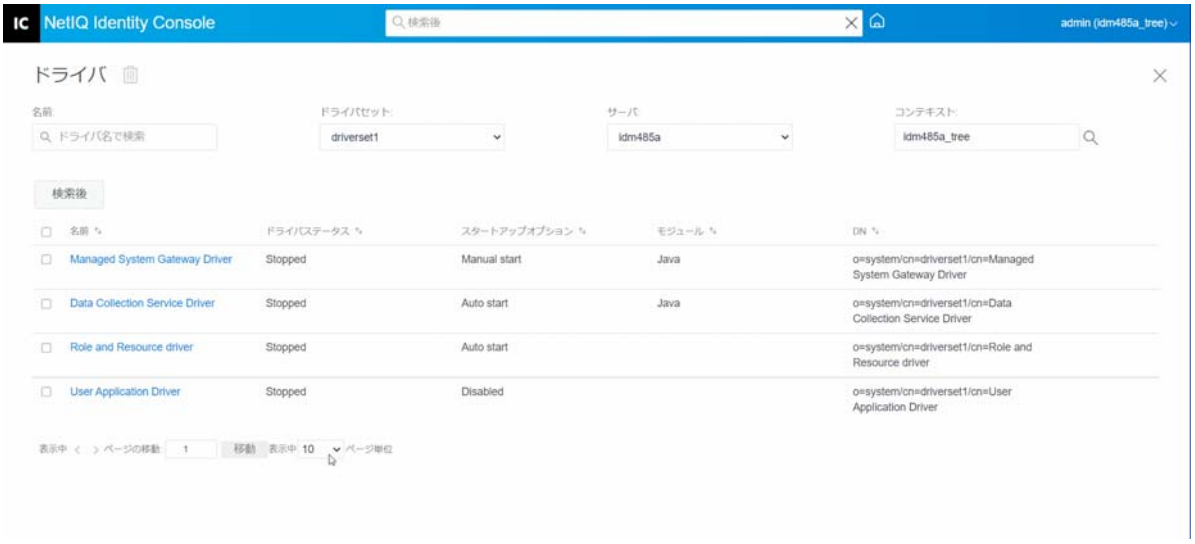
特定のドライバのトレースを設定できます。ドライバに指定されたトレースレベルに応じて、エンジンがイベントを処理するときにトレースにドライバ関連のイベントが表示されます。ドライバトレースレベルは、トレースが設定されているドライバまたはドライバセットにのみ影響します。リモートローダを使用している場合は、リモートローダのトレースファイルは直接リモートローダに設定され、ドライバシムトレースのみが含まれます。

ドライバのトレースを設定するには、[[ログとトレースの環境設定]] > [[トレース]] タブを選択します。次のテーブルは、トレース設定を示します。

パラメータ	ドライバ
トレースレベル	ドライバのトレースレベルを上げると、トレースに表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因にはなりません。パスワード同期の情報を表示するには、トレースレベルを 5 に設定します。 [[ドライバセットの設定を使用する]] を選択した場合、値はドライバセットから取得されます。

パラメータ	ドライバ
トレースファイル	選択したドライバに対して、ファイル名および Identity Manager 情報を書き込む場所を指定します。 [**[ドライバセットの設定を使用する]**] を選択した場合、値はドライバセットから取得されます。
トレース名	ドライバトレースメッセージの前に、ドライバ名の代わりに入力した値が付きます。ドライバ名が長い場合に使用します。
トレースファイルのエンコーディング	トレースファイルはシステムのデフォルトのエンコーディングを使用します。必要な場合には、他のエンコーディングを指定できます。
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズが増加します。 **注 :** ファイルサイズの制限が指定されている場合、トレースファイルは複数のファイルに作成されます。Identity Manager により自動的に最大のファイルサイズが 10 で割られ、10 個のファイルが作成されます。これらのファイルを組み合わせたサイズが、トレースファイルの最大サイズと等しくなります。 [**[ドライバセットの設定を使用する]**] を選択した場合、値はドライバセットから取得されます。

図 23-5 *ドライバのログレベルとトレースレベルの管理*



ドライバを点検する

ドライバインスペクタを使用して、ドライバに関連付けられているオブジェクトに関する詳細情報を表示できます。このセクションは、次のカテゴリで構成されています。

ドライバインスペクタ

ドライバに関連付けられているオブジェクトを表示するには、次の手順を実行します。

1 Identity Console で、[ドライバ] > [インスペクタ] > [ドライバインスペクタ] タブを選択します。

2 [ドライバ] フィールドで、点検するドライバの完全識別名を指定するか、[ブラウズ] アイコンをクリックして目的のドライバをブラウズして選択します。

3 点検するドライバを選択した後、[OK] をクリックして [ドライバインスペクタ] ページを表示します。

このページには、選択したドライバに関連付けられているオブジェクトに関する情報が表示されます。次の任意のアクションを実行できます。

- **削除** : ドライバとオブジェクトの関連付けを解除します。ドライバに関連付けたくないオブジェクトの前にあるチェックボックスをオンにして、アイコンをクリックし、[OK] をクリックして削除を確認します。
- **更新** : リフレッシュアイコンを選択します。このオプションは、ドライバに関連付けられているすべてのオブジェクトを再読み込みして、情報を更新します。
- **表示** : 1 ページごとに表示する関連付けの数を選択します。定義済みの数 (25、50、または 100) を選択することも、それ以外の好きな数を指定することもできます。デフォルトは 1 ページに 10 の関連付けです。表示されている数よりも関連付けが多い場合は、矢印およびボタンを使用すると、関連付けの次のページおよび前のページを表示できます。
- **アクション** : ドライバに関連付けられたオブジェクトに対してアクションを実行します。[アクション] をクリックし、次のいずれかのオプションを選択します。
  - **すべての関連付けを表示** : ドライバに関連付けられているすべてのオブジェクトを表示します。
  - **無効な関連付け用フィルタ** : 無効状態のドライバに関連付けられているすべてのオブジェクトを表示します。
  - **手動関連付け用フィルタ** : 手動状態のドライバに関連付けられているすべてのオブジェクトを表示します。

- **マイグレート関連付け用フィルタ**：マイグレート状態のドライバに関連付けられているすべてのオブジェクトを表示します。
- **保留中の関連付け用フィルタ**：保留中状態のドライバに関連付けられているすべてのオブジェクトを表示します。
- **処理された関連付け用フィルタ**：処理された状態のドライバに関連付けられているすべてのオブジェクトを表示します。
- **未定義の関連付け用フィルタ**：未定義の状態のドライバに関連付けられているすべてのオブジェクトを表示します。
- **関連付けの概要**：ドライバに関連付けられているすべてのオブジェクトの状態を表示します。

- **オブジェクト DN:** 関連付けられているオブジェクトの DN を表示します。
- **ステータス**：オブジェクトの関連付けの状態を表示します。
- **オブジェクト ID:** 関連付けの値を表示します。

ドライバキャッシュインスペクタ

Identity Console を使用して、ドライバのキャッシュファイルでトランザクションを表示できます。[ドライバキャッシュインスペクタ] には、ドライバによって処理されるイベントのリストなどのキャッシュファイルに関する情報が表示されます。

1 Identity Console で、[[ドライバ]] > [[インスペクタ]] > [[ドライバキャッシュインスペクタ]] タブを選択します。

2 [[ドライバ]] フィールドで、点検するキャッシュを持つドライバの完全識別名を指定するか、ブラウズアイコンをクリックして目的のドライバをブラウズして選択し、[[OK]] をクリックして、[ドライバキャッシュインスペクタ] ページを表示します。

ドライバのキャッシュファイルは、ドライバが実行されていない場合にのみ読み込み可能です。ドライバが停止している場合、[ドライバキャッシュインスペクタ] ページにキャッシュが表示されます。ドライバが実行中の場合、このページには、キャッシュエントリの代わりに Driver not stopped, cache cannot be read（ドライバが停止されておらず、キャッシュを読み込めません）メモが表示されます。ドライバを停止するには、⏸ボタンをクリックします。その後、キャッシュが読み込まれ、表示されます。

- **サーバ上のドライバのキャッシュ**：キャッシュファイルのこのインスタンスが含まれるサーバを一覧表示します。ドライバが複数のサーバで実行されている場合は、リスト内の別のサーバを選択して、そのサーバのドライバのキャッシュファイルを表示できます。
- **ドライバの起動 / 停止アイコン**：ドライバの現在の状態が表示され、ドライバを起動または停止できます。キャッシュは、ドライバが停止している間のみ読み込み可能です。
- **削除**：キャッシュ内のエントリを選択し、🗑アイコンをクリックしてキャッシュファイルから削除します。

- **アクション**：キャッシュファイル内にあるエントリに対してアクションを実行できます。[**[アクション]**] をクリックしてメニューを展開し、次のいずれかのオプションを選択します。
  - **すべてのキャッシュされたイベントのクリア**：キャッシュされたイベントをすべてクリアできます。
  - **キャッシュの概要**：キャッシュファイルに保存されているイベントすべての概要を表示します。

ドライバの接続システムの詳細を表示する

特定のドライバについて接続システムの詳細を表示するには、次の操作を実行します。

1. Identity Console で、[**[オブジェクトインスペクタ]**] モジュールをクリックします。
2. 接続システムを表示する特定のドライバオブジェクトをブラウズして選択します。
3. 選択したドライバオブジェクトについて、すべての接続システムの詳細がコンピュータに表示されます。

アウトオブバンド同期キャッシュインスペクタ

アウトオブバンド同期キャッシュのイベントを表示するには、次の手順を実行します。

1. Identity Console で、[**[ドライバ]**] > [**[インスペクタ]**] > [**[アウトオブバンド同期キャッシュインスペクタ]**] タブを選択します。
2. [**[ドライバ]**] フィールドで、キャッシュを点検するドライバの完全識別名を指定するか、ブラウズアイコンをクリックして目的のドライバをブラウズして選択し、[**[OK]**] をクリックします。

   ドライバのキャッシュファイルは、ドライバが実行されていない場合にのみ読み込み可能です。ドライバが停止している場合、[ドライバキャッシュインスペクタ] ページにキャッシュが表示されます。ドライバが実行中の場合、このページには、キャッシュエントリの代わりに Driver not stopped, cache cannot be read（ドライバが停止されておらず、キャッシュを読み込めません）メモが表示されます。ドライバを停止するには、⏸ボタンをクリックします。その後、キャッシュが読み込まれ、表示されます。
   - **キャッシュファイル名**：キャッシュのファイル名が表示されます。
   - **サーバ上のドライバのキャッシュ**：キャッシュファイルのこのインスタンスが含まれるサーバを一覧表示します。ドライバが複数のサーバで実行されている場合は、リスト内の別のサーバを選択して、そのサーバのドライバのキャッシュファイルを表示できます。
   - **ドライバの起動 / 停止アイコン**：ドライバの現在の状態が表示され、ドライバを起動または停止できます。キャッシュは、ドライバが停止している間のみ読み込み可能です。
   - **削除**：キャッシュ内のエントリを選択し、🗑アイコンをクリックしてキャッシュファイルから削除します。

- **アクション**: キャッシュファイル内にあるエントリに対してアクションを実行できます。[[アクション]] をクリックしてメニューを展開し、次のいずれかのオプションを選択します。
  - **キャッシュの概要**: キャッシュファイルに保存されているイベントすべての概要を表示します。
  - **すべてのキャッシュされたイベントのクリア**: キャッシュされたイベントをすべてクリアできます。

ドライバマニフェスト

ドライバマニフェストは、ドライバの要約のようなものです。ドライバのサポートする対象を示し、いくつかの環境設定情報も含まれます。ドライバマニフェストは、ドライバの開発者が指定します。通常、ネットワーク管理者がドライバマニフェストを編集する必要はありません。管理者がドライバマニフェストを編集する場合は、[[ドライバ]] > [[インスペクタ]] > [[ドライバマニフェスト]] > [[Enable XML Editing（XML 編集を有効にする）]] オプションを選択します。

ドライバのヘルスの監視

ドライバヘルスモニタリングを使用すると、ドライバの現在のヘルス状態を緑、黄色、または赤で参照したり、これらの各ヘルス状態に対応して実行するアクションを定義したりすることができます。

各ヘルス状態を判断する条件 (基準) を作成します。さらに、ドライバのヘルス状態が変化したときに実行するアクションも定義します。たとえば、ドライバのヘルスが緑の状態から黄色の状態に変化した場合、ドライバを再起動する、ドライバをシャットダウンする、ドライバの問題解決担当者に電子メールを送信するなどのアクションを実行できます。

このモジュールを使用して、次のタスクを実行することができます。

- 184 ページの 「ドライバのヘルス状態の変更」
- 187 ページの 「ドライバのヘルスアクションの変更」
- 189 ページの 「カスタム状態の作成」
- 189 ページの 「カスタム状態の変更」

ドライバのヘルス状態の変更

各ヘルス状態を判断する条件を制御します。緑の状態はヘルスの良好なドライバを表し、赤の状態はヘルスに問題があるドライバを表します。

緑の状態の条件が最初に評価されます。ドライバが緑の条件を満たさなかった場合、黄色の条件が評価されます。黄色の条件も満たさなかった場合は、自動的に赤の状態がドライバに割り当てられます。

状態の条件を変更する

1 Identity Console で、条件を変更するドライバの［ドライバヘルス環境設定］ページを開きます。

1a Identity Console のホームページを開きます。

1b ［**[ドライバ]**］>［**[リストから適切なドライバをクリック]**］>［**[インスペクタ]**］>［**[ドライバヘルス環境設定]**］を選択します。

2 変更する状態のタブ (［緑］または［黄色］) をクリックします。

ヘルス状態の現在の条件がタブに表示されます。条件はグループにまとめられています。AND または OR の論理演算子を使用して、各条件と各グループを結合できます。次に示す緑の状態の例について考えてみてください。

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

この例では、GROUP1 の条件または GROUP2 の条件のいずれかが true に評価されると、ドライバに緑の状態が割り当てられます。どちらの条件グループにも当てはまらない場合は、黄色の状態の条件が評価されます。

評価できる条件は次のとおりです。

- **ドライバ状態** : 実行中、停止、起動中、未実行、またはシャットダウン中のいずれかです。たとえば、緑のヘルス状態のデフォルト条件の 1 つは、ドライバが実行されていることです。
- **キャッシュオーバーフロー内のドライバ** : ドライバトランザクションを保持するために使用されるキャッシュの状態。ドライバがキャッシュオーバーフロー内にある場合、利用可能なキャッシュはすべて使用されています。たとえば、緑のヘルス状態のデフォルト条件は、キャッシュオーバーフロー内のドライバの状態が false であり、黄色のヘルス状態のデフォルトがキャッシュオーバーフロー内のドライバの状態が true であることです。
- **最新** : キャッシュ内にある最も新しいトランザクションの経過期間。
- **最も古い** : キャッシュ内にある最も古いトランザクションの経過期間。
- **合計サイズ** : キャッシュのサイズ。
- **未処理サイズ** : キャッシュ内にあるすべての未処理トランザクションのサイズ。
- **未処理のトランザクション** : キャッシュ内にある未処理トランザクションの数。すべてのトランザクションタイプを指定することも、特定のトランザクションタイプ (追加、削除、名前変更など) を指定することもできます。
- **トランザクション履歴** : 指定した時間内に発行者チャネルまたは購読者チャネルのさまざまなポイントで処理されたトランザクションの数。この条件は、

< トランザクションタイプ > < トランザクションの場所と期間 > < 関係演算子 > < トランザクション数 > という形式の複数の要素を使用します。

- < トランザクションタイプ >: 評価するトランザクションのタイプを指定します。ここには、すべてのトランザクション、追加、削除、名前変更などを指定できます。
- < *トランザクションの場所と期間*>: 発行者チャネルおよび購読者チャネルの場所と、評価する期間を指定します。たとえば、過去 48 時間に発行者レポートイベントとして処理されたトランザクションの合計数を評価できます。デフォルトでは、トランザクション履歴データは 2 週間保持されます。つまり、［トランザクション履歴データ期間］のデフォルト設定を変更しない限り、2 週間を超える期間を指定することはできません。
- < 関係演算子 >: 指定したトランザクションが < トランザクション数 > と等しいか、等しくないか、より小さいか、それ以下か、より大きいか、またはそれ以上でなければならないように指定します。
- < トランザクション数 >: 評価に使用するトランザクションの数を指定します。

次に、トランザクション履歴条件の例を示します。

< 追加の数 >< 発行者コマンドとして >< 過去 10 分間 >< は次の値より少ない ><1000>

- **利用可能な履歴** : 評価に利用できるトランザクション履歴データの量。この条件の主要な目的は、評価する期間中に十分なトランザクション履歴データが収集されていなかったために、トランザクション履歴条件が原因で現在の状態が失敗しないようにすることです。

  たとえば、トランザクション履歴条件を使用して、過去 48 時間における発行者コマンドとしての追加の数を評価するとします (前の「トランザクション履歴」の項に示した例)。ただし、まだ 48 時間分のデータがなくても、条件が失敗しないようにする必要があります。これには、ドライバのヘルス環境設定の初期セットアップ後や、ドライバのサーバが再起動した場合 (トランザクション履歴データはメモリ内に保持されるため) が該当します。したがって、次のような条件グループを作成します。

  Group1 使用可能な履歴 < は次の値より少ない ><48 時間 > または Group2 の利用可能な履歴 < は次の値以上 ><48 時間 > およびトランザクション履歴 < 追加の数 >< 発行者コマンドとして >< 過去 48 時間 >< は次の値より少ない ><1000>

  この状態は、いずれかの条件グループが true の場合、true と評価されます。つまり、a）48 時間以下のデータがあるか、b）少なくとも 48 時間分のデータがあり、過去 48 時間の発行者コマンドとしての追加の数が 1000 より小さい場合です。

  両方の条件が false に評価された場合、この状態は false に評価されます。つまり、a) 少なくとも 48 時間分のデータがあり、かつ b) 過去 48 時間における発行者コマンドとしての追加の数が 1000 より大きい場合です。

3 必要に応じて、条件を変更します。

- 新しいグループを追加するには、**[条件グループ]**の横にある＋アイコンをクリックします。

- 条件を追加するには、論理演算子 (AND/OR) の横にある＋アイコンをクリックします。または、[**新しい条件の追加**] リンクをクリックします。
- 条件グループまたは個々の条件を並べ替えるには、移動するグループまたは条件の隣にあるチェックボックスをオンにし、矢印ボタンをクリックして上または下へ移動します。矢印ボタンを使用してグループ間で条件を移動することもできます。

4 完了したら、[**保存**] ボタンをクリックして変更を保存します。

5 設定した条件に関連付けられているアクションを変更する場合は、187 ページの 「ドライバのヘルスアクションの変更」に進みます。

ドライバのヘルスアクションの変更

ドライバヘルス状態が変化したときに実行するアクションを指定することができます。たとえば、状態が緑から黄色に変化した場合、ドライバをシャットダウンまたは再起動してイベントを生成し、ワークフローを開始できます。または、状態が黄色から緑に変化した場合は、緑の状態に関連付けられているアクションが実行されます。

ヘルス状態のアクションは、条件が満たされるたびに一度だけ実行されます。状態が true のままである限り、アクションは繰り返されません。条件を満たさなくなったために状態が変化すると、次回条件を満たしたときにアクションが再度実行されます。

1 Identity Console で、変更するアクションを持つドライバの［ドライバヘルス環境設定］ページを開きます。

1a Identity Console のホームページを開きます。

1b [**ドライバ**] > [**リストから適切なドライバをクリック**] > [**インスペクタ**] > [**ドライバヘルス環境設定**] を選択します。

2 アクションを変更する状態の［ **緑** ］タブ、［ **黄色** ］タブ、または［ **赤** ］タブをクリックします。

3 [**アクション**] 見出しの横にあるプラス（＋）アイコンをクリックしてアクションを追加し、目的のアクションタイプを選択します。

- **［Start Driver］**：ドライバを起動します。
- **［Stop Driver］**：ドライバを停止します。
- **Restart Driver (ドライバの再起動):** ドライバを停止して起動します。
- **ドライバキャッシュのクリア :** 未処理のトランザクションを含むすべてのトランザクションをキャッシュから削除します。
- **電子メールの送信 :** 1 人または複数の受信者に電子メールを送信します。電子メールメッセージの本文に使用するテンプレートがすでに存在している必要があります。電子メールにドライバ名、サーバ名、および現在のヘルス状態の情報を含めるには、電子メールテンプレートに $Driver$、$Server$、および $HealthState$ トークンを追加し、メッセージテキストにこれらのトークンを含めます。例 :

  ```
  The current health state of the $Driver$ driver running on $Server$
  is $HealthState$.
  ```

重要 : 複数のユーザに電子メールを送信するには、各電子メールアドレスをカンマ (,) で区切ります。カンマの代わりにセミコロンを使用することはできません。

- **トレースメッセージの書き込み :** トレースファイルがドライバヘルスジョブで設定されていない場合は、ドライバヘルスジョブのログファイルまたはドライバセットのログファイルにメッセージを書き込みます。
- **イベントの生成 :** Audit および Sentinel で使用できるイベントを生成します。
- **ECMAScript の実行 :** 既存の ECMAScript を実行します。

  ECMA スクリプトの構築方法については、「*NetIQ Identity Manager - Using Designer to Create Policies（NetIQ IdentityManager-Designer を使用したポリシーの作成）*」の Using ECMAScript in Policies（ポリシーでの ECMAScript の使用）を参照してください。
- **ワークフローの開始 :** プロビジョニングワークフローを開始します。
- **エラー発生中 :** アクションが失敗した場合に、残りのアクション、現在のヘルス状態、およびドライバヘルスジョブを処理する方法を指示します。
  - **アクションへの影響の与え方 :** 残りのアクションを引き続き実行するか、残りのアクションの実行を停止するか、または現在の設定のデフォルトに戻すことができます。現在の設定が適用されるのは、複数のエラー時アクションを設定していて、前のいずれかのエラー時アクションで［アクションの実行者］オプションを設定している場合だけです。
  - **状態への影響の与え方 :** 現在の状態を保存するか、現在の状態を拒否するか、または現在の設定のデフォルトに戻すことができます。状態を保存すると、その状態の条件は引き続き true に評価されます。状態を拒否すると、その状態の条件は false に評価されます。現在の設定が適用されるのは、複数のエラー時アクションを設定していて、前のいずれかのエラー時アクションで［状態の実行者］オプションを設定している場合だけです。
  - **ドライバヘルスジョブへの影響の与え方 :** ジョブの実行を続行するか、ジョブを中止して使用不可にするか、または現在の設定のデフォルトに戻すことができます。ジョブの実行を続行すると、ジョブは条件の評価を終了し、ドライバのヘルス状態を決定して、その状態に関連付けられたアクションを実行します。ジョブを中止して使用不可にすると、ジョブの現在の動作が停止されてジョブがシャットダウンされます。使用可能にしない限り、このジョブは再度実行されません。現在の設定が適用されるのは、複数のエラー時アクションを設定していて、前のいずれかのエラー時アクションで［ドライバヘルスジョブの実行者］を設定している場合だけです。

4 完了したら、［**[保存]**］ボタンをクリックして変更を保存します。

カスタム状態の作成

1 つ以上のカスタム状態を作成して、ドライバの現在のヘルス状態 (緑、黄色、赤) とは別に、アクションを実行することができます。カスタム状態の条件を満たすと、現在のヘルス状態とは関係なく、そのアクションが実行されます。

緑、黄色、および赤のヘルス状態と同様に、カスタム状態のアクションは、条件を満たすたびに一度だけ実行されます。状態が true な状態のままである限り、アクションが繰り返されることはありません。条件を満たさなくなったために状態が変化すると、次回条件を満たしたときにアクションが再度実行されます。

1 Identity Console で、カスタム状態を作成するドライバの［ドライバヘルス環境設定］ページを開きます。

1a Identity Console のホームページを開きます。

1b［[ドライバ]］>［[リストから適切なドライバをクリック]］>［[インスペクタ]］>［[ドライバヘルス環境設定]］を選択します。

2 ドライバのヘルスステータスアイコン (緑、黄色、および赤) の横にある＋アイコンをクリックします

3 184 ページの 「ドライバのヘルス状態の変更」および 187 ページの 「ドライバのヘルスアクションの変更」の指示に従い、カスタム状態の条件とアクションを定義します。

カスタム状態の変更

カスタム状態を変更するには、次の手順を実行します。

1 Identity Console で、カスタム状態を作成するドライバの［ドライバヘルス環境設定］ページを開きます。

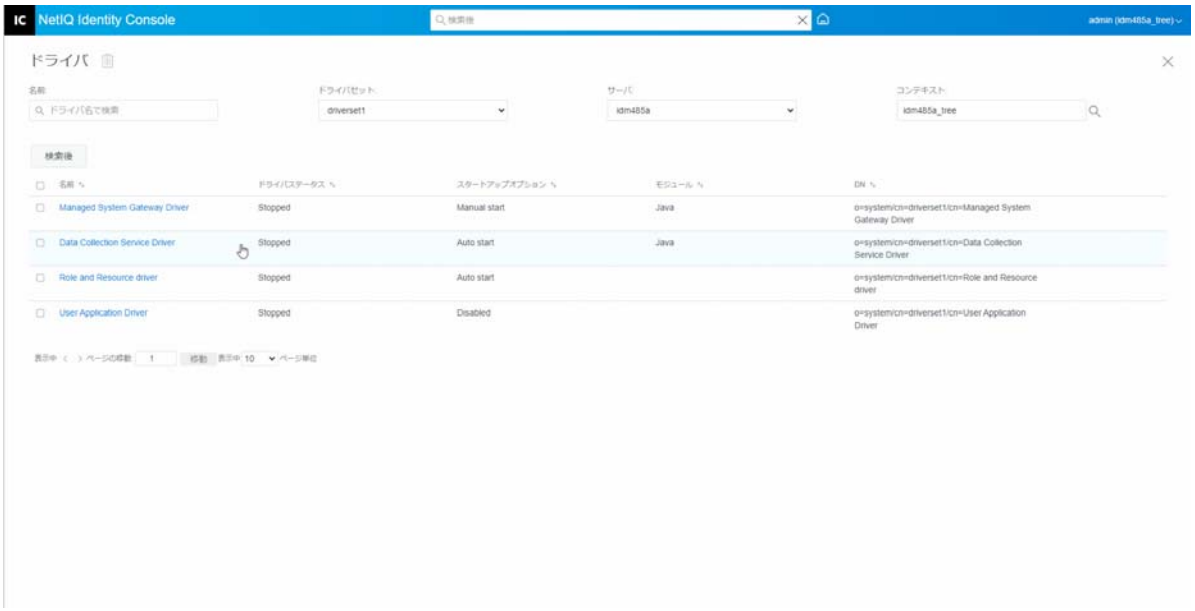
1a Identity Console のホームページを開きます。

1b［[ドライバ]］>［[リストから適切なドライバをクリック]］>［[インスペクタ]］>［[ドライバヘルス環境設定]］を選択します。

2 ドライバのヘルスステータスアイコン (緑、黄色、および赤) の横にある  アイコンをクリックします

3 184 ページの 「ドライバのヘルス状態の変更」および 187 ページの 「ドライバのヘルスアクションの変更」の指示に従い、カスタム状態の条件とアクションを定義します。

図 23-6 ドライバインスペクタの管理



24 ドライバセット統計の管理

Identity Console ポータルを使用して、単一のドライバまたはドライバセット全体に関するさまざまな統計情報を表示できます。これには、キャッシュファイルのサイズ、キャッシュファイル内の未処理トランザクションのサイズ、最も古いトランザクションと最新のトランザクション、およびカテゴリ別の未処理トランザクションの総数 (追加、削除、変更など) などの統計情報が含まれます。ドライバセットの統計を表示するには、次の手順を実行します。

1 Identity Console で、[**[ドライバセット統計]**] ページを開きます。

2 ドロップダウンから適切なサーバを選択します。

ドライバセットに含まれるすべてのドライバの統計を表示できるページが表示されます。

- 統計情報を更新するには、アイコンをクリックします。
- ドライバの統計情報を閉じるには、ドライバの統計情報ウィンドウの右上隅にあるボタンをクリックします。
- すべてのドライバの統計情報を開く場合は、[**[アクション]**] > [**[すべてを表示]**] をクリックします。
- ドライバの未処理トランザクションのリストを折りたたむには、リストの上にあるボタンをクリックします。すべてのドライバの未処理トランザクションのリストを折りたたむには、[**[アクション]**] > [**[すべてのトランザクションを折りたたむ]**] をクリックします。
- トランザクションのリストを開くには、ボタンをクリックします。すべてのドライバの未処理トランザクションのリストを開くには、[**[アクション]**] > [**[すべてのトランザクションを開く]**] をクリックします。
- 無効になっているドライバの統計ダッシュボードを閉じるには、[**[アクション]**] をクリックして、[**[無効なドライバを閉じる]**] を選択します。

図 24-1 ドライバセット統計の管理

25 Identity Manager オブジェクトの点検

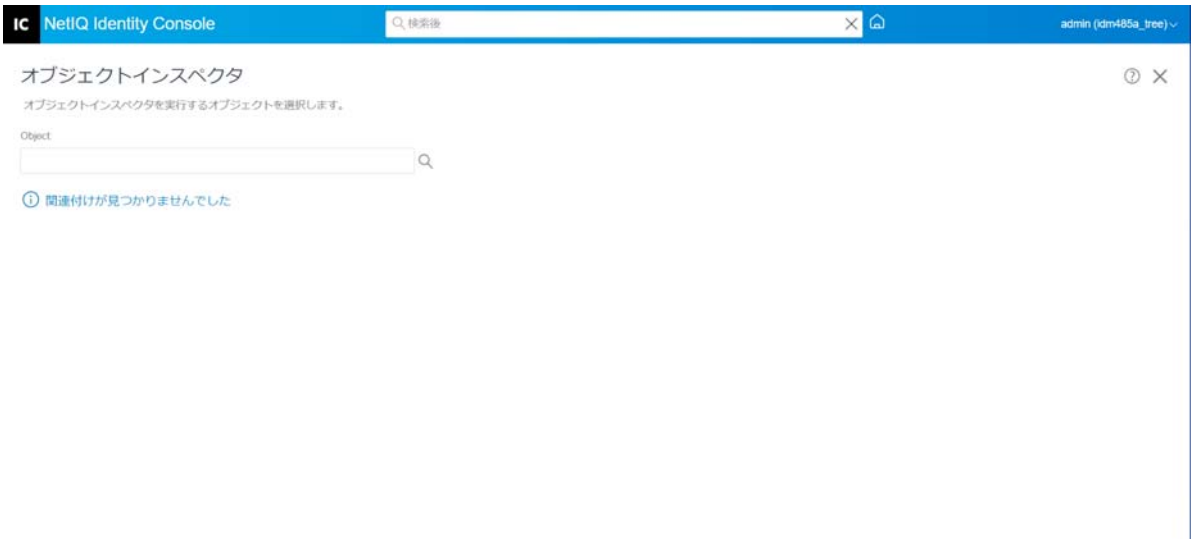
オブジェクトインスペクタを使用して、オブジェクトが Identity Manager 関係に参加する方法に関する詳細情報を表示できます。これらの関係には、オブジェクトに関連付けられている接続システム、アイデンティティボールトと接続システム間のデータフローの方法、現在アイデンティティボールトに格納されていて接続システムにある属性値、接続システムドライバ環境設定などが含まれます。

Identity Manager オブジェクトを点検するには、Identity Console のメインページから［[オブジェクトインスペクタ]］オプションをクリックします。点検するオブジェクトの完全識別名を指定するか、［ブラウズ］アイコンをクリックして、希望するオブジェクトをブラウズして、選択します。

［接続システム］セクションには、オブジェクトが関連付けられている各接続システムが一覧表示されます。［[オブジェクトインスペクタ]］ページでは、次のアクションを実行できます。

- **関連付けの追加** : 接続システムとの新しい関連付けを追加するには、＋アイコンをクリックします。［[統合ドライバオブジェクト]］をブラウズして選択し、[関連付けられたオブジェクト ID] を指定します。
- **関連付けの削除** : 接続システムとの関連付けを削除するには、関連付けの左にあるチェックボックスをオンにして、🗑アイコンをクリックします。すべての関連付けを削除するには、［削除］カラムの下にあるチェックボックスをオンにしてから、🗑アイコンをクリックします。

図 25-1 *Identity Manager オブジェクトの点検*



26 データフローの管理

データフローは、複数のドライバの発行者チャネルと購買者チャネルを 1 つのビューで示します。このオプションを使用して、すべてのドライバのデータ所有権を表示および更新できます。

データフローのテーブルビューにアクセスするには、Identity Console のメインページから [[データフロー (テーブルビュー)]] モジュールをクリックします。次に、適切なコンテナをブラウズして選択し、ドライバのリストを表示します。

個々のドライバのデータ所有権を管理するには、次の手順を実行します。

1 各ドライバには、発行者チャネルと購読者チャネルのデータフローを管理する 2 つのボタンがあります。左側のボタンは発行者チャネルのデータフローを管理し、右側のボタンは購読者チャネルのデータフローを管理します。

   1a **同期** : 特定の属性を同期するには、このオプションを選択します。このオプションを選択すると、発行者チャネルではアイコンが↑に、購読者チャネルではアイコンが↓に変更されます。

   1b **無視** : 特定の属性の同期を停止するには、このオプションを選択します。このオプションを選択すると、アイコンが⊘に変更されます。

   1c **通知** : 特定の属性に加えた変更について通知を受け取る場合は、このオプションを選択します。ただし、変更は自動的には同期されません。このオプションを選択すると、アイコンが🔔に変更されます。

   1d **リセット** : 属性値を他のチャネルで指定された値にリセットするには、このオプションを選択します。このオプションを選択すると、アイコンが⟳に変更されます。

   注 : この値は、発行者チャネルまたは購読者チャネルで設定できます。両方のチャネルでこの値を同時に設定することはできません。

図 26-1 データフローの管理

27 エンタイトルメント受信者の管理

エンタイトルメントの参照と結果は、エンタイトルメントが付与されたオブジェクト、またはエンタイトルメントから取り消されたオブジェクトに保持されます。エンタイトルメントの参照および結果には、エンタイトルメントが現在そのオブジェクトで付与または取り消されているかどうかを示す情報が含まれます。エンタイトルメント受信者は、エンタイトルメントへの参照を含むオブジェクトです。

エンタイトルメントの参照

エンタイトルメントの参照と結果を表示するには、Identity Console のメインページから［[エンタイトルメント受信者]］オプションをクリックし、［エンタイトルメントの参照］を選択します。次に、DirXML-EntitlementRecipient であるオブジェクトの完全識別名を入力します。オブジェクトセレクタボタンをクリックして、オブジェクトを選択することができます。

エンタイトルメントの結果

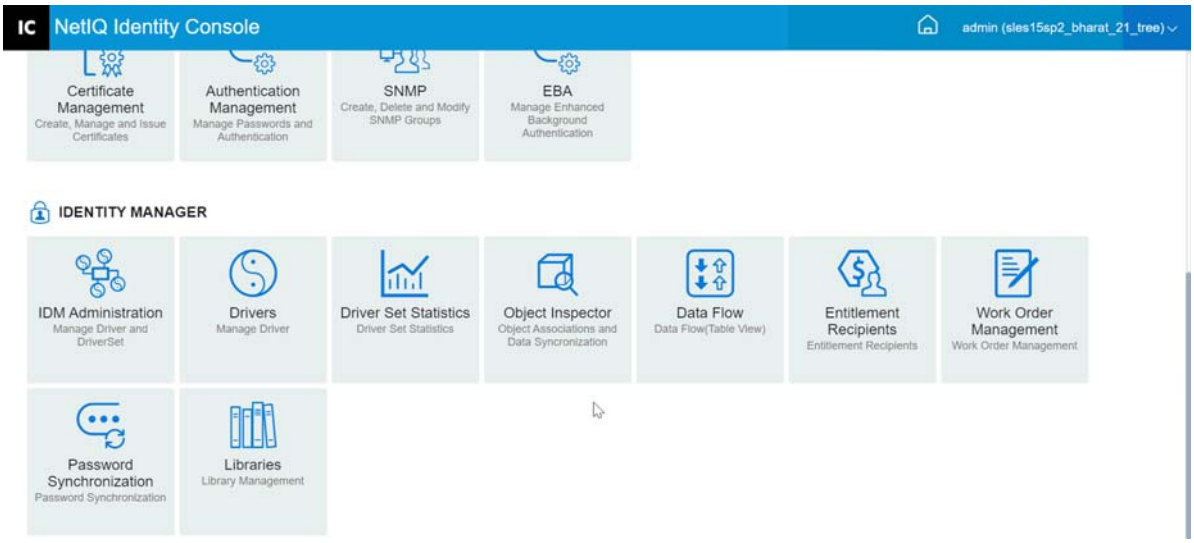
Identity Console のエンタイトルメント結果テーブルには、選択したオブジェクトに関連付けられているエンタイトルメントの結果が一覧表示されます。関連付けられているエンタイトルメントを表示するには、［エンタイトルメント DN］を選択します。エンタイトルメントの結果を XML 形式で表示するには、対応する［結果 ID］を選択します。

- **エンタイトルメントの結果のカラムヘッダ** : カラムヘッダには、エンタイトルメントの完全識別名、付与または取り消されているエンタイトルメントの現在の状態、結果の元 (ソース)、結果のステータス、結果とともに表示されたメッセージ、結果のタイムスタンプ、および結果の ID が含まれます。
  - **エンタイトルメント DN**: オブジェクトのエンタイトルメントの完全識別名をクリックして、［オブジェクトの変更］ページを表示します。このページで、eDirectory 属性がどのようにオブジェクトに割り当てられているかを確認できます。このページで、オブジェクトの属性を変更することもできます。［オブジェクトの変更］ページに表示されるカテゴリの数は、選択したオブジェクトによって異なります。
  - **状態** : エンタイトルメントが付与されたか、取り消されたかが表示されます。プラグインによって XML ストリーム内の他の値が検出された場合、その値が直接表示されます。
  - **メッセージ** : 結果ステータスに関連付けられた DirXML シムのメッセージです。XML 結果ファイルの <msg></msg> 部分に格納されている情報です。［結果 ID］エントリをクリックして、［XML ビューア］ページで結果の詳細を確認します。

- **タイムスタンプ** : エンタイトルメントエンジンが処理を実行し、結果を書き込んだ時刻です。［結果 ID］エントリをクリックして、［XML ビューア］ページで結果の詳細を確認します。
- **結果 ID**: ［結果 ID］エントリをクリックして、［XML ビューア］ページで結果の詳細を表示します。結果の確認が終わったら、［閉じる］をクリックします。

エンタイトルメント結果エントリを削除するには、エンタイトルメント結果エントリの左側にあるチェックボックスをオンにして、［ **[削除]**］をクリックします。

図 27-1 *エンタイトルメント受信者の管理*



28 ワークオーダーの管理

Identity Manager ドライバは、ドライバによって処理されるイベントの結果としてワークオーダーを作成できます。たとえば、人事ドライバ (SAP HR、PeopleSoft など) を使用する場合、新しいユーザが追加されるたびに、ドライバでワークオーダーを生成することができます。

Identity Console を使用して、この特定の機能をサポートするさまざまなドライバ用に作成されたワークオーダーを作成および管理できます。

新しいワークオーダーの作成

新しいワークオーダーを作成するには、次の手順を実行します。

1. Identity Console のランディングページから、[[ワークオーダー]] オプションをクリックします。
2. 新しいワークオーダーを作成するには、＋アイコンをクリックします。
3. ワークオーダーの名前を指定して、[[OK]] をクリックします。

   この名前は、アイデンティティボールト内の WorkOrder オブジェクトの名前に使用されます。
4. 次のフィールドに入力します。

   ステータス : 新しいワークオーダーのステータスは「 [保留中]」または「 [保留]」になります。通常、ワークオーダーのステータスは「 [保留中]」です。[[保留]] を選択することで、ワークオーダーを停止できます。ワークオーダーが処理された後に、結果のワークオーダーステータスがこのフィールドに表示されます。

   期日 : ワークオーダーをドライバでただちに処理するか、それともワークオーダーをスケジュールするかを選択できます。期日をスケジュールするには、カレンダアイコンをクリックします。カレンダを使用して日付を選択します。矢印を使用して、月、年、および時刻を選択します。

   ワークオーダーの繰り返し : ワークオーダーを複数回処理する場合は、このオプションを選択します。ワークオーダーを繰り返す前に、週、日、時間、または分の数を選択して時間間隔を指定します。ワークオーダーは手動で削除、編集しない限り、削除日になると繰り返しを止めます。それ以外はドライバからエラーメッセージが返されます。

削除日：カレンダコントロールを使用して、設定済みのワークオーダーを削除する日付を選択します。エラーステータスが付いているワークオーダーは、[**[ワークオーダーにエラーがある場合でも、ワークオーダーを削除します]**] を選択しない限り、削除されません。

従属ワークオーダー：新しいワークオーダーを作成できる場合、1 つまたは複数のワークオーダーに従属させることができます。  をクリックして、従属ワークオーダーをブラウズして選択します。ワークオーダーをリストから削除するには、ワークオーダーを選択して、  をクリックします。

[タイプ]：このフィールドを使用して、ワークオーダータイプを指定します。ドライバはこの属性を変更しません。この属性は、ワークオーダーの処理時に WorkToDo オブジェクトに渡されます。

ワークオーダー番号：ワークオーダーの固有の番号です。この値は、ワークオーダーデータベースなどの NetIQ eDirectory 以外の企業ワークオーダーシステムによって割り当てることができます。

連絡先情報：ワークオーダーの責任者の連絡先情報です。

ワークオーダーの処理ログ：ワークオーダーが処理された後、ドライバによってこのフィールド内のステータスを含む、ワークオーダーの結果がログされます。これにより、ワークオーダーの現在のステータスを確認し、ワークオーダーの設定を試みた際にドライバが遭遇した問題を特定できます。

ワークオーダーステータス属性は、ワークオーダーが処理されるまで「保留中」のままです。ワークオーダーは、締切日を過ぎた時に処理されます。ドライバは、ステータス属性を「設定済み」、「警告」、または「エラー」に設定することで処理結果を報告します。ワークオーダーが「保留」の場合、ドライバはそのワークオーダーを無視します。

- **保留中**：ドライバは期日になってから、ワークオーダーを完了させます。
- **設定済み**：ワークオーダーは正常に処理されています。
- **エラー**：ドライバがワークオーダーを実行できませんでした。
- **警告**：ワークオーダーに関する警告があります。たとえば、ワークオーダーに期日が遅い従属ワークオーダーがある場合、ドライバにより「警告」が送信されます。

説明：ワークオーダーの説明です。

ワークオーダーの内容：このフィールドのデータは、ワークオーダーを処理するためにドライバのルールによって使用されます。たとえば、ワークオーダーを処理するために XML コマンド変換によって使用されることがあります。

既存のワークオーダーの削除

既存のワークオーダーを削除するには、次の手順を実行します。

1. Identity Console のランディングページから、[**[ワークオーダー]**] オプションをクリックします。
2. 削除するワークオーダーを選択します。
3.  アイコンをクリックします。

ワークオーダーリストのフィルタリング

ワークオーダーのリストをフィルタするには、次の手順を実行します。

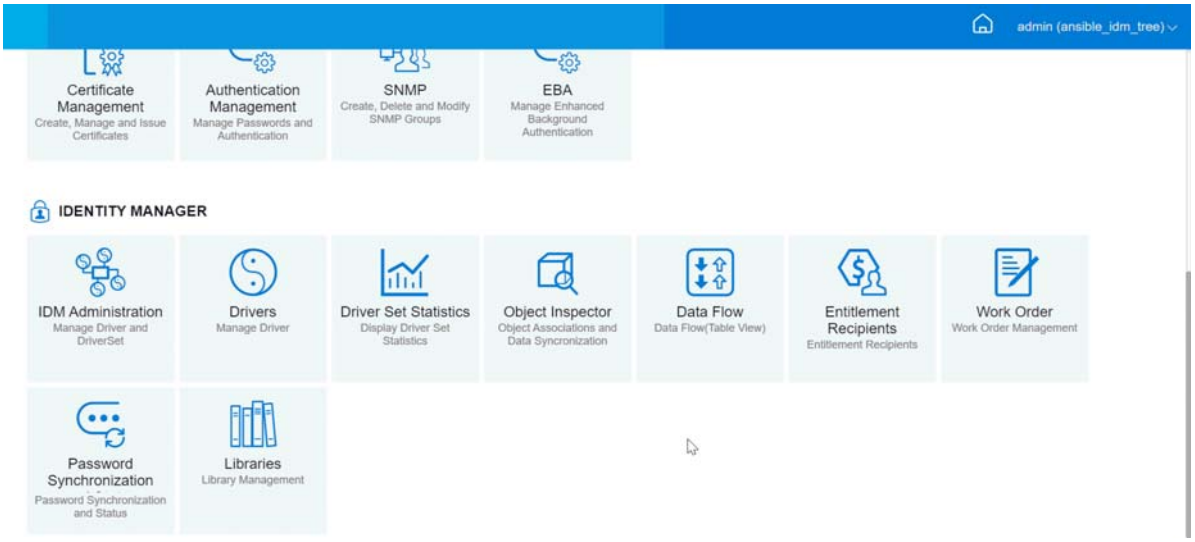
1 Identity Console のランディングページから、[**[ワークオーダー]**]オプションをクリックします。

2 [ワークオーダー管理]の下の [**[アクション]**] をクリックします。

3 ドロップダウンメニューから、フィルタタイプを選択します。

- **すべてを表示** : ドライバに関連付けられているすべてのワークオーダーが一覧表示されます。
- **設定済み** : ドライバに関連付けられている設定済みのワークオーダーのみが一覧表示されます。
- **エラー** : エラーステータスが付いているワークオーダーのみが表示されます。
- **保留** : 手動で保留にされたワークオーダーが一覧表示されます。
- **保留中** : まだ期限が切れていないワークオーダーが一覧表示されます。

図 28-1 ワークオーダーの管理



29 パスワードステータスと同期の管理

Identity Console ポータルを使用して、個々のドライバのパスワード同期とパスワードステータスを確認できます。確認するには、Identity Console のメインページから［[パスワード同期]］モジュールを選択します。

このモジュールを使用して、次のアクションを実行できます。

- 203 ページの 「パスワード同期ステータスの確認」
- 204 ページの 「パスワード同期の設定の確認」

パスワード同期ステータスの確認

特定のユーザの配布パスワードが接続システムのパスワードと同じかどうかを判断できます。パスワード同期ステータスを確認するには、次の手順を実行します。

1. Identity Console で、［[パスワード同期]］>［[パスワードステータス]］を選択します。
2. パスワードステータスを確認するユーザをブラウズして選択します。
3. 次のパスワードステータスが表示されます。
   - パスワードが同期されます。
   - パスワードは同期されません。
   - 接続システムへ問い合わせてパスワード確認を要求することができないため、パスワードステータスが不明になっています。
   - エラーが発生しました。

注 : これらの各ステータスの詳細を表示するには、[[パスワードステータス]] 列の下のステータスをマウスオーバーする必要があります。

［Password Status］タスクにより、ドライバで［Check Object Password］アクションが実行されます。すべてのドライバでパスワードチェックがサポートされているわけではありません。パスワードチェックがサポートされているドライバには、ドライバのマニフェストにパスワードチェック機能が含まれている必要があります。Identity Console では、マニフェストにこの機能が含まれていないドライバにパスワードチェック操作を送信することはできません。

［オブジェクトパスワードの確認］アクションは、配布パスワードを確認します。配布パスワードがアップデートされていない場合、［オブジェクトパスワードの確認］によって、パスワードが同期化されていないとレポートされることがあります。

次のいずれかが発生した場合、配布パスワードは更新されません。

- NDS パスワードを使用した同期を使用しているか、ユニバーサルパスワードを使用した同期を使用している場合。詳細については、120 ページの 「カスタム設定値を使用したパスワードポリシーの作成」を参照してください。

注 : [パスワードステータス] アクションは、アイデンティティボールトのユニバーサルパスワードの代わりに NDS パスワードを確認します。したがって、ユーザのパスワードポリシーで NDS パスワードをユニバーサルパスワードに同期するよう指定されていない場合は、必ず、パスワードが同期されていないとレポートされます。配布パスワードおよび接続システムのパスワードは同期化されないことがありますが、NDS パスワードおよび配布パスワードの両方がユニバーサルパスワードに同期化されない限り、[Check Password Status（パスワードステータスの確認）] は正確とは限りません。

パスワード同期の設定の確認

パスワード同期では、Identity Manager を使用して接続システム間でパスワードを同期できます。接続システムのパスワード同期設定を表示するには、ドロップダウンから適切なドライバセットを選択します。

パスワード同期を使用することで、次のことを行えるように接続システムを設定できます。

- Identity Manager にパスワードを発行する。
- Identity Manager または他の接続システムからパスワードを購読する。
- 接続システムでパスワードポリシーを強制する。
- 電子メール通知を送信すること。

パスワード同期設定を確認するには、次の手順を実行します。

1. Identity Console で、メインページから [**[パスワード同期]**] > [**[パスワード同期]**] を選択します。
2. 設定を確認するドライバを含むドライバセットを選択します。
3. リストからドライバの名前をクリックします。

   注 : 有効または無効になっている設定は、ドライバによって異なります。ドライバでサポートされている機能の設定のみを使用できます。

4. 設定が正しく設定されていることを確認します。

   パスワードを受理する Identity Manager (発行者チャネル): このオプションを有効にすると、Identity Manager によって、接続システムからアイデンティティボールトへパスワードを送信することができます。このオプションを無効にすると、<password> 要素は Identity Manager に送信されません。発行者チャネルのパスワード同期ポリシーによって、XML から取り除かれます。

   この設定は、接続システム自身によって提供されるユーザパスワード、および発行者チャネルのポリシーを使用して作成されるパスワード値に適用されます。

   このオプションが有効になっているが、その下の [配布パスワード] オプションが無効になっている場合、接続システムから取得した <password> 値は、アイデンティティボールト内のユニバーサルパスワードに直接書き込まれます。ユーザのパスワードポリシーによってユニバーサルパスワードが有効にされていない場合、パスワードは NDS パスワードに書き込まれます。

パスワード同期に配布パスワードを使用する: この設定は、[パスワードを受理する Identity Manager (発行者チャネル)] 設定が有効になっている場合にのみ使用できます。

このオプションを有効にすると、接続システムから受信したパスワード値は、配布パスワードに書き込まれます。配布パスワードは逆方向の同期が可能です。つまり、アイデンティティボールトのデータストアから取得してパスワードを同期することができます。この動作は、接続システムと双方向のパスワード同期を行うために Identity Manager によって使用されます。Identity Manager がこのシステムから他のシステムにパスワードを配布する場合、このオプションを有効にする必要があります。

ユーザのパスワードポリシーに従っている場合のみパスワードを受理します: この設定は、[[パスワード同期に配布パスワードを使用する]] 設定が有効になっている場合にのみ使用できます。

このオプションを選択すると、パスワードがユーザのパスワードポリシーに従ってない場合は、Identity Manager はそのパスワードを、この接続システムからアイデンティティボールトの配布パスワードに書き込まないか、接続システムに発行しません。

パスワードがポリシーに準拠していない場合は、[[Reset the user's password to the Distribution Password（ユーザのパスワードを配布パスワードにリセットする）]] 設定を有効にして、接続システム上のユーザのパスワードをリセットします。これにより、接続システムだけでなく、アイデンティティボールトでもパスワードポリシーを強制できます。このオプションを選択しない場合、接続システムでユーザパスワードが非同期になる可能性があります。ただし、このオプションを使用するかどうかを決定する際には、接続システムのパスワードポリシーを考慮する必要があります。接続システムの中には、パスワードを繰り返し使用できないようにするため、パスワードのリセットを許可していないものがあります。

[[パスワード同期の失敗を電子メールでユーザに通知する]] 設定を使用すると、パスワードの設定またはリセットに失敗した場合にユーザに通知できます。通知機能は、このオプションでは特に役立ちます。ユーザが、接続システムによって許可されているパスワードに変更しても、パスワードポリシーが原因でアイデンティティボールトによって拒否される場合、そのユーザは、通知を受信するか、または古いパスワードで接続システムにログインを試みるまでは、パスワードがリセットされていることに気づきません。

常にパスワードを受理します。パスワードポリシーを無視します: この設定は、[[パスワード同期に配布パスワードを使用する]] 設定が有効になっている場合にのみ使用できます。

このオプションを選択すると、Identity Manager は、この接続システムにユーザのパスワードポリシーを強制適用しません。Identity Manager は、この接続システムからアイデンティティボールト内の配布パスワードにパスワードを書き込み、パスワードポリシーのコンプライアンスに関係なく他の接続システムに配布します。

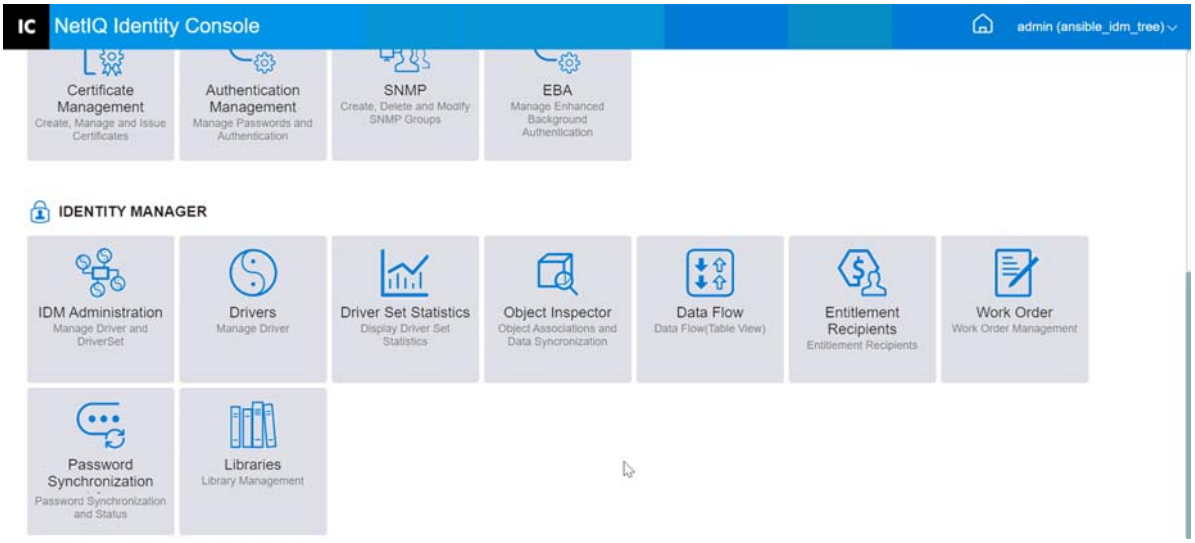
パスワードを受け入れるアプリケーション (購読者チャネル): このオプションを有効にすると、ドライバは、アイデンティティボールトからこの接続システムにパスワードを送信します。つまり、ユーザが、パスワードを発行している別の接続システムのパスワードを、アイデンティティボールトの配布パスワードに変更した場合は、そのパスワードはこの接続システムでも変更されます。

デフォルトでは、配布パスワードはアイデンティティボールト内のユニバーサルパスワードと同じです。そのため、アイデンティティボールトでユニバーサルパスワードを変更すると、その内容は接続システムにも送信されます。

電子メール経由でユーザにパスワード同期障害を通知する：このオプションを有効にすると、パスワードが同期、設定、またはリセットできない場合に、ユーザに電子メールが送信されます。ユーザに送信される電子メールは、電子メールテンプレートに基づいています。このテンプレートは、パスワード同期アプリケーションによって提供されます。ただし、テンプレートを動作させる場合は、これをカスタマイズして、通知メッセージを送信する電子メールサーバを指定する必要があります。手順については、「*NetIQ Identity Manager パスワード管理ガイド*」の Configuring E-Mail Notification（電子メール通知の設定）を参照してください。

5 完了したら、[**[保存]**] をクリックして、変更を保存します。設定はグローバル構成値として保存されます。

図 29-1 *パスワード同期の管理*



30 ライブラリの管理

ライブラリオブジェクトは、複数のポリシーおよび 1 つまたは複数のドライバによって共有されているその他のリソースを保存します。ライブラリオブジェクトは、ドライバセットオブジェクトまたは任意の eDirectory コンテナ内で作成できます。eDirectory ツリーには複数のライブラリが存在できます。ドライバは、そのドライバが動作しているサーバがライブラリオブジェクトの読み書き可能レプリカまたはマスタレプリカを保持している限り、ツリー内のどのライブラリでも参照できます。

ライブラリにスタイルシート、ポリシー、ルール、その他のリソースオブジェクトを保存して、これを 1 つ以上のドライバに参照させることができます。

ライブラリ管理モジュールを使用して、次のタスクを実行できます。

- 207 ページの 「既存のライブラリの表示と削除」
- 207 ページの 「ライブラリからのオブジェクトの表示と削除」

既存のライブラリの表示と削除

既存のライブラリを表示および削除するには、次の手順を実行します。

1. Identity Console で、ホームページから［[ライブラリ]］モジュールを選択します。
2. 適切なライブラリをリストから選択します。
3. アイコンをクリックします。[OK] をクリックして、確認します。

ライブラリからのオブジェクトの表示と削除

ライブラリオブジェクトからポリシーおよびマッピングテーブルを表示および削除できます。オブジェクトを削除するには、次の手順を実行します。

1. Identity Console で、ホームページから［[ライブラリ]］モジュールを選択します。
2. リストから適切なライブラリをクリックします。
3. ポリシーを削除するには、［[ポリシー]］タブを選択します。
4. リストから適切なポリシーを選択して、アイコンをクリックします。
5. マッピングテーブルを削除するには、［[マッピングテーブル]］タブを選択します。
6. リストから適切なマッピングテーブルを選択して、アイコンをクリックします。
7. [OK] をクリックして、確認します。

図30-1 ライブラリの管理

31 電子メールサーバオプションの管理

[電子メールサーバオプション] を使用して、SMTP(シンプルメール転送プロトコル) 電子メールサーバの設定を指定できます。

ホスト名

SMTP 電子メールサーバのホスト名です。IP アドレスを指定することもできます。カスタムポートを指定し、その後にホスト名または IP アドレスを指定することもできます。

重要 : ホスト名または IP アドレスとポート間の区切り文字としてコロン (:) を使用します。

送信者

電子メールヘッダの [送信者] フィールドとして表示される有効な電子メールアドレスを指定できます。

タイムアウト値

タイムアウトオプションを使用すると、通知電子メールを送信する時間制限 (秒) を設定できます。

SSL を有効にする

必要に応じて、SSL オプションを有効にすることもできます。

アカウント情報を使用してサーバで認証

セキュリティ保護された SMTP サーバで使用されます。電子メールを送信する前にサーバで認証が必要な場合、ここにユーザ名とパスワードを指定します。

認証情報をここに指定した場合でも、さらに、通知メールを送信するアプリケーションに対しても別途認証情報を指定しなければならない場合もあります。

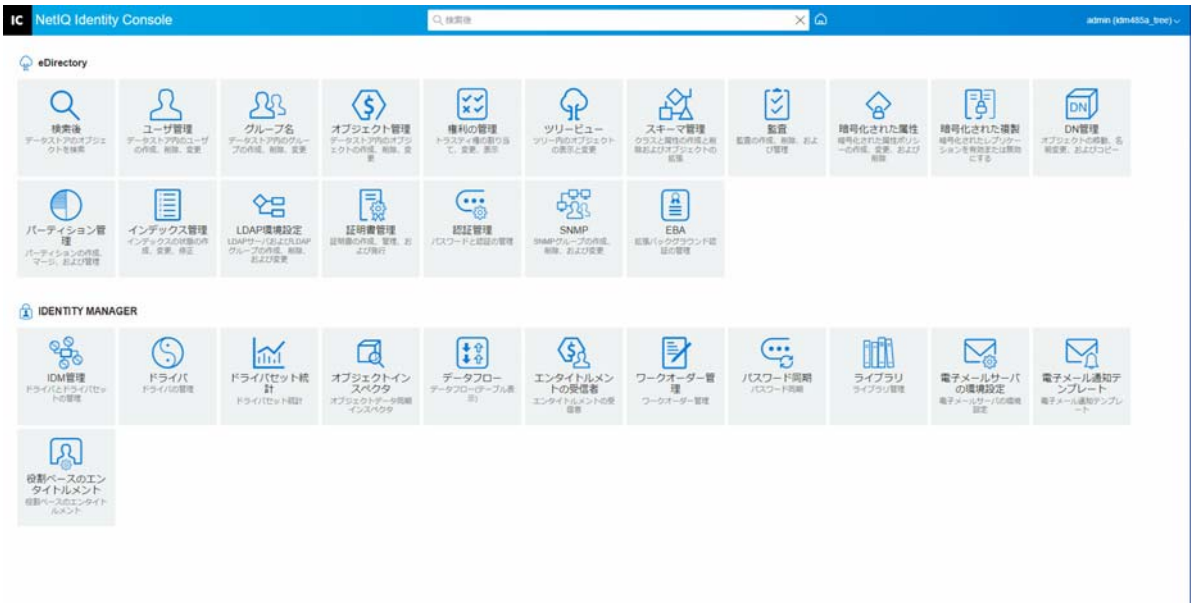
たとえば、「パスワードを忘れた場合」通知メールを送信する際に、ここで指定する認証情報を使用できますが、Identity Manager のパスワード同期は、通知メールを送信するのにドライバポリシーを使用します。この場合、認証情報がそのドライバポリシーにも含まれていることが必要になります。

サーバを認証するには、次の手順を実行します。

1. [**資格情報を使用してサーバに認証する**] オプションを選択します。
2. **ユーザー名**と**パスワード**を指定します。
3. [**[サーバ接続のテスト]**] をクリックしてコネクティビティを確認します。
4. [**[保存]**] をクリックします。

注 : 資格情報の詳細を保存すると、[サーバ接続のテスト] が無効になります。

図 31-1 電子メールサーバ設定



32 電子メールテンプレートの管理

このリストには、使用可能な通知テンプレートが一覧表示されます。これらのテンプレートを使用して、このツリー内のユーザに対して電子メールメッセージを送信できます。テンプレートをカスタマイズして独自のテキストを使用できます。

アプリケーションに独自のテンプレートが用意されている場合もあります。テンプレートオブジェクトは、通常はツリーのルートにあるセキュリティコンテナにあります。

名前、日付、または件名でリストをソースできます。

件名

電子メールのサブジェクト見出しとして表示されるテキストです。テンプレートを編集するには、そのテンプレートのサブジェクト見出しをクリックします。[電子メール通知テンプレートの編集] インタフェースを使用すると、テンプレートとその詳細を変更できます。

テンプレート名

各テンプレートには固有の名前がついています。電子メールを送信するアプリケーションは、この名前を参照します。

最終更新日時

テンプレートが最後に変更された日時。

新規

新しい電子メールテンプレートを作成できます。

1. ＋アイコンをクリックします。
2. 新しいテンプレートの名前 (たとえば「承認」) を指定し、[[OK]］をクリックします。

ポップアップを無効にしている場合は、［電子メール通知テンプレートの編集］ページに戻ります。新しいテンプレート名が［名前］列に表示されますが、［サブジェクト］列には、［No Subject(サブジェクトなし)］と表示されます。この場合、［No Subject(サブジェクトなし)］をクリックすると、新しいテンプレートに詳細を入力できます。

電子メール通知テンプレートの編集

[電子メール通知テンプレートの編集] ページでは、電子メールテンプレートを変更できます。テンプレートを独自のテキストでカスタマイズできます。

テンプレート名

テンプレートの名前を表示します。

件名

電子メールのサブジェクト見出しとして表示されるテキストです。件名行のテキストを変更することができます。テンプレートの実際の名前は変更されません。

別名送信

SMTP サーバが使用する電子メール送信形式 : テキストまたは HTML。

トークンまたは置換タグ

置換タグを使って、メッセージをユーザ用にパーソナライズできます。置換タグは、使用可能なタグリストからコピーして、メッセージに貼り付けることができます。

各テンプレートにはデフォルトのトークンまたは置換タグが組み込まれています。これらは、電子メールをユーザ用にパーソナライズするために必要な変数です。たとえば、ユーザにパスワードを送信するための「Forgot Password (パスワードを忘れた場合)」電子メールテンプレートには、「CurrentPassword」というトークンまたは置換タグがデフォルトで含まれています。

追加 : メッセージ本文内で使用する他のトークンまたは置換タグを定義することもできます。

トークンまたは置換タグを追加するには、次の手順を実行します。

1.  アイコンをクリックします。
2. [**[置換タグの追加]**] ウィンドウで **[名前]** と **[説明]** を指定します。
3. **[OK]** をクリックします。
4. 新しいトークンまたは置換タグのリストが [置換タグ] 列に表示されます。

タグのコピー : 選択したタグをシステムバッファにコピーするために  をクリックします。次に、マウスをクリックして貼り付け、メッセージの件名行または本文で利用できます。

削除 : リストからトークンまたは置換タグを選択し、  をクリックしてリストからタグを削除します。メッセージの本文に必要なタグは削除しないようにしてください。

メッセージ本文

電子メールメッセージのテキスト。

電子メール通知テンプレートのすべての変更を指定した後、[**[更新]**] をクリックします。

削除

作成したテンプレートをアイデンティティボールトから削除します。Identity Manager などのアプリケーションに同梱されているデフォルトテンプレートは削除できません。

1. 削除するテンプレートを選択します。

   テンプレートのサブジェクト見出しをクリックすると、Identity Console に［Edit Email Templates(電子メールテンプレートの編集)］ダイアログボックスが表示されます。

2. ［削除］アイコンをクリックします。
3. [[OK]] をクリックします。

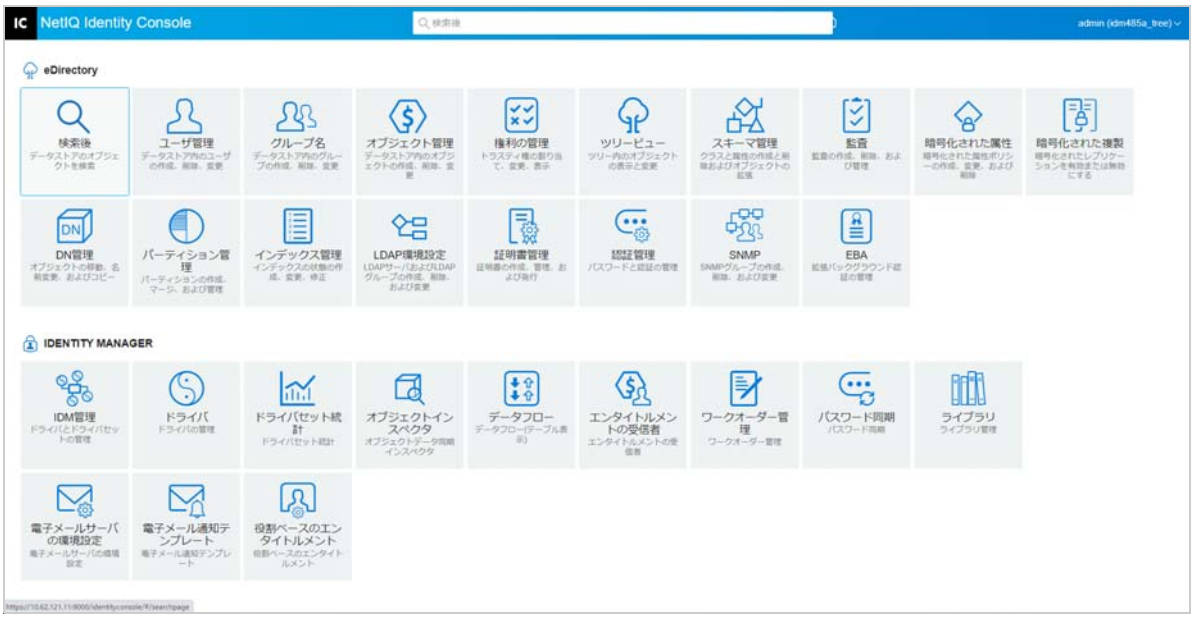
テンプレートをフィルタする

表示する電子メールテンプレートをフィルタできます。選択したテンプレートだけが表示されます。Filter by all(すべてのフィルタ条件) オプションを選択すると、すべてのテンプレートが表示されます。

テンプレートの更新

適用されたフィルタテンプレートを更新および削除するには、この  アイコンをクリックします。

図 32-1 *電子メール通知テンプレート*



33 役割ベースエンタイトルメントの管理

RBE では、接続システムのエンタイトルメントを NetIQ® Identity Console ユーザのグループに付与できます。RBE ポリシーにより、ビジネスポリシーの管理を合理化できるため、Identity Manager ドライバを設定する必要性が軽減されます。

役割ベースエンタイトルメントモジュールには次の機能があります。

- 215 ページの 「役割ベースエンタイトルメント」
- 224 ページの 「メンバーシップの再評価」

役割ベースエンタイトルメント

RBE ポリシーは、接続システムの RBE を付与するために追加される、付加機能を備えた Identity Console のダイナミックグループオブジェクトです。RBE ポリシーを作成するときは、そのポリシーのメンバーシップおよびその RBE ポリシーのメンバーに付与するエンタイトルメントを定義します。各 RBE ポリシーは、特定のサーバに割り当てられている 1 つのドライバセットオブジェクトに関連付けられます。Identity Manager ドライバと同様、各エンタイトルメントポリシーが管理できるのは、割り当てられたサーバ上のマスタレプリカまたは読み書き可能レプリカに存在するオブジェクトだけです。

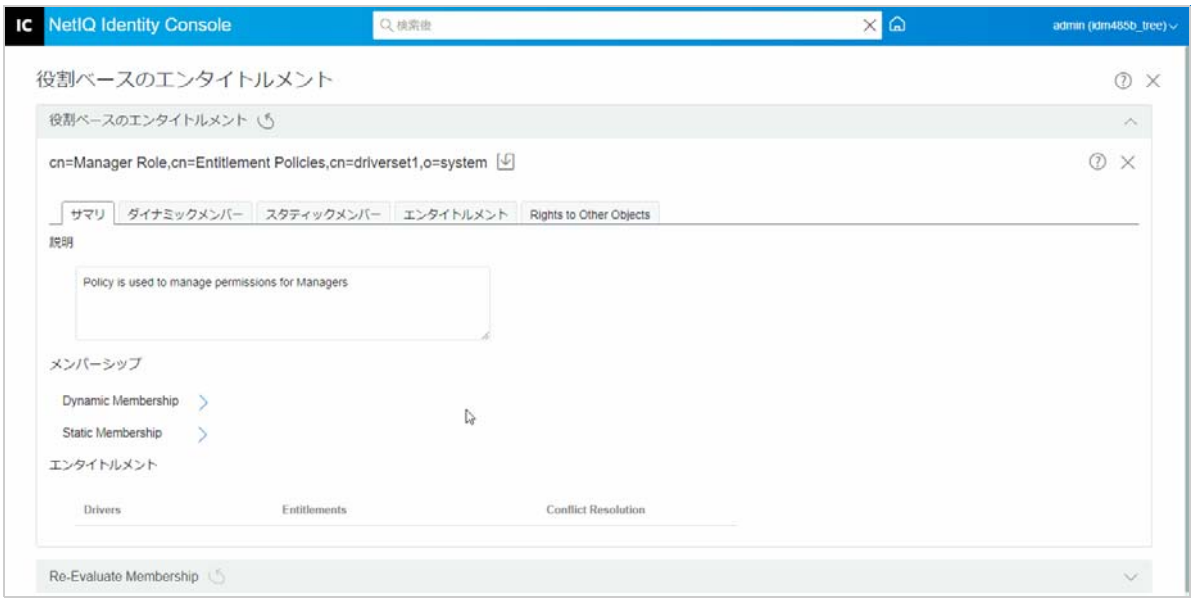
次のセクションでは、役割ベースエンタイトルメントについて詳しく説明します。

- 215 ページの 「概要」
- 218 ページの 「ダイナミックメンバー」
- 220 ページの 「スタティックメンバー」
- 220 ページの 「エンタイトルメント」
- 221 ページの 「Rights to other Objects(他のオブジェクトへの権利)」
- 223 ページの 「RBE ポリシーの優先順位付け」

概要

このページには、エンタイトルメントポリシーのメンバーシップ基準とエンタイトルメントの概要がまとめられています。

図 33-1 概要ページ



メンバーシップ :

ダイナミックメンバーシップに指定された条件が、LDAP フィルタの構文で表示されます。［識別情報の検索］では、ダイナミックメンバーシップのクエリを実行するときに使用されるオブジェクト権利が示されます。［ベース DN］と［スコープ］では、クエリにツリーのどの部分を含めるかが示されます。

チェックボックスを選択して、スタティックメンバーシップに含まれるものと、メンバーシップから除外されるものを確認できます。

すべてのメンバーを結合したリストは、長くなるので［概要］ページには表示されません。エンタイトルメントポリシー、ダイナミックとスタティックのすべてのメンバーを結合したリストを表示するには、［メンバーシップ］［メンバーシップの表示］タブの順に選択します。

エンタイトルメント :

エンタイトルメントポリシーのメンバーに付与された接続システムのエンタイトルメントです。役割ベースエンタイトルメントと接続システムとの一貫性は、緩やかに保たれていることに注意してください。つまり、接続システム上のエンタイトルメントのステータスは、エンタイトルメントポリシーのインタフェースには表示されないということです。エンタイトルメントポリシーにエンタイトルメントを付与すると、そのエンタイトルメントは接続システムでは利用できなくなりますが、リストから手動で削除するまではエンタイトルメントポリシー内にリストされたままになります。

衝突の解決 :

これらの方法は、値を持つ RBE の場合、2 つ以上の RBE ポリシーによって異なる値がユーザに付与されているときに、どの値をユーザに付与するかを決定するのに使用されます。値を持つエンタイトルメントの例としては、電子メール配布リストのメンバーシップがあります。この場合の値は、配布リストの名前になります。

衝突の解決方法は、各ドライバオブジェクトの個々のエンタイトルメントごとに設定されます。1 つのエンタイトルメントが複数の RBE ポリシーで使用される場合、衝突の解決方法は、すべての RBE ポリシーで同じになります。エンタイトルメントの衝突解決方法を変更するには、ドライバのドライバマニフェストで、そのエンタイトルメントの設定を変更します。

- **未認識** : RBE ポリシーがウィザードで完了していないか、またはドライバマニフェストに設定が正しく入力されていません。
- **マージ** : デフォルト設定は［マージ］(ドライバマニフェストでの「結合」) です)。このエンタイトルメントのすべての値を、ユーザがメンバーである RBE ポリシーから付与します。

  ［マージ］のデフォルト設定を使用している場合、この特別なエンタイトルメントにとってポリシーの優先順位は重要ではありません。

  たとえば、あるユーザに、Managers ポリシーと Team Members ポリシーという 2 つの RBE ポリシーによって、GroupWise® ドライバ A の電子メール配布リストのメンバーシップが付与されているとします。ポリシー 1 では、ユーザは Manager s 電子メール配布リストのメンバーシップを付与されており、ポリシー 2 では、Team Members 電子メール配布リストのメンバーシップを付与されています。［マージ］の設定により、このユーザは両方の電子メール配布リストでメンバーシップが付与されます。
- **優先度** : この設定は、同じドライバオブジェクトからの同じエンタイトルメントに対し、複数の RBE ポリシーがユーザに異なる値を付与している場合、そのユーザにはリストの最上位の RBE ポリシーで指定された値のみが付与されます。

  ［優先度］デフォルト設定を使用している場合、この特別なエンタイトルメントにとってポリシーのリストの優先順位は重要ではありません。

  たとえば、あるユーザに、Managers ポリシーと Team Members ポリシーという 2 つの RBE ポリシーによって、GroupWise ドライバ A の電子メール配布リストのメンバーシップが付与されているとします。Manager s ポリシーでは、ユーザは Manager s 電子メール配布リストのメンバーシップを付与されており、Team Members ポリシーでは、Team Members 電子メール配布リストのメンバーシップを付与されています。Manager s ポリシーは、ポリシーのリストでは Team Members ポリシーよりも上位にリストされています。［優先度］の設定により、このユーザは Manager s 電子メール配布リストのメンバーシップのみが付与されます。

  衝突の解決に優先度を使用すると、接続システムの属性で 1 つの値しか指定できない場合に便利です。異なる RBE ポリシーによって同じユーザへの属性値が付与されている場合、ユーザはリスト内の最上位の RBE ポリシーで付与されている値を受け取ります。

注 : 衝突の解決設定は、アカウントなどの値を持たないエンタイトルメントには使用できません。値を持たないエンタイトルメントは、リスト内のポリシーの優先度に関係なく、常に RBE ポリシーのメンバーに対して付与されます。

ダイナミックメンバー

ダイナミックメンバーシップに指定された条件が、LDAP フィルタの構文で表示されます。［識別情報の検索］では、ダイナミックメンバーシップのクエリを実行するときに使用されるオブジェクト権利が示されます。［ベース DN］と［スコープ］では、クエリにツリーのどの部分を含めるかが示されます。

メンバーシップフィルタ

ツリー内の場所やオブジェクトの属性などのメンバーシップの条件を定義できます。たとえば、メンバーシップは、ユーザが Active コンテナ内に存在するかどうか、または役職名にマネージャという言葉が含まれるかどうかによって異なります。条件に合致するユーザは自動的に RBE ポリシーのメンバーになります。各ユーザを個別にポリシーに追加する必要はありません。ダイナミックメンバーシップは、ダイナミックグループオブジェクトと同様です。

オブジェクトが変更され、ダイナミックメンバーシップの条件に合致しなくなった場合には、エンタイトルメントは、次にユーザが再評価されるときに自動的に取り消されます。

検索パラメータの設定

エンタイトルメントポリシーを管理するユーザの場所を指定します。ユーザ (ベース DN) を保持するコンテナを選択し、そのコンテナから検索を実行する範囲 (検索スコープ) を指定します。指定したコンテナ内のユーザを管理するエンタイトルメントポリシーの場合、ユーザはサーバ上の読み書き可能レプリカまたはマスタレプリカに存在する必要があります。

検索スコープには、次のオプションがあります。

- このコンテナとそのサブコンテナ: ユーザがダイナミックメンバーシップの条件を満たしている場合、ツリーにおけるこのコンテナ内のユーザは、エンタイトルメントポリシーのメンバーになります。サブコンテナ内のユーザも、条件を満たしている場合はメンバーになります。
- このコンテナのみ : ユーザがダイナミックメンバーシップの条件を満たしている場合、このコンテナ内のユーザのみが、エンタイトルメントポリシーのメンバーになります。ユーザが条件を満たしている場合でも、このコンテナのサブコンテナ内のユーザはメンバーにはなりません。

フィルタ条件の定義

エンタイトルメントポリシーのメンバーであるユーザを特定する特性を指定します。

エンタイトルメントポリシーの［概要］ページに、指定したダイナミックメンバーシップの条件が LDAP フィルタの構文で表示されます。

デフォルトでは、ダイナミックメンバーシップは、エンタイトルメントポリシーのメンバーの検索スコープ内で、すべてのユーザクラスオブジェクト (およびそのユーザクラスから派生したクラスオブジェクト) を含めるために設定されます。

注 : ユーザから派生する新しいオブジェクトクラスを作成する場合、既存のエンタイトルメントポリシーは、そのエンタイトルメントポリシーに変更を加えるまでは、作成したクラスを認識しません。これにより、新しいユーザクラスにエンタイトルメントを無意識に付与してしまうことを避けられます。エンタイトルメントポリシーへ変更を行うと、そのポリシーのユーザから派生したクラスのリストが更新されます。

ダイナミックメンバーシップの作成

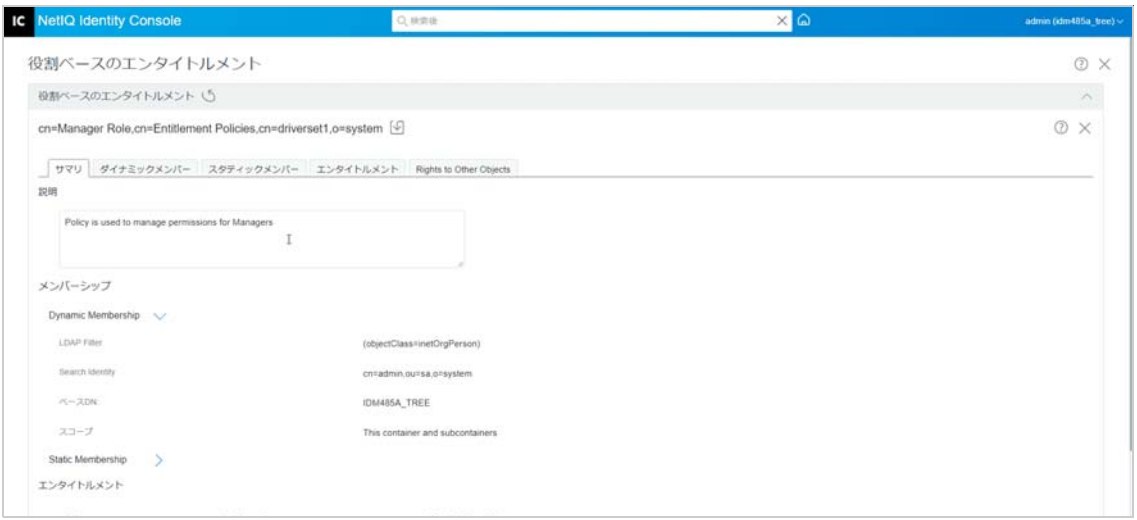
[ダイナミックメンバー] タブで、次の操作を実行します。

1 [[ダイナミックメンバー]] タブをクリックします。

2 要件に従って、[[検索識別情報]] フィルタ、[[検索開始範囲]] フィルタ、および [[検索スコープ]] フィルタを使用します。

3 特定の [[グループの作成]] をクリックして新しい条件または行を作成し、必要な検索条件または条件を指定します。

図 33-2 *ダイナミックメンバー*



検索スコープ : 検索スコープは、検索操作で一致する可能性がある検索ベース DN の、または検索ベース DN の下にあるエントリのセットを示します。

検索条件 : 検索を制限して、多数のレコードから特定のレコードまたはレコードのグループを検索できます。

ベース DN: ベース DN は、サーバがユーザを検索するポイントです。

LDAP グループ : ユーザ、グループ、および組織単位の階層構造であり、ユーザおよびグループのコンテナです。

注 : ユーザは、条件を持つ単一または複数のグループを作成できます。条件は、属性、演算子、および値で構成されます。デフォルトでは、[[オブジェクトクラス]] > [[は等しい]] > [[ユーザ]] は入力されています。

スタティックメンバー

スタティックメンバーは、スタティックキーワードを使用して宣言されるメンバーのクラスです。スタティックメンバーには、特定の制限付きアクセスがあります。

[スタティックメンバー] タブでは、次の操作を実行できます。

メンバーを含める :

ダイナミックメンバーシップフィルタに含まれていないメンバーをスタティックに追加します。

メンバーを除外する :

フィルタの条件に合致していても、エンタイトルメントポリシーに含めるべきではないメンバーを除外します。

エンタイトルメント

RBE(役割ベースエンタイトルメント) では、接続システムのエンタイトルメントと、Identity Manager の権利を付与できます。エンタイトルメントは、次のものを使用できます。

- 接続システムのアカウント。
- 接続システム上の電子メール配布リストのメンバーシップ。
- 接続システム上のグループメンバーシップ。
- 指定した値が入力されている、接続システムにおける対応オブジェクトの属性。

注 : エンタイトルメントの機能は Identity Manager の一部であるため、エンタイトルメントをサポートするために Identity Manager ドライバのインストールと設定を行ってから、接続システムのエンタイトルメントを付与する必要があります。

エンタイトルメントの作成

［エンタイトルメント］タブで、次の操作を実行します。

1 ［**[エンタイトルメント]**］タブをクリックします。

2 クリック＋して［**[ドライバを追加]**］し、接続システムにエンタイトルメントを付与します。

[**[ドライバの追加]**] 画面が表示されます。

3 ドロップダウンメニューからドライバを選択します。

4 ［**[追加]**］をクリックします。

［**[エンタイトルメントの追加]**］画面が表示されます。

5 ドロップダウンメニューから、［**[エンタイトルメントの選択]**］をクリックし、追加するグループを選択します。

6 [クエリタイプ] を選択します。

- **キャッシュ** : クエリが以前に実行されている場合。
- **外部クエリ** : クエリが新しい場合。

[グループエンタイトルメントの追加] 画面が表示されます。

7 ドロップダウンメニューからグループエンタイトルメントを選択し、[選択] をクリックします。

Rights to other Objects(他のオブジェクトへの権利)

このページは、エンタイトルメントポリシーのトラスティ権を eDirectory オブジェクトに割り当てるために使用します。エンタイトルメントポリシーの各メンバーは、オブジェクトのトラスティになります。

すべての属性への権利を割り当てるほかに、[プロパティの追加] をクリックして特定のプロパティへの権利を割り当てることができます。

[継承] チェックボックスでは、権利をツリーの下位に継承するかどうかを指定します。たとえば、コンテナオブジェクトに権利を割り当てる場合に、エンタイトルメントポリシーにこのオブジェクトおよび下位のサブコンテナへの同じ権利を持たせたい場合は、[継承] チェックボックスを選択します。

このページで変更を完了すると、eDirectory 内のオブジェクトに対する権利が、エンタイトルメントポリシーのメンバーに付与されます。反対に、次回、ユーザのダイナミックメンバーシップに使用される属性が変更されたとき、またはそのユーザが移動されたり名前変更されたりしたときには、接続システムのエンタイトルメントがエンタイトルメントポリシーの各メンバーに付与されます。(権利およびエンタイトルメントが取り消された場合も同様です) 更新を強制的に実行するには、[メンバーシップの再評価] を使用します。

Rights to other Objects(他のオブジェクトへの権利) の作成

権利を作成するには、次の手順を実行します。

1 [[Rights to other Objects(他のオブジェクトへの権利)]] タブをクリックします

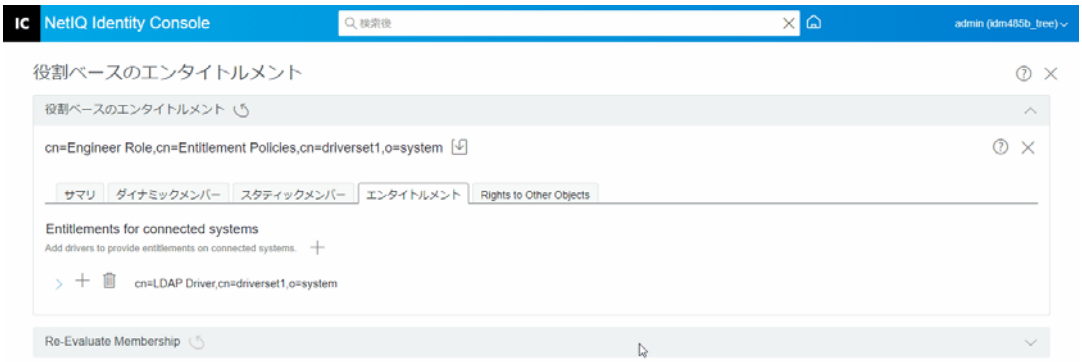
ここでは、新しいオブジェクトを追加し、このエンタイトルメントポリシーをトラスティにするオブジェクトを参照できます。

1a オブジェクトを追加するには、＋ボタンをクリックします。

[コンテキストブラウザ] ページが表示されます。このページはオブジェクトで構成されます。

1b オブジェクトを展開し、要件に従ってグループまたは個々のユーザを選択し、権利を割り当てます。

図 33-3 Rights to other Objects(他のオブジェクトへの権利)

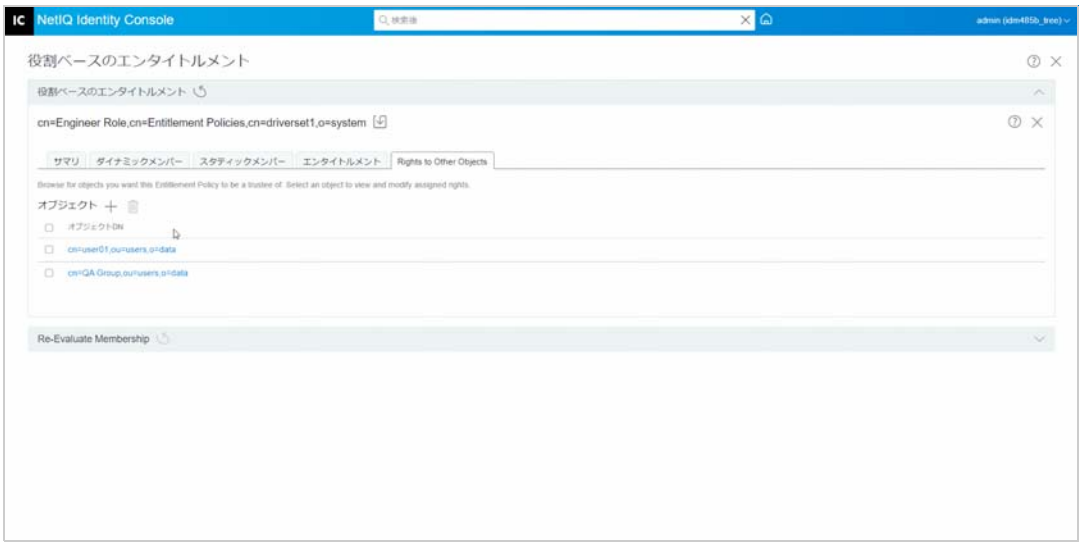


1c さらにプロパティを追加するには、[+] をクリックします。

[[プロパティの選択]] ページが表示されます。このページには、オブジェクトに設定できるプロパティのリストが表示されます。

1d [[完了]] をクリックします。

図 33-4 プロパティの選択



2 (オプション) RBE ポリシーに優先順位を付ける場合は、[[上]] と [[下]] 矢印を使用します。

ポリシーに優先順位を付けることは、複数のポリシー間のエンタイトルメントの競合を解決するためです。最上位のポリシーの優先度が最も高くなります。詳細については、223 ページの 「RBE ポリシーの優先順位付け」を参照してください。

RBE ポリシーの優先順位付け

RBE ポリシーを作成する場合、特定のユーザに影響を与えるポリシーが衝突する可能性があります。

リスト内の RBE ポリシーの順序は、優先度を示します。リスト内の順序を変更するには、上矢印や下矢印ボタンを使用します。

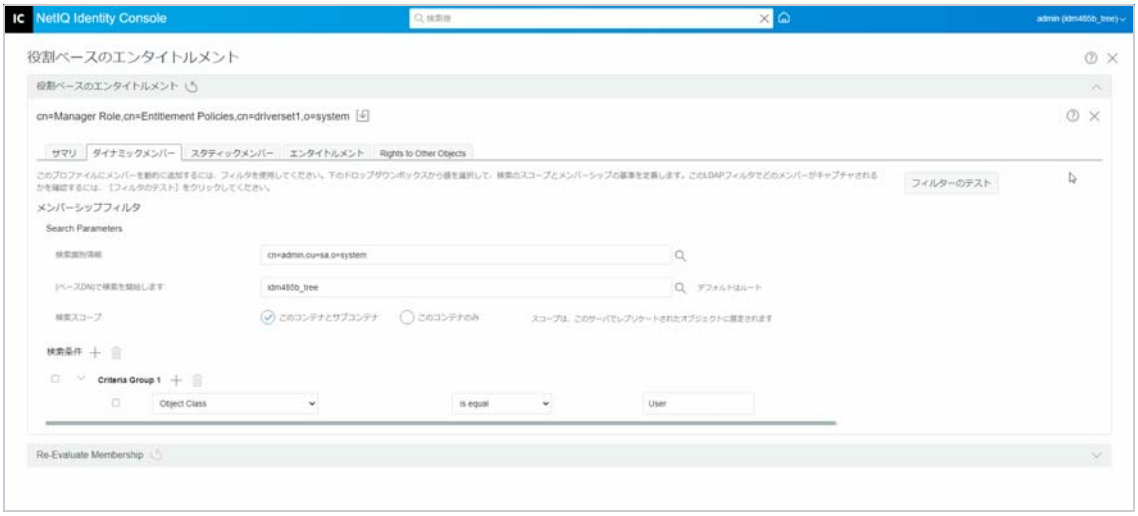
- この設定は、たとえば、接続システムの属性で 1 つの値しか指定できない場合に便利です。異なる RBE ポリシーによって同じユーザへの属性値が付与されている場合、ユーザはリスト内の最上位の RBE ポリシーで付与されている値を受け取ります。他の例では、エンタイトルメントを使用して別のシステムの階層構造にユーザを配置するよう環境を設定した場合などが考えられます。ユーザは任意の 1ヶ所に配置でき、同時に 2ヶ所に配置することはできません。
- 設定は、ドライバごとに提供される各エンタイトルメントとは関係ありません。
- ルールとして管理者またはマネージャのポリシーは、エンドユーザまたは各貢献者のポリシーより上位に配置する必要があります。広いメンバーシップを持つグループは、狭いメンバーシップを持つグループより上位に配置することをお勧めします。

RBE ポリシーに優先順位を付けるには、次の手順を実行します。

1 アップグレードまたはダウングレードするエンタイトルメントポリシーを選択します。

2 RBE ポリシーの優先順位を設定するには、[**[上]**] または [**[下]**] 矢印を使用します。

図 33-5 *ポリシーの優先順位付け*

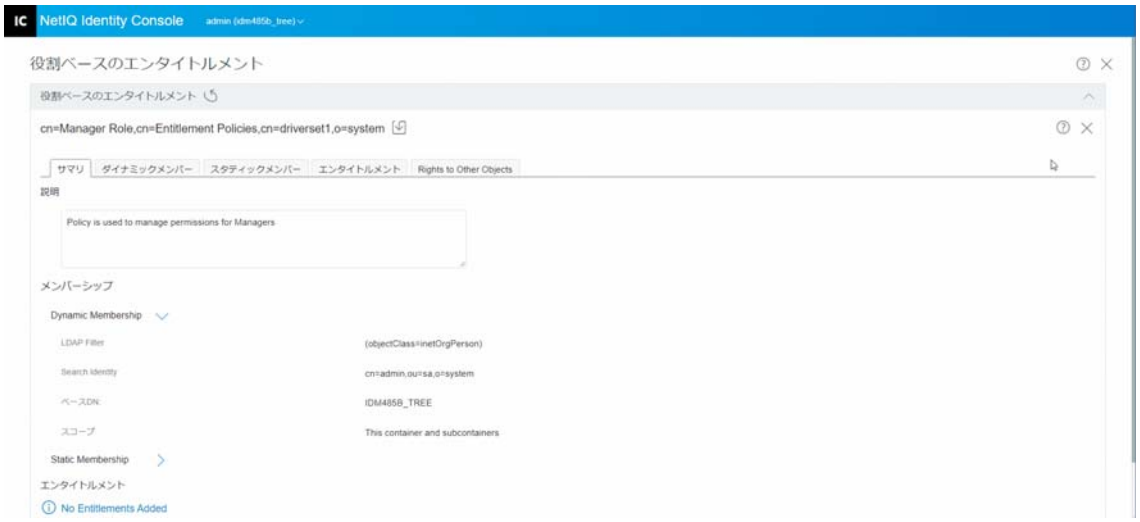


3 保存ボタンをクリックします。

ポリシーメンバーシップの詳細の概要が [**[概要]**] タブに表示されます。

4 ドライバを再起動します。

図33-6 [閉じる] と [再起動]



注 : 変更を有効にするには、ドライバを再起動する必要があります。

メンバーシップの再評価

[役割ベースエンタイトルメント] 機能により、接続システムのエンタイトルメントをユーザのグループに付与できます。

RBE ポリシーを作成または編集する場合、各ユーザのメンバーシップを再評価して、接続システムのエンタイトルメントを付与、変更または取り消すかどうかを決定する必要があります。デフォルトでは、再評価は、メンバーシップに影響を与える属性が各ユーザごとに変更されるか、またはユーザが移動されるか名前変更された場合に、一人ずつ行われます。こうしたデフォルトの動作によってシステムリソースは最小限に抑えられますが、RBE ポリシーが変更された時刻と、特定ユーザにエンタイトルメントが付与、変更または取り消される時刻との間に大きな遅延が発生するおそれがあります。

[225 ページの 「RBE ポリシーの再評価」] タスクを使用して、ただちに再評価を実行するユーザを指定することにより、ユーザのエンタイトルメントが一度に更新されるように設定できます。この設定は、RBE ポリシーを作成または編集するたびに行うことをお勧めします。

Identity Manager 3.6 より前では、個々のエンタイトルメントポリシーではなく、ドライバセット内のすべての RBE ポリシーに対してメンバーシップの再評価が実行されていました。一方、Identity Manager 3.6 では、RBE ポリシーを [評価] して、そのメンバーを選択した［[オブジェクトリスト]］に [追加] できます。エンタイトルメントポリシーを定義して、メンバーシップリストを作成してある場合、［選択したオブジェクト］のエントリの横に［メンバーをリストに [追加] するエンタイトルメントポリシーを評価します。］という見出しが表示されます。ポリシーを選択し、＋アイコンをクリックしてポリシーのメンバーを選択した［[オブジェクトリスト]］に追加します。選択した［[オブジェクトリスト]］では、メンバーやオブジェクトを追加または削除できます。

システムリソースを効率的に使用するには、特定のドライバセット内の RBE ポリシーへの変更をすべて行ってから、[225 ページの 「RBE ポリシーの再評価」] を使用してください。

注 : エンタイトルメントの再評価が必要なのは、接続システムのエンタイトルメントだけです。RBE ポリシーの Identity Console 権利が変更された場合、その変更はただちに各ユーザに反映されます。メンバーシップの再評価を実行するには、エンタイトルメントサービスドライバが実行されている必要があります。

RBE ポリシーの再評価

メンバーシップを再評価するには、次の方法を実行します。

1 [**[メンバーシップの再評価]**] > [**[ドライバセットの選択]**] をクリックします。

作成されたポリシーのリストが表示されます。

2 評価する必要があるポリシーを選択し、[**[評価]** Evaluate] をクリックします。

[**[オブジェクト]**] タブにグループの一部であるユーザが表示されます。

3 (オプション) 特定のユーザを追加するには、[+] をクリックします。

ユーザがリストに表示されず、特定のユーザを追加する場合にのみ、この [**[追加]** +] 機能を使用できます。

4 (オプション) 特定のユーザを削除するには、[🗑] をクリックします。

特定のユーザをリストから削除する必要がある場合にのみ、[**[削除]** 🗑] 機能を使用できます。

5 [メンバーシップの再評価] ボタン▷をクリックします 。

図 33-7 メンバーシップの再評価