OpenAM 14 ベストプラクティスガイド

OSSTech **株式会社**

更新日	2023 **年** 4 **月** 28 **日**
リビジョン	1.2

目次

1 はじめに

1.1 本書の目的

本文書は弊社提供の OpenAM 14 向けベストプラクティスガイドです。

1.2 前提情報

本文書では、弊社提供の OpenAM 14 及び OpenAM Apache Policy Agent 4 を対象としています。

事前に別紙「OpenAM 14 初期設定ガイド（冗長構成）」をお読みいただき、OpenAM のサイト構成を理解していただく必要があります。

2 システム構成例

本章では、標準的なシステム構成について説明します。

2.1 サーバー構成及び通信ポート

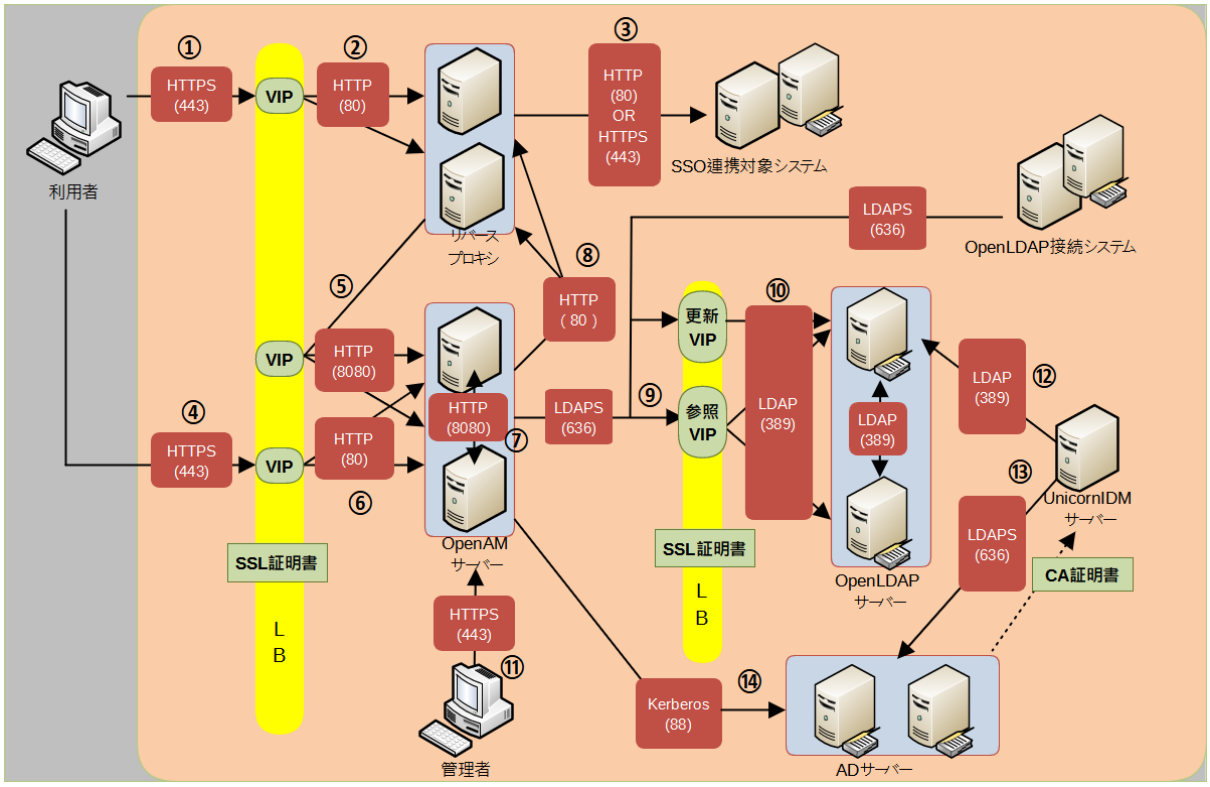

図 1　サーバー構成図

NO.	プロトコル (ポート)	説明
1	HTTPS(443)	ユーザーはリバースプロキシ経由で SSO 連携対象システムのページにアクセスする場合は HTTPS(443) で通信を行います。
2	HTTP(80)	ユーザーからのリバースプロキシへのアクセスは LB で処理され、SSL を解き HTTP(80) で通信が行われます。負荷分散にあたりセッションの維持（LB が発行する Cookie）が必要です。

NO.	プロトコル (ポート)	説明
3	HTTP(80) or HTTP(443)	リバースプロキシから SSO 連携対象システムへは HTTP(80) または HTTPS(443) 通信となります。HTTP(80) または HTTPS(443) かは対象システムによって異なります。
4	HTTPS(443)	ユーザーは OpenAM サーバーで認証する際は HTTPS（443）で通信を行います。
5	HTTP(8080)	リバースプロキシ上の OpenAM Policy Agent は、OpenAM サーバーに設定情報の問い合わせや認可の問い合わせを行います。LB 経由で問い合わせを行い HTTP(8080) で通信します。
6	HTTP(80)	ユーザーから OpenAM サーバーへのアクセスは LB で処理され、SSL を解き HTTP(80) で通信が行われます。負荷分散にあたりセッションの維持（LB が発行する Cookie）が必要です。
7	HTTP(8080) 等	2 台の OpenAM サーバー間はセッション情報等の参照や OpenDJ のレプリケーションのため複数のプロトコルの通信が発生します。8080 以外は TCP/1689,4444,50389,50889,58989 です。
8	HTTP(80)	OpenAM サーバーはリバースプロキシへポリシーやユーザーセッションのキャッシュの変更を HTTP(80) で通知します。
9	LDAPS(636)	OpenAM サーバーやその他の OpenLDAP 接続システムから OpenLDAP サーバへ LB 経由で問い合わせを行います。LDAPS(636) で通信します。LB 上に更新用の VIP と参照用の VIP があり、サーバーの用途によりどちらかの VIP に向けて接続します。
10	LDAP(389)	LB から OpenLDAP サーバーへ LDAP(389) で通信します。
11	HTTPS(443)	管理者は OpenAM 管理コンソールへ HTTPS(443) でアクセスします。
12	LDAP(389)	UnicornIDM サーバーから更新用のサーバーに向けて LDAP(389) でアクセスします。
13	LDAPS(636)	UnicornIDM サーバーから AD サーバに向けて LDAPS(636) でアクセスします。パスワード属性更新のため CA 証明書をあらかじめ設置して LDAPS(636) でアクセスできるようにします。
14	Kerberos(88)	OpenAM サーバーは統合 Windows 認証を行うために Active Directory との Kerberos プロトコルの通信を行います。

2.2 ソフトウェア構成

推奨構成では OpenAM (Tomcat) の前段に Apache を配置し、Apache - Tomcat 間は AJP で接続します。

サーバー	ソフトウェア名
OpenAM	Apache 2.4 (OS 標準パッケージ)
	OSSTech Tomcat 9
	OSSTech OpenAM 14.x
OpenLDAP	OSSTech OpenLDAP
リバースプロキシ	Apache 2.4 (OS 標準パッケージ)
	OSSTech OpenAM Policy Agent 4

2.3 FQDN 構成

OpenAM では FQDN に含まれるドメインの Cookie がセッション管理に利用されるため、FQDN の設計が必要です。

サーバー	ホスト名 (FQDN)
ロードバランサー (OpenAM)	sso.example.co.jp
OpenAM 1 号機	openam01.example.co.jp
OpenAM 2 号機	openam02.example.co.jp

2.4 アクセス URL

2.4.1 管理者ログイン

OpenAM の各種設定を行う際は以下の URL にアクセスし、管理者アカウントでログインします。この URL からログインして表示される画面を「管理コンソール」と呼びます。

- 1 号機 : https://openam01.example.co.jp/openam
- 2 号機 : https://openam02.example.co.jp/openam

2.4.2 一般ユーザーログイン

一般ユーザーとしてログインする場合は以下の URL にアクセスします。

- https://sso.example.co.jp/openam

2.4.3 コンテキスト名 (URI) の変更

初期値の openam から任意の文字列に変更する場合は、インストールガイドの「コンテキスト名の変更」の章を参照します。

2.5 OpenAM レルム構成

OpenAM のレルムとは、認証設定を構成する管理単位を示します。本書では以下のように構成します。

レルム	説明
/(最上位のレルム)	OpenAM 管理者用の設定を行います。 各サーバーのホスト名でアクセスされた場合に適用されます。
/sso	一般ユーザー用の設定を行います。 sso.example.co.jp でアクセスされた場合に適用されます。

3 推奨設定 (OpenAM)

本章では、OpenAM の推奨設定について記載します。

3.1 OpenAM の設定

OpenAM の管理コンソールで指定する推奨設定について記載します。

3.1.1 レルム設定 (共通)

最上位のレルムとサブレルムで共通して設定すべき内容を記載します。

3.1.1.1 「認証」の設定

設定項目	設定値	変更理由	備考
管理者用認証設定	組織認証設定と同じにする	クエリーパラメーターに service=adminconsoleservice を指定して、組織認証設定で認証連鎖を設定したのにもかかわらずデータストア認証だけでログインされることを防ぐため	
モジュールインスタンス	使用しない認証モジュールを全て削除する	クエリーパラメーターにモジュール名を指定して、意図しない認証方式でログインされることを防ぐため	
モジュールベースの認証	無効	クエリーパラメーターにモジュール名を指定して、意図しない認証方式でログインされることを防ぐため	ssoadm コマンドの対応も行うこと。

3.1.1.2 「サービス」の設定

設定項目	設定値	変更理由	備考
「Validation Service」→「Valid goto URL Resources」	OpenAM 認証後に遷移して良い URL	オープンリダイレクト対策	レルム単位で設定します。ドメイン単位で許可する場合ワンレベルワイルドカード (-*-) を使用します 。 [設定例] https://-*-.example.co.jp/* https://-*-.example.co.jp/*?*

3.1.2 最上位のレルム（OpenAM 管理者用）

最上位のレルムで設定すべき内容を記載します。

3.1.2.1 「認証」の設定

サブレルム用 FQDN から amadmin の認証ができることのを防ぐため、認証連鎖 (ldapService) にアダプティブリスク認証を追加し、管理者ログイン可能な IP アドレスを制限します。 設定のミスにより amadmin で認証できなくなることを防ぐため、設定後はブラウザを閉じる前に、別のブラウザで amadmin のログインができる事を確認してください。

3.1.2.2 「対象」の設定

OpenAM のデフォルトで存在する以下のユーザを削除します。

- anonymaous
- demo

3.1.3 デフォルトサーバー

本設定は管理コンソールの「設定」→「デフォルトサーバー」で設定します。

3.1.3.1 「セキュリティ」の設定

設定項目	設定値	変更理由
「Cookie」タブ→「セキュリティー保護された Cookie」	有効にする	Cookie に Secure 属性を付与するため (セキュリティ対策)

3.1.3.2 「セッション」の設定

設定項目	設定値	変更理由
最大セッション数	5000(初期値)	1 台のサーバーに許容するセッション数を設定します。ユーザー数 x 許容される多重ログイン数 + 100 (管理用/agent 等)

3.1.3.3 「詳細設定」の設定

設定項目	区分	設定値	変更理由	備考
com.sun.identity.cookie .httponly	変更	true	Cookie に HTTPOnly 属性をを付与するため (セキュリティ対策)	OpenAM を SAML SP (JSP 方式) として使用する場合は true にしてしまうと、セッション発行時に httponly が付き、OpenAM のページ (XUI) の JavaScript が Cookie を認識できなくなるため false を指定します。

3.1.4 グローバルサービス

本設定は管理コンソールの「設定」→「グローバルサービス」で設定します。

3.1.4.1 「セッション」の設定

許容される多重ログイン数 (既定無制限)

設定項目	設定値	変更理由	備考
「グローバル属性」→「割り当て制限を有効」	オン	一人のユーザーが無制限に多重ログインしてセッションを大量に発行することを防止するため	アクティブなユーザーセッション数はヒアリングして決定します。

3.1.5 連携

本設定は管理コンソールの「連携」で設定します。SAML の設定の設定の確認／変更に利用します。

3.1.5.1 ホストエンティティープロバイダの設定

中継状態 (Relay State) の URL リストは、以下のケースでは必ず設定してください。

- OpenAM を SAML SP として使用し、spSSOInit.jsp を利用する場合
- シングルログアウト起点 URL へ Apache でアクセス制限をしていない場合

設定項目	設定値	変更理由	備考
「対象の EntityID」→「高度」→「中継状態の URL リスト」	OpenAM 認証後に遷移して良い URL	オープンリダイレクト対策のため	OpenAM は RelayState に URL を入れることで OpenAM 認証後の遷移先 URL を制御することができます。

3.2 Apache の設定

OpenAM の前段に配置する Apache での推奨設定について記載します。

3.2.1 各ディレクティブの推奨値

設定項目	区分	設定値	変更理由	備考
ServerTokens	変更	ProductOnly	Apache のバージョン情報を応答しない (セキュリティ対策)	レスポンスヘッダーの Server で応答する情報が Apache となります (バージョンや OS が入らない)。
ServerSignature	変更	Off	Apache のバージョン情報を応答しない (セキュリティ対策)	Apache のデフォルトのエラー画面にバージョン情報を応答しません。

設定項目	区分	設定値	変更理由	備考
Options	変更	Indexes を削除	ファイル一覧を表示しない (セキュリティ対策)	
TraceEnable	追加	off	TRACE メソッドを無効にする	

3.2.2 リッスンポート

OpenAM サーバー (Apache) は用途を分けた 3 つのポートでリッスンする構成を推奨します。

ポート番号	説明
80	サービス提供用です。一般ユーザーからのアクセスを処理します。
8080	サーバー間通信用です。OpenAM/Agent サーバー間のアクセスを処理します。
443	管理コンソール用です。管理者の端末からのアクセスを処理します。

この構成にすることで次のメリットがあります。

- <VirtualHost>で区切ることで、それぞれの用途がわかりやすい
- 用途毎にアクセス制御も設定しやすい
- VirtualHost 単位でアクセスログを分けて出力することができ、障害時に解析しやすい

3.2.3 プロキシ設定

`retry=0` をつけることで復帰した OpenAM に対してタイムラグなく接続することができます。

【設定例】

```
ProxyPass /openam ajp://localhost/openam retry=0
```

3.2.4 アクセス制御

必要な URL のみを外部に開放するように設定します。これにより、把握していない機能の悪用を防ぐ／脆弱性の影響を限定させることができます。

3.2.4.1 サービス提供用ポートのアクセス制御

提供するサービスに従い、必要な URL のみアクセスを許可します。

【設定例】

```
<VirtualHost *:80>
    ServerName https://sso.example.co.jp:443

    <Location /openam>
        Require all denied
    </Location>

    <LocationMatch "^/+openam$">
        <RequireAll>
            Require all granted
            Require method GET POST
        </RequireAll>
    </LocationMatch>

    <LocationMatch "^/+openam/+$">
        <RequireAll>
            Require all granted
            Require method GET POST
        </RequireAll>
    </LocationMatch>

    <LocationMatch "^/+openam/+(UI/+Login|UI/+Logout|ArtifactResolver|SSORedirect
|SSOPOST|AuthConsumer|IDPSloRedirect|IDPSloInit|IDPSloPOST|idpssoinit|SAMLAwareSe
rvlet|SAMLSOAPReceiver|cdcservlet|XUI|isAlive\.jsp)">
        <RequireAll>
            Require all granted
            Require method GET POST
        </RequireAll>
    </LocationMatch>
```

```
    <LocationMatch "^/+openam/+json/+(authenticate|serverinfo|sessions|dashboard
)">
        <RequireAll>
            Require all granted
            Require method GET POST
        </RequireAll>
    </LocationMatch>

    <LocationMatch "^/+openam/+json/+users">
        <RequireAll>
            Require all granted
            Require method GET POST DELETE
        </RequireAll>
    </LocationMatch>

    <LocationMatch "^/+openam/+oauth2/+(\.well-known/+openid-configuration|access
_token|authorize|connect/+jwk_uri|userinfo|tokeninfo|introspect)">
        <RequireAll>
            Require all granted
            Require method GET POST
        </RequireAll>
    </LocationMatch>

</VirtualHost>
```

3.2.4.2 サーバー間通信用ポートのアクセス制御

OpenAM サーバーの IP アドレス及びリバースプロキシサーバーがリクエストする LB の VIP からのアクセスを許可します。

【設定例】

```
<VirtualHost *:8080>
    ServerName sso.example.co.jp

    <Location /openam>
        Require ip 10.0.119.124 // OpenAM 1 号機の IP アドレス
        Require ip 10.0.119.125 // OpenAM 2 号機の IP アドレス
        Require ip 10.0.119.121 // リバースプロキシがリクエストする LB の VIP
    </Location>
</VirtualHost>
```

3.2.4.3 管理コンソール用ポートのアクセス制御

管理者端末の IP アドレスによるアクセスのみを許可します。

【設定例】

```
<VirtualHost *:443>
    ServerName https://openam01.example.co.jp:443
    SSLEngine On
    SSLCertificateKeyFile /etc/pki/tls/private/openam01.key
    SSLCertificateFile /etc/pki/tls/certs/openam01.crt
    #SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

    <Location /openam>
        Require ip 10.0.119.100 // 管理者端末の IP アドレス
    </Location>

</VirtualHost>
```

3.2.5 パストラバーサル対策

Apache と Tomcat 間でパスの解釈が異なることによるパストラバーサルを防ぐため、下記の設定を行います。

```
RewriteRule \.\.; - [forbidden]
```

設定は<VirtualHost>内に記載します。

3.2.6 ログ設定

3.2.6.1 ログフォーマット

トレーサビリティ強化のため、ログ出力項目に %D (出力時間) と %P:%{tid}P (プロセス ID とスレッド ID) を追加します。

【設定例】

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %D
%P:%{tid}P" osstech
```

3.2.6.2 サービス提供用ポートの出力設定

一般ユーザーのアクセスと LB による死活監視のアクセス (isAlive.jsp) を個別のログに出力します。

【設定例】

```
<VirtualHost *:80>
    ...
    SetEnvIf Request_URI "^/openam/isAlive.jsp$" healthcheck=on
    CustomLog logs/access_log osstech env=!healthcheck
    CustomLog logs/healthcheck-access_log osstech env=healthcheck

</VirtualHost>
```

3.2.6.3 サーバー間通信用ポートの出力設定

OpenAM 間のアクセスとリバースプロキシからのアクセスを個別のログに出力します。

【設定例】

```
<VirtualHost *:8080>
    ...
    <Location "/openam/namingservice">
        SetEnvIf Remote_Addr "(10.0.119.124|10.0.119.125)" openam-failover-access
=1
    </Location>

    CustomLog logs/openam-agent-access_log osstech env=!openam-failover-access
    CustomLog logs/openam-failover-healthcheck-access_log osstech env=openam-fail
over-access
    ErrorLog logs/openam-agent-error_log

</VirtualHost>
```

3.2.6.4 管理コンソール用ポートの出力設定

管理コンソールのアクセスを個別のログに出力します。

【設定例】

```
<VirtualHost *:443>
    ...
    CustomLog logs/openam-console-access_log osstech_ssl
```

```
    ErrorLog logs/openam-console-error_log

</VirtualHost>
```

3.3 Tomcat の設定

3.3.1 server.xml

server.xml (/opt/osstech/etc/tomcat/server.xml) では以下の設定を変更してください。

- スレッド数
  - Apache のスレッド数を上回るような Tomcat スレッド数を maxThreads に設定します
- スキーム／ポート
  - OpenAM に HTTPS で動作していることを認識させるため、scheme と proxyPort を変更します
  - Tomcat が発行する Cookie に Secure 属性が付与されるように secure に true を設定します
- エンコーディング
  - URIEncoding に UTF-8 を設定します
- AJP
  - AJP をリッスンする IP アドレスを address に指定します
  - ローカルホスト以外を指定する場合は secretRequired を true にし、secret を設定します

【設定例】

```
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
               maxThreads="512"
               URIEncoding="UTF-8"
               scheme="https"
               secure="true"
               secretRequired="false"
               address="127.0.0.1"
               proxyPort="443" />
```

3.3.2 tomcat.conf

tomcat.conf (/opt/osstech/etc/tomcat/tomcat.conf) では以下の設定を変更してください。

- Java ヒープサイズ

【設定例】

```
JAVA_HEAPSIZE="2048M"
```

3.4 ログローテーションの設定

3.4.1 OpenAM

OpenAM のログは以下の 4 つに分類されます。

種類	デフォルトの出力先
監査ログ	/opt/osstech/var/lib/tomcat/data/openam/openam/log
デバッグログ	/opt/osstech/var/lib/tomcat/data/openam/openam/debug
統計ログ	/opt/osstech/var/lib/tomcat/data/openam/openam/stats
OpenDJ ログ	/opt/osstech/var/lib/tomcat/data/openam/opends/logs

- 監査ログはファイル先頭にヘッダーが付与された CSV ファイルです。logrotate で分割されヘッダーが無い状態になると出力エラーとなります
- OpenDJ ログは内部にローテーション設定 (24h, size) を持っています

以上のことから次の方針でローテーションを行います

- 監査ログは OpenAM の機能でローテーションして、logrotate で圧縮・削除の処理をします
- OpenDJ ログは内部のローテーション設定を時刻に変更して、logrotate で圧縮・削除の処理をします
- デバッグログ及び統計ログは logrotate でローテーション・圧縮・削除の処理をします

それぞれのログは以下のようなローテーション実行プログラムで分担します。

種類	ローテーション実行	世代管理
監査ログ	OpenAM 内蔵ローテーション機能	logrotate
デバッグログ	logrotate	logrotate
統計ログ	logrotate	logrotate
OpenDJ ログ	OpenDJ 内蔵ローテーション機能	logrotate

各ログの初期ローテーション設定は以下表の通りです。

種類	ローテーションタイミング	保存世代
監査ログ	サイズ 100MB	100 世代
デバッグログ	日次 (O.S の logrotate 実行時)	100 世代
統計ログ	日次 (O.S の logrotate 実行時)	100 世代
OpenDJ access/audit ログ	起動から 24 時間毎、又はサイズ	100 世代
OpenDJ error/replication ログ	起動から 7 日間毎、又はサイズ	100 世代

3.4.1.1 OpenAM 用 logrotate の設定ファイル

監査ログと OpenDJ のログでは世代管理、デバッグログと統計ログではログローテーションと世代管理に logrotate を使用しています。

OpenAM 14 の RPM パッケージには 100 日分ログを保持する logrotate の設定ファイルが同梱されています。

実行時間は OS 標準の logrotated が動作するタイミングで同時に処理されます。

なお、OpenAM のコンテキストパスを変更している場合は各ログの出力先がデフォルトから変わるため logrotate 設定ファイルのパス修正が必要です。

設定を変更するには以下のファイルを変更して下さい。

```
/opt/osstech/etc/logrotate.d/openam
```

3.4.1.2 OpenAM 内蔵ローテーションの機能　(Global CSV Handler)　の設定

初期値の 100MB でローテーションされる状態を、日次でローテーションされるように変更する場合

メニュー表示により以下いずれかを開く

- 設定>グローバルサービス>Audit Logging を開く
- 設定>グローバル>Audit Logging を開く

Audit Event Handlers>Global CSV Handler から設定

設定項目	設定値	変更理由
Maximum File Size	0(初期値=100000000)	ファイルサイズでローテーションされないようにする
Rotation Times	10800(初期値=無し)	0 時からの秒数を設定 10800 だと 03:00 にローテーションされる

設定項目	設定値	変更理由
Maximum Number of Historical Files	30(初期値=1)	OpenAM のローテート実行でファイルを削除しないようにする

3.4.1.3 OpenDJ 内蔵ローテーション機能の設定

ローテーションのタイミングは、初回は OpenAM 起動からの経過時間、2 回目以降は前回ローテーションからの経過時間になっています。また、サイズ制限もあり 100MB を超えるとローテーションされます。

種類	ローテーションタイミング
OpenDJ access/audit ログ	起動から 24 時間毎又はサイズ
OpenDJ error/replication ログ	起動から 7 日間毎又はサイズ

弊社パッケージの世代管理は logrotate で行っていますが、OpenDJ 自身の初期値では総容量 500MB、ディスクの空き 500MB、又は 10 ファイルを制限としています。※弊社パッケージでは logrotate でファイルを old ディレクトリ以下へ移動しているため、10 ファイル制限は実行されません。

- コマンド実行時のパスワード設定

${DS_DIRMGRPASSWD} は、OpenAM 初期設定時の amadmin のパスワードです。
環境変数へセットしてから以下を実行します。

```
# DS_DIRMGRPASSWD=パスワード文字列
```

- OpenDJ カスタムローテーションポリシーの作成

ここでは AM3 時になるとローテーションされるポリシーを、ポリシー名「Fixed Time(3:00) Rotation Policy」として作成しています。

```
# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    create-log-rotation-policy \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --policy-name "Fixed Time(3:00) Rotation Policy" \
    --type fixed-time \
```

```
    --set time-of-day:0300 \
    --no-prompt \
    --trustAll
```

- ログ毎の既定ログローテーションポリシー設定の削除

access,audit,error,replication ４種類のログの既存ログローテーションポリシー設定の削除します。

```
# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Access\ Logger \
    --remove "rotation-policy:24 Hours Time Limit Rotation Policy" \
    --remove "rotation-policy:Size Limit Rotation Policy" \
    --no-prompt \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Audit\ Logger \
    --remove "rotation-policy:24 Hours Time Limit Rotation Policy" \
    --remove "rotation-policy:Size Limit Rotation Policy" \
    --no-prompt \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Error\ Logger \
    --remove "rotation-policy:7 Days Time Limit Rotation Policy" \
    --remove "rotation-policy:Size Limit Rotation Policy" \
    --no-prompt \
    --trustAll
```

```
# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name Replication\ Repair\ Logger \
    --remove "rotation-policy:7 Days Time Limit Rotation Policy" \
    --remove "rotation-policy:Size Limit Rotation Policy" \
    --no-prompt \
    --trustAll
```

- 作成したカスタムローテーションポリシーの適用設定

４種類のログに作成したカスタムローテーションポリシーを適用します。

```
# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Access\ Logger \
    --set rotation-policy:"Fixed Time(3:00) Rotation Policy" \
    --no-prompt \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Audit\ Logger \
    --set rotation-policy:"Fixed Time(3:00) Rotation Policy" \
    --no-prompt \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
```

```
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Error\ Logger \
    --set rotation-policy:"Fixed Time(3:00) Rotation Policy" \
    --no-prompt \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    set-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name Replication\ Repair\ Logger \
    --set rotation-policy:"Fixed Time(3:00) Rotation Policy" \
    --no-prompt \
    --trustAll
```

- カスタムローテーションポリシーが適用されているかの確認

4 種類のログの rotation-policy の設定 (Value) が全て “Fixed Time(3:00) Rotation Policy” となっているか確認します

```
# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    get-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Access\ Logger \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    get-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Audit\ Logger \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    get-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
```

```
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name File-Based\ Error\ Logger \
    --trustAll

# /opt/osstech/var/lib/tomcat/data/openam/opends/bin/dsconfig \
    get-log-publisher-prop \
    --hostname localhost \
    --port 4444 \
    --bindDN "cn=Directory Manager" \
    --bindPassword ${DS_DIRMGRPASSWD} \
    --publisher-name Replication\ Repair\ Logger \
    --trustAll
```

- 設定確認の出力例

```
Property               : Value(s)
-----------------------:---------------------------------
append                 : true
enabled                : true
filtering-policy       : no-filtering
log-control-oids       : false
log-file               : logs/access (該当のログ名が表示されます)
log-file-permissions   : 640
log-format             : multi-line
log-record-time-format : dd/MMM/yyyy:HH:mm:ss Z
retention-policy       : File Count Retention Policy
rotation-policy        : Fixed Time(3:00) Rotation Policy
```

3.4.2 Apache

Apache のログローテーションは OS 標準パッケージ (httpd) に含まれる logrotate の設定 (/etc/logrotate.d/httpd) を利用します。

3.4.3 Tomcat

Tomcat のログローテーションは OSSTech Tomcat パッケージに含まれる logrotate の設定 (/opt/osstech/etc/logrotate.d/tomcat) を利用します。

3.5 ssoadm コマンド

コマンドラインツールである ssoadm を本文書の推奨設定を行った環境で利用するためには ssoadm に変更が必要です。

詳細は別紙「OpenAM 14 コマンドライン 利用手順書」をご覧ください。

4 推奨設定 (Agent)

4.1 Agent の設定

OpenAM の管理コンソールで指定する推奨設定について記載します。

4.1.1 「グローバル」の設定

設定項目	設定値	変更理由	備考
エージェント設定変更通知	無効	OpenAM -> Agent への通信を無くすため	
通知を有効	無効	OpenAM -> Agent への通信を無くすため	クロスドメイン SSO を有効にした場合は、通知を使った方が良いため有効にします。
エージェントのデバッグファイルサイズ	0	Agent のログローテートは logrotate で行うため	
監査アクセスタイプ	LOG_BOTH	監査ログを出力するため	
監査ログ位置	ローカル	監査ログは Agent 導入したサーバーに出力する	設定値にリモートを選択すると監査ログは出力されません。
ローカル監査ログローテーションサイズ	0	Agent のログローテートは logrotate で行うため	
FQDN 確認	（サーバー構成に依存）	意図しない FQDN で動作することを防ぐため基本は有効する	リバースプロキシサーバーで名前ベースのバーチャルホストを使用している場合のみ無効にします。

4.1.2 「アプリケーション」の設定

設定項目	設定値	変更理由	備考
適用されない URL	isAlive.html の URL 等	OpenAM の認証なしにアクセスできる URL を設定する	ポート番号は省略せずに記載します。

4.1.3 「OpenAM サービス」の設定

設定項目	設定値	変更理由	備考
ユーザー ID パラメータ	uid	デフォルトの UserToken だと全角入力でログインしたユーザーは、全角のユーザー ID となる。また、全角文字だと Apache のログでリモートユーザーがエスケープされて出力されてしまう	ユーザー名が uid 属性ではない場合、適切な属性をセットします。また、LDAP 属性の利用は SSO のみモードでは使用できないため注意が必要です。
ユーザー ID パラメータタイプ	LDAP	同上	

4.1.4 「高度」の設定

設定項目	設定値	変更理由	備考
ロードバランサの設定	無効	ロードバランサー配下に配置するときは、Apache の ServerName で設定する 設定例： ServerName https://[サーバーFQDN]:443	この設定で https やポート番号を Agent が認識しても Apache 自身は認識していません。そのため Agent ではなく、Apache 自身がリダイレクトする際 (例：末尾に/なしのディレクトリへのアクセス）には遷移する Location ヘッダーの値が http となります。ServerName で定義することで Apache と Agent の両方がロードバランサー配下でも https に遷移する構成の設定とすることができます。
要求 URL プロトコルの上書き	無効	同上	同上
要求 URL ホストの上書き	無効	同上	同上
要求 URL ポートの上書き	無効	同上	同上
通知 URL の上書き	無効	同上	同上

4.1.5 クロスドメイン SSO 向けの設定

Agent の設定の内、クロスドメイン SSO を有効にした場合に設定すべき内容について記載します。

設定項目	設定値	変更理由	備考
「グローバル」→「通知を有効」	有効	セッションの無効化を Agent に通知するため	クロスドメイン SSO では OpenAM は Agent のドメインクッキーを破棄できません。通知により SSO キャッシュの利用を防ぐ必要があります。
「SSO」→「Cookie セキュリティ」	有効	Cookie に Secure 属性を付与するため (セキュリティ対策)	
「高度」→「カスタムプロパティー」 com.sun.identity .cookie.httponly	true	Cookie に HTTPOnly 属性を付与するため (セキュリティ対策)	

4.1.6 Agent 4 で使用できないパラメーター

いくつかの設定は Agent 4 では使用できません。

設定項目	備考
「グローバル」→「エージェントデバックファイルのローテーション」	ローテーションを行わない様にする場合、ローテーションサイズに 0 を設定します。ローテーションする場合のサイズの最小値は 5 MB です。-1 とすると 24 時間に 1 回ローテーションします。
「グローバル」→「ローカル監査ログのローテーション」	同上
「グローバル」→「設定再読み込み間隔」	定期的な設定の再読み込みは行われません。設定変更後に Apache を再起動するか、通知を有効にします。
「グローバル」→「設定クリーンアップ間隔」	同上
「その他」→「サーバー確認を無視」	

4.2 Apache の設定

4.2.1 各ディレクティブの推奨値

設定項目	区分	設定値	変更理由	備考
ServerTokens	変更	ProductOnly	Apache のバージョン情報を応答しない (セキュリティ対策)	レスポンスヘッダーの Server で応答する情報が Apache となります (バージョンや OS が入らない)。
ServerSignature	変更	Off	Apache のバージョン情報を応答しない (セキュリティ対策)	Apache のデフォルトのエラー画面にバージョン情報を応答しません。
Options	変更	Indexes を削除	ファイル一覧を表示しない (セキュリティ対策)	
TraceEnable	追加	off	TRACE メソッドを無効にする	
AddDefaultCharset	変更	off	バックエンドサーバーからの応答レスポンスに Apache が文字コードをセットしてしまうことを防ぐため	Apache は text/plain と text/html に対して charset を付与します。
SSLProxyEngine	追加	on	バックエンドサーバーと SSL 接続するため	SSL 接続する際この定義が無いとエラーが発生します。mod_ssl を読み込む必要があります。
RequestHeader	追加	set Accept-Encoding identity	コンテンツの書き換えのため、バックエンドでコンテンツ圧縮をさせない	

設定項目	区分	設定値	変更理由	備考
RequestHeader	追加	unset [代理認証で使用するパスワードのヘッダー名]	バックエンドに代理認証で使用するパスワードを送信しないため	代理認証用の設定です。
SetEnvIf	追加	Request_URI ^/ proxy-nokeepalive=1	バックエンドと KeepAlive 接続はしない。通信相手が Windows だと HTTP の終了を正しく検知できないケースがある	

4.2.2 ログ設定

4.2.2.1 ログフォーマット

トレーサビリティ強化のため、ログ出力項目に %D (出力時間)、%P:%{tid}P (プロセス ID とスレッド ID)、%{Host}i (ホストヘッダー)、%{proxy-status}n (バックエンドのステータスコード) を追加します。

【設定例】

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %D
%P:%{tid}P %{Host}i  %{proxy-status}n" osstech_rp
```

4.2.2.2 出力設定

一般ユーザーのアクセスと LB による死活監視のアクセス (isAlive.html) を個別のログに出力します。 isAlive.html は死活監視用のコンテンツとして用意しています。

【設定例】

```
SetEnvIf Request_URI "^/isAlive.html$" healthcheck=on
CustomLog logs/access_log osstech_rp env=!healthcheck
CustomLog logs/healthcheck-access_log osstech env=healthcheck
```

4.3 logrotate の設定

4.3.1 Agent

Agent のログは以下の 2 つに分類されます。

種類	デフォルトの出力先
監査ログ	/opt/osstech/share/openam-agent4-apache24/instances/agent_1/logs/audit
デバッグログ	/opt/osstech/share/openam-agent4-apache24/instances/agent_1/logs/debug

これらのログのローテーションに logrotate を利用する場合、Apache のログローテーションは OS 標準パッケージ (httpd) に含まれる logrotate の設定 (/etc/logrotate.d/httpd) に追記してください。 これにより Apache の reload を重複して実行することを防ぎます。

【設定例】

```
/var/log/httpd/*log
/opt/osstech/share/openam-agent4-apache24/instances/agent_1/logs/audit/audit.log
/opt/osstech/share/openam-agent4-apache24/instances/agent_1/logs/debug/debug.log
{
    missingok
    notifempty
    sharedscripts
    delaycompress
    postrotate
        /bin/systemctl reload httpd.service > /dev/null 2>/dev/null || true
    endscript
}
```

4.3.2 Apache

Apache のログローテーションは OS 標準パッケージ (httpd) に含まれる logrotate の設定 (/etc/logrotate.d/httpd) を利用します。

5 改版履歴

- 2021 年 11 月 1 日 リビジョン 1.0
  - 初版作成
- 2021 年 12 月 7 日 リビジョン 1.1
  - OpenDJ 内蔵ローテーション機能記述
- 2023 年 4 月 28 日 リビジョン 1.2
  - OpenAM ローテーションの実行時刻の変更とファイル数を追加
  - Agent のデバッグと監査ログファイルのサイズ設定を追加
  - Apache のログフォーマットにスレッド ID の出力を追加
  - Apache のアクセス制御で cdsso の URL の許可設定を追加