クラウドネイティブ
CLOUD NATIVE INC.

Oktaのよいところ・これからなところ

忖度なしで正直に話します！

2021/6/29

クラウドネイティブ
CLOUD NATIVE INC.

1. はじめに
2. Oktaのよいところ
3. Oktaのこれからなところ
4. まとめ

クラウドネイティブ
CLOUD NATIVE INC.

1. はじめに
2. Oktaのよいところ
3. Oktaのこれからなところ
4. まとめ

このセッションについて

- この資料は公開します！画面キャプチャ、SNS公開どんとこい！
- 小さい子供がいます。セッション中、叫び声や喚き声が入るかもしれませんがご了承ください🙇‍♀️
- Zoomのコメント欄盛り上げてください！
  - みなさんが思うOktaのよいところ・これからなところ
  - みなさんが思うAzure ADのよいところ・これからなところ
  - コメント欄 ~~炎上~~ エンジョイしましょう！

自己紹介

五戸 禎人 (gonoway)
Yoshihito Gonohe
Cloud Native Inc.
Cloud Security Architect

経歴

- セキュリティ製品のデプロイ（前職）->MDM（Intune、Jamf）
  ->育休（1年→CISSP取得）->IdP（Okta、Azure AD）

今やっていること

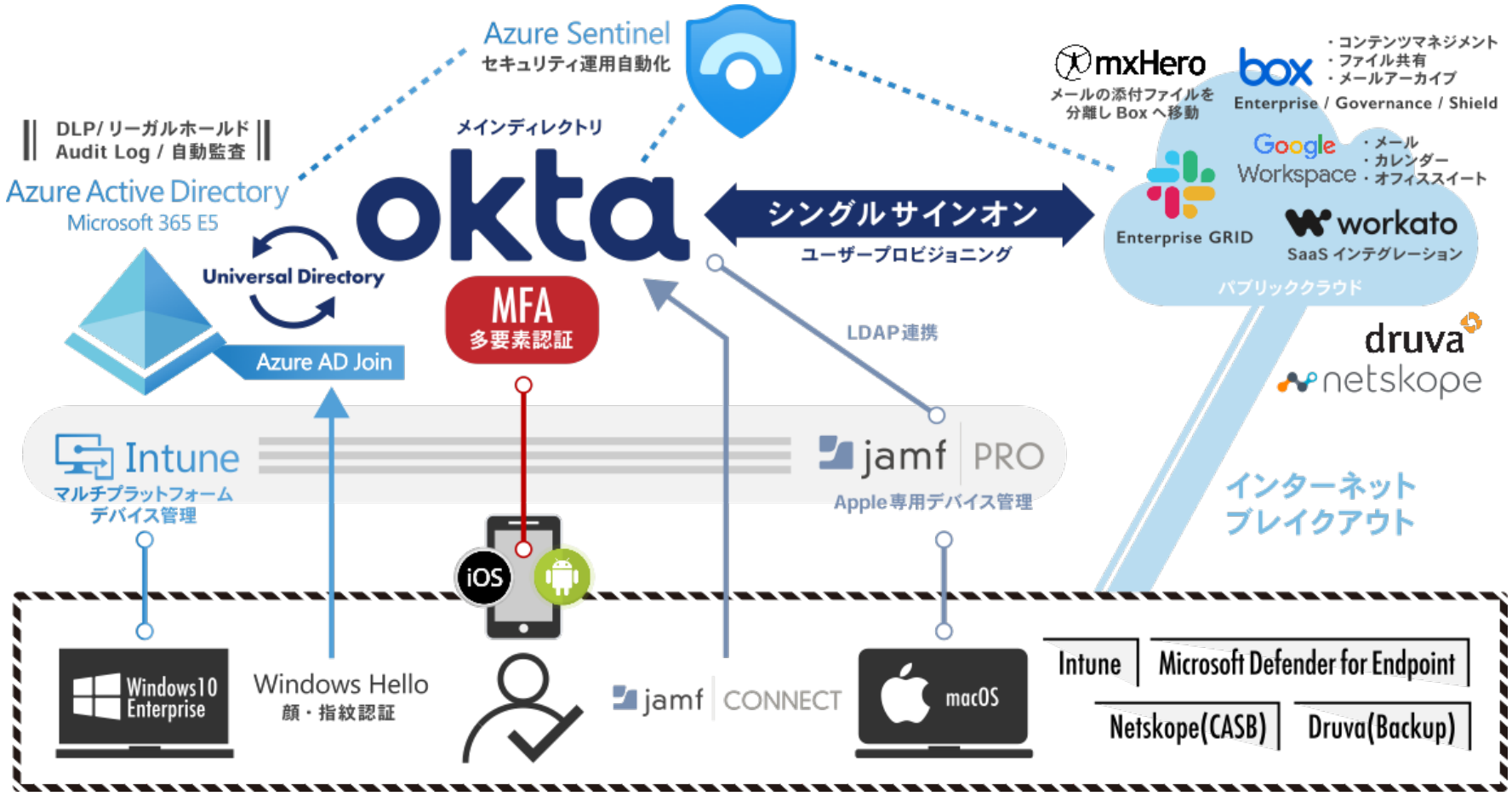
- 情報システム部門へのコンサルティング業務
- 新製品の調査・検証

その他言いたいこと

- JOUGも好きだし、JPEMSUGも好きだし、JMUGも好きです！！

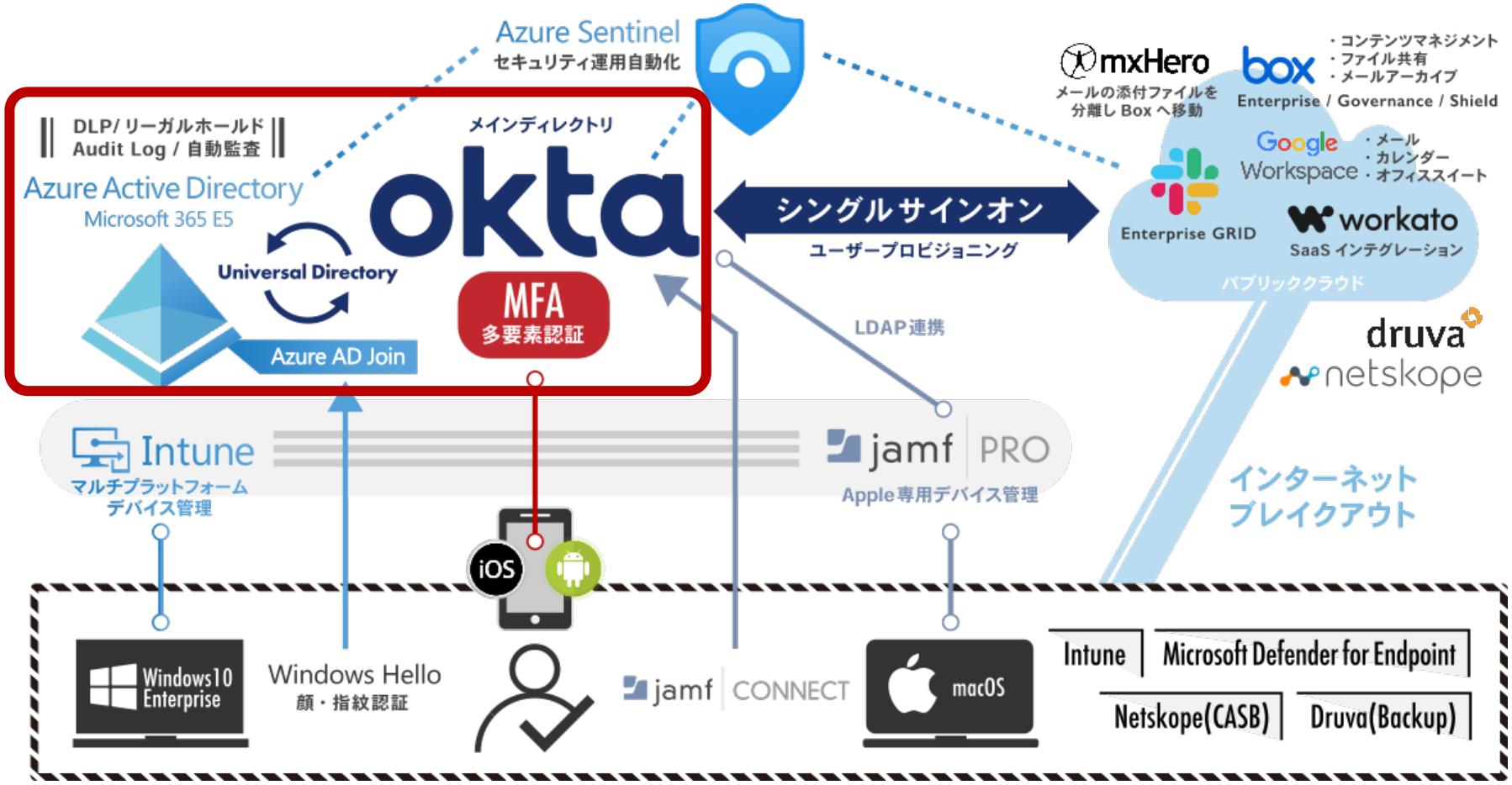
自社の構成

クラウドネイティブでは、自社の環境をゼロトラストモデルの実証としています



自社の構成

クラウドネイティブでは、自社の環境をゼロトラストモデルの実証としています



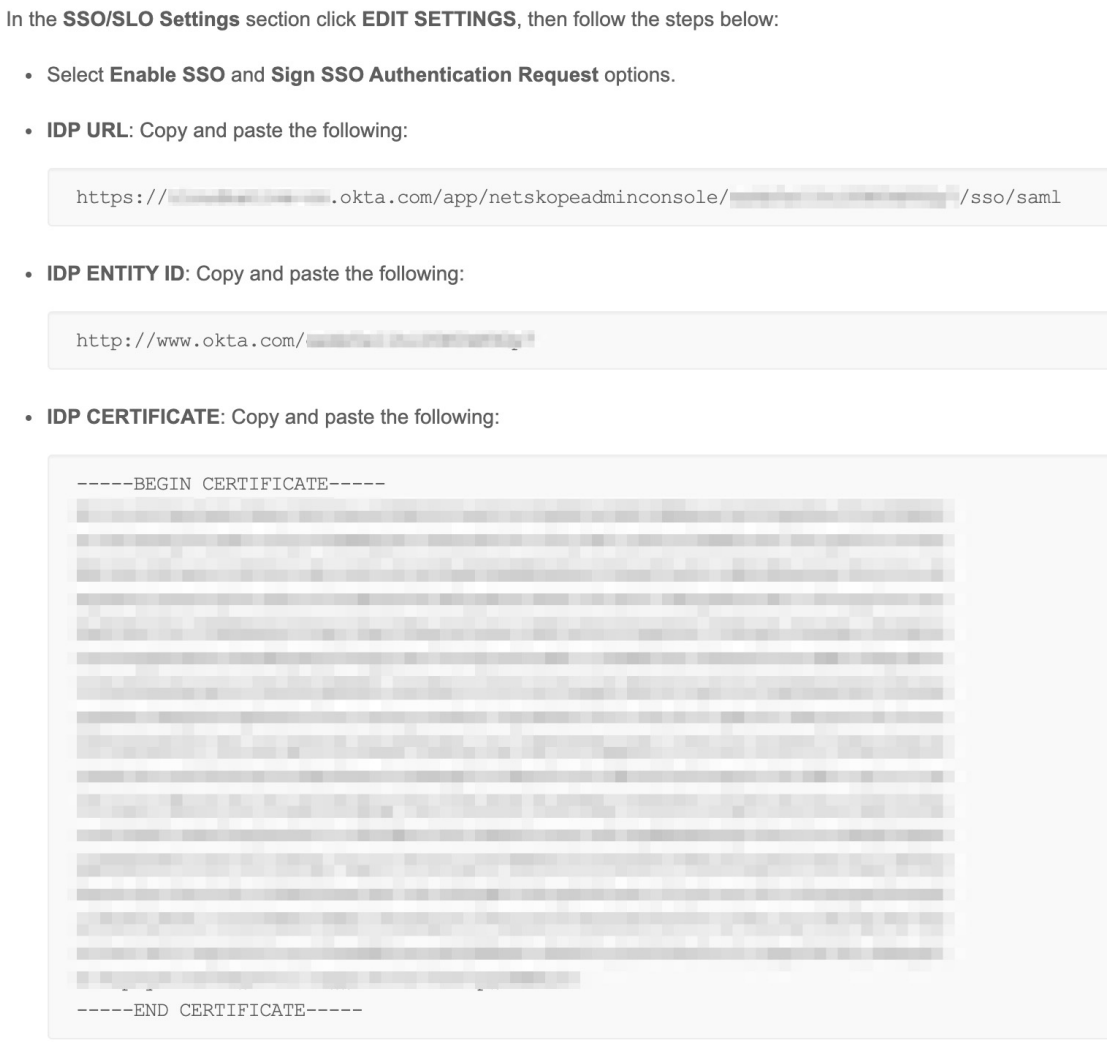
クラウドネイティブ
CLOUD NATIVE INC.

1. はじめに
2. Oktaのよいところ
3. Oktaのこれからなところ
4. まとめ

SSOのしやすさ！

- SSOを構成する際に、SSOの手順がアプリケーションごとに表示できる。
- Entity IDや証明書の自社の情報をコピペできる！

- Azure ADのSSO手順のページ読みにくい。慣れが必要な気がしてます。。
  - 上から下に手順を見れば良いって訳ではないのが辛い。



In the **SSO/SLO Settings** section click **EDIT SETTINGS**, then follow the steps below:

- Select **Enable SSO** and **Sign SSO Authentication Request** options.
- **IDP URL**: Copy and paste the following:

```
https://[redacted].okta.com/app/netskopeadminconsole/[redacted]/sso/saml
```

- **IDP ENTITY ID**: Copy and paste the following:

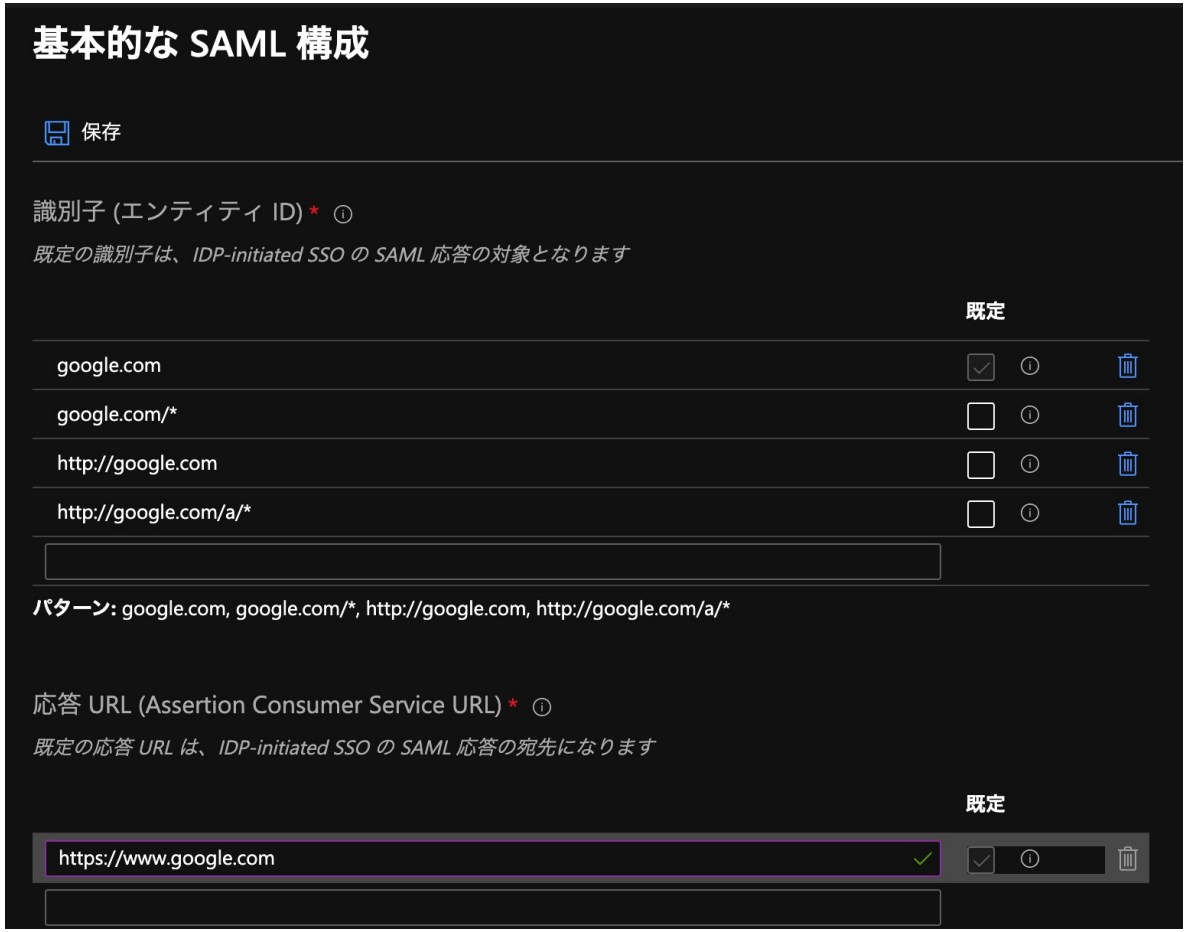
```
http://www.okta.com/[redacted]
```

- **IDP CERTIFICATE**: Copy and paste the following:

```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

一方Azure ADのSSOでは。。

- Azure ADでSSOする時にアスタリスクあるとエラーになる。
- 一度設定をリセットしないと設定を保存できないバグ？をなんとかしてほしい。。



UI/UXが良い！

例）プロビジョニングにおけるUX

- Oktaはプロビジョニング設定後、ユーザーをアサインすると即時にアプリケーションへのプロビジョニングが実行される！

- Azure ADはプロビジョニング設定後、ユーザーをアサインしても即時にアプリケーションへのプロビジョニングが実行されない。
  - 定期サイクルでプロビジョニングが実行される。
  - 手動で即時にプロビジョニングの実行はできるけど、、めんどくさい。

Oktaの可用性の高さ！

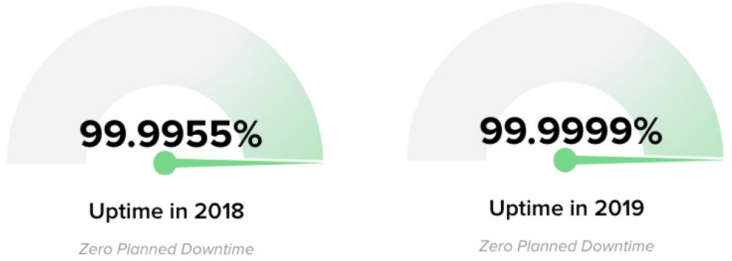
- OktaのSLAは99.99%
- 稼働率の実績ベース可用性とダウンタイム
  - 2018年：99.9955%＝年間 23.7分以内
  - 2019年：99.9999%＝年間 0.5分以内
- Oktaが落ちて使えない印象がない！

- Azure ADもSLAは99.99%だけど
  - 2020/9/29、2021/3/16でそれぞれ障害発生。

How does 99.99% change the landscape of IAM reliability?

99.99% uptime means 52 minutes and 35 seconds of allowed downtime per year, whereas 99.9% uptime means 8 hours, 45 minutes and 56 seconds of allowed downtime per year. This difference continues to increase when you factor in that some identity providers allow for more than 30 minutes of maintenance per week—upwards of 34 hours of downtime per year! What would it mean for your business if your most loyal customers were unable to access your products and services during that time period?

Through our highly available cloud architecture and unwavering focus on reliability, Okta has already achieved greater than 99.99% uptime since 2017. We do this while deploying over 48 releases per year with zero planned downtime, as the Okta service never shuts down for maintenance.



Okta's approach brings a sea of change compared to on-premises identity platforms of the past, cloud identity platforms that have not invested similarly, or build-it-yourself solutions. On-premise platforms and build-it-yourself solutions are expensive, time consuming to set up, and difficult to maintain. These platforms are deployed per company, and the onus for reliability is typically on that individual business. Often, cloud identity solutions inherit reliability from their infrastructure providers without fully understanding that additional capabilities need to be built to handle the complex nuances of identity. Okta has built a global, scalable, reliable, and redundant cloud architecture that makes 99.99% uptime a reality, and makes identity one of the most reliable components of the modern technology stack.

If you'd like to learn more about Okta's historical uptime, please visit: ***trust.okta.com****.*

Universal Directory便利！

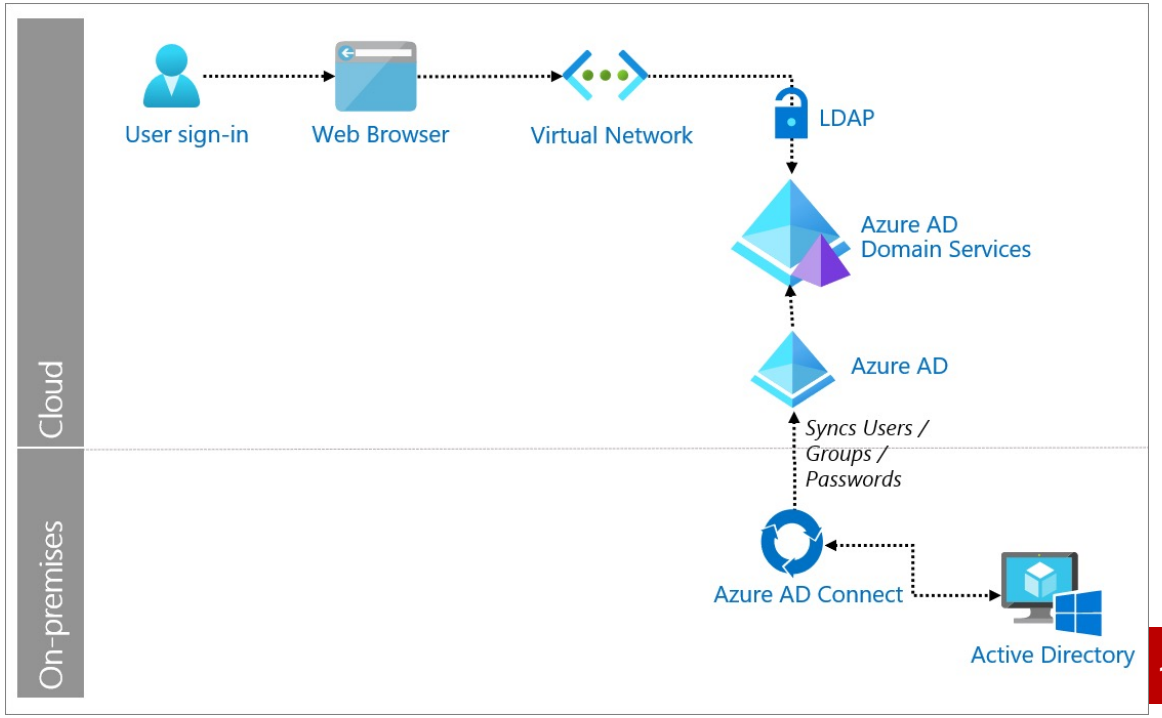
- Okta Universal Directoryの主要な機能
  - AD・LDAPや人事システムなどのアプリやデータソースから情報を簡単にインプットし管理できる。
  - 複数AD・LDAPがある場合にOkta Universal Directoryを使うと、Oktaがユーザ情報を吸い上げて、以降Oktaをマスターとして管理ができる！

- Azure AD の場合、Azure AD Connect クラウド同期という類似の機能がある。
  - Azure AD Connectと根本は変わらないためAD側がマスターとなる。
  - デバイス情報の送信がサポートされない。
    - Hybrid Azure AD Joined構成やEndpoint Managerが使えない。

Universal Directory便利！

- Okta LDAP Interfaceの機能で
  Okta自身がLDAPとして振る舞う
  ことができる！
  - 既存環境にLDAPがある場合に
    Oktaで代替できる！

- Azure ADではAzure ADDSという
  別サービスを構成しないといけな
  い。



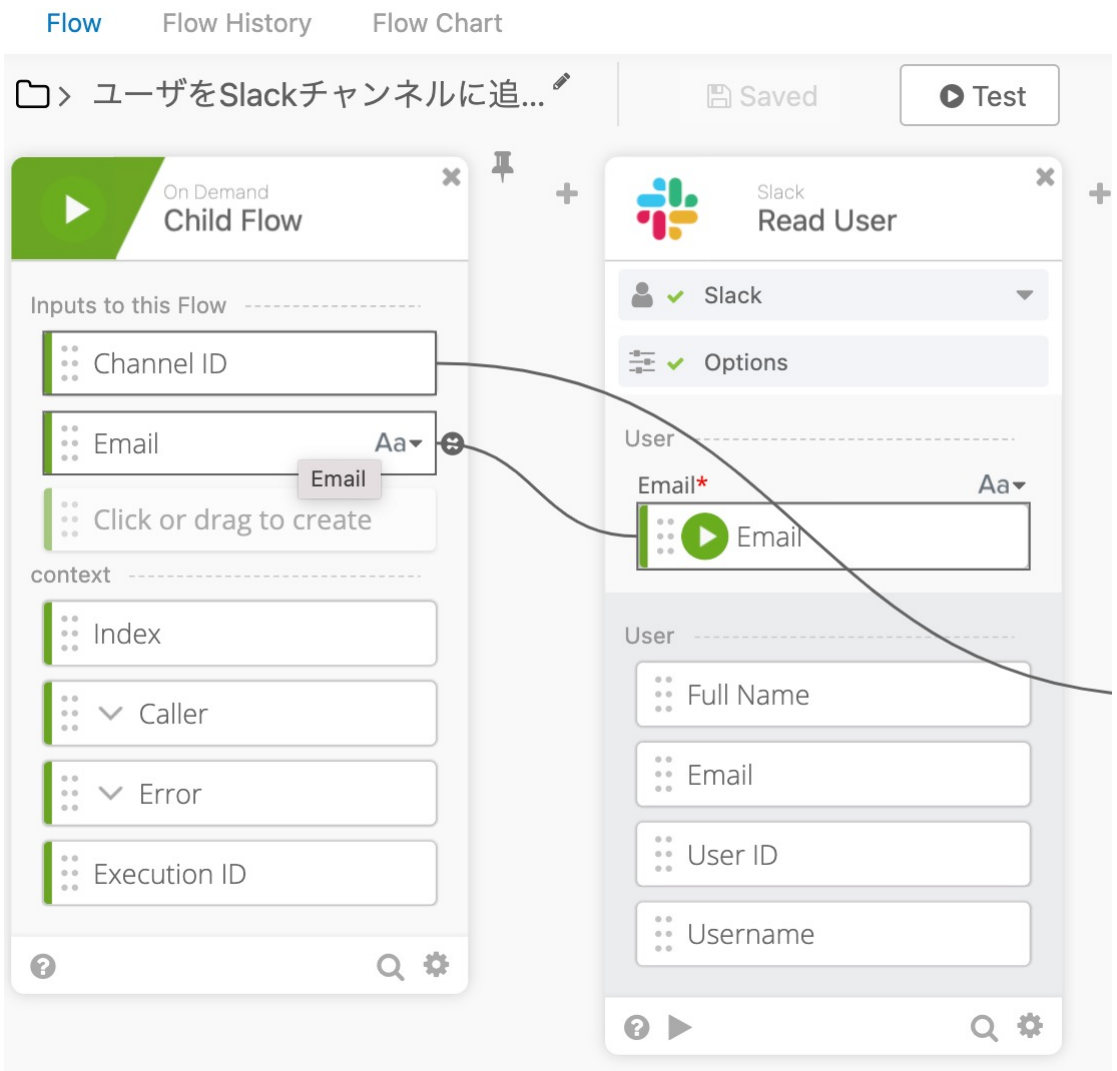
いろんなSaaSと掛け合わせやすい！

- いわゆるベストオブブリードの思想
- OktaはIdP専業のためIdP以外の製品は使いたいものを使おうっていう思想
  - コミュニケーションツール、クラウドストレージ、CASB、etc.
- 新しいツールをすぐテストでき、すぐ捨てることができる
- Azure ADはMicrosoftの製品・機能群でまとめた方が強い。

各種SaaSとの連携がしやすい！

- Okta Workflows
  - 各種SaaSとの連携を直感的操作で実現できる。
  - まだ発展途上なところも見られるので、今後のアップデートにも期待してます！

- Azure ADはLogic Appを使う。
  - あまり直感的でない（個人の感想）
  - 用意されているコネクターのアプリケーションがMSのものが多い。



クラウドネイティブ
CLOUD NATIVE INC.

1. はじめに
2. Oktaのよいところ
3. Oktaのこれからなところ
4. まとめ

簡単にデバイス認証ができるようになってほしい！

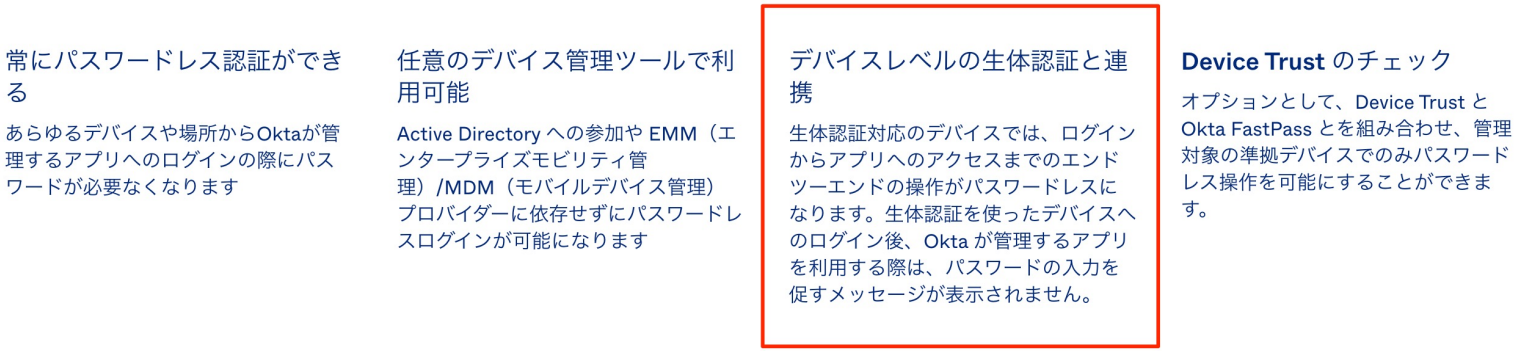
- Azure ADだとIntuneとの組み合わせで簡単にできる。
  - デバイスの状態を見て、アクセス制御を行うこともできる。

- Oktaの場合、Windowsデバイスに対するデバイス認証の実現が面倒。
  - Okta Devices機能(Okta Identity Engine)リリース待ってます！
  - 暫定的に別製品を使って代替することもありっちゃあり。

Azure ADだとアプリへのSSO楽チン（なケース有）

- Azure ADの場合、Azure AD Join・Hybrid Azure AD Join端末だとデバイスへのログインかつ特定のブラウザの場合に、Azure ADのアプリケーションダッシュボードへのログインが不要になる。
  - デバイスへログインした際に発行されるトークンを利用できるため。

- Oktaは現時点ではデバイスへのログインとOktaダッシュボードでの認証の2つが必ず発生する。
  - Okta Fastpass(Okta Identity Engine)リリース待ってます！



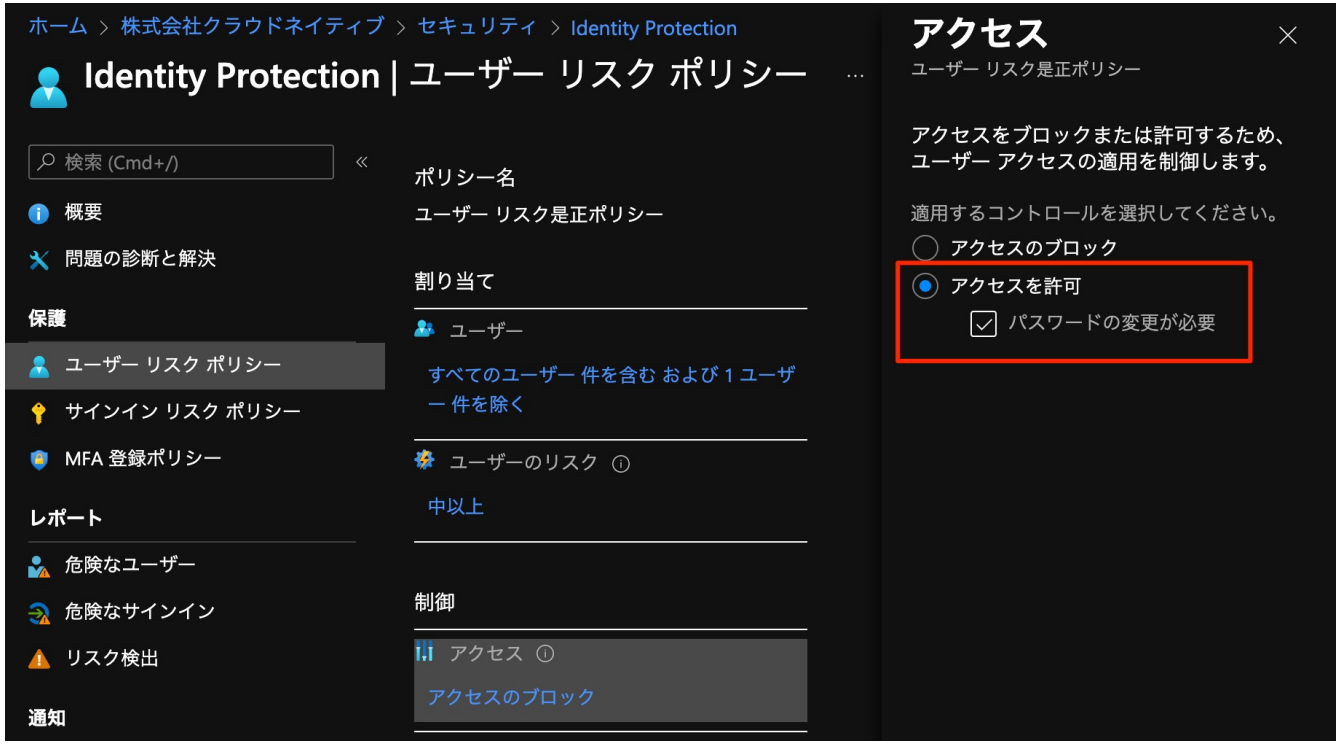
Azure ADの継続的アクセス評価の機能が欲しい

- Azure ADの継続的アクセス評価とは？
  - クライアント/ユーザーの状態の変化に応じて、ほぼリアルタイムにアクセスの失効や条件付きアクセスポリシーの評価を行う。
  - ゼロトラストの思想に合致した機能
  - Exchange、Teams、SharePoint Online等、MS製品がメイン

- Oktaもできるようになると嬉しい！
  - Okta Identity Engineの追加アップデートに期待してます！

ユーザのリスクポリシーが欲しい

- Azure ADはパスワード漏洩等のユーザのリスク状態によって、ユーザにパスワード変更の要求ができる。
- Oktaにもこの機能が欲しいです！



ライセンスわかりにくい問題

- これはAzure ADとOktaのどっちも当てはまります。
- Oktaはどのライセンスにどの機能が紐づいてるかわからない。。
  - Okta社公式で対応表を出してくれるとすごい嬉しいです！
- Azure ADはAzure AD Premium P1 or P2やEMSライセンスの範囲ではギリギリわかります。
  - が、Windows EnterpriseやOffice系、Sec E5等範囲を広げると、どのライセンスでどの機能が使えるかわからない。。

クラウドネイティブ
CLOUD NATIVE INC.

1. はじめに
2. Oktaのよいところ
3. Oktaのこれからなところ
4. まとめ

まとめ

- SSOやプロビジョニングなど一般的にIdPに求められる要件は、OktaでもAzure ADでもできる。
- 利便性重視、色々なSaaSと掛け合わせたいならOktaが良い。
- Microsoftの製品を多く使っている/使う予定である、セキュリティ重視でいきたいならAzure ADが良い。
- Okta Identity Engineが来たら形勢が変わるかも！

クラウドネイティブ
CLOUD NATIVE INC.

https://cloudnative.co.jp

ITの世界だからこそ、人と人とのコミュニケーションを最重要視し、
全員が前を向いて楽しく仕事を進められる世界を作るのが最大のミッションです。

お問い合わせはこちら →

株式会社クラウドネイティブ
Cloud Native Inc.
設立：2017年5月
所在地：〒106-0032 東京都港区六本木1-4-5
アークヒルズサウスタワー 16F
代表電話番号：050-1744-0150
Eメールアドレス：info@cloudnative.co.jp

Thank you !!