Identity and access

10 minutes

Network perimeters, firewalls, and physical access controls used to be the primary protection for corporate data. But netw perimeters have become increasingly porous with the explosion of bring your own device (BYOD), mobile apps, and clouc applications.

Identity has become the new primary security boundary. Therefore, proper authentication and assignment of privileges is maintaining control of your data.

Your company, Contoso Shipping, is focused on addressing these concerns right away. Your team's new hybrid cloud solu needs to account for mobile apps that have access to secret data when an authorized user is signed in — in addition to h shipping vehicles constantly send a stream of telemetry data that is critical to optimizing the company's business.

Authentication and authorization

Two fundamental concepts that need to be understood when talking about identity and access control are authenticatior authorization. They underpin everything else that happens and occur sequentially in any identity and access process:

- *Authentication* is the process of establishing the identity of a person or service looking to access a resource. It invol of challenging a party for legitimate credentials, and provides the basis for creating a security principal for identity a control use. It establishes if they are who they say they are.
- *Authorization* is the process of establishing what level of access an authenticated person or service has. It specifies v they're allowed to access and what they can do with it.

> **Note**
>
> Authentication is sometimes shortened to *AuthN*, and authorization is sometimes shortened to *AuthZ*.

Azure provides services to manage both authentication and authorization through Azure Active Directory (Azure AD).

What is Azure Active Directory?

Azure AD is a cloud-based identity service. It has built in support for synchronizing with your existing on-premises Active or can be used stand-alone. This means that all your applications, whether on-premises, in the cloud (including Office 365 mobile can share the same credentials. Administrators and developers can control access to internal and external data an applications using centralized rules and policies configured in Azure AD.

Azure AD provides services such as:

- **Authentication.** This includes verifying identity to access applications and resources, and providing functionality su service password reset, multi-factor authentication (MFA), a custom banned password list, and smart lockout service

- **Application management.** You can manage your cloud and on-premises apps using Azure AD Application Proxy, S My apps portal (also referred to as Access panel), and SaaS apps.
- **Business to business (B2B) identity services.** Manage your guest users and external partners while maintaining co your own corporate data
- **Business-to-Customer (B2C) identity services.** Customize and control how users sign up, sign in, and manage the when using your apps with services.
- **Device Management.** Manage how your cloud or on-premises devices access your corporate data.

Let's explore a few of these in more detail.

Single sign-on

The more identities a user has to manage, the greater the risk of a credential-related security incident. More identities me passwords to remember and change. Password policies can vary between applications and, as complexity requirements in becomes increasingly difficult for users to remember them.

Now, consider the logistics of managing all those identities. Additional strain is placed on help desks as they deal with ac lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring the disabled can be challenging. If an identity is overlooked, this could allow access when it should have been eliminated.

With single sign-on (SSO), users need to remember only one ID and one password. Access across applications is granted identity tied to a user, simplifying the security model. As users change roles or leave an organization, access modification to the single identity, greatly reducing the effort needed to change or disable accounts. Using single sign-on for accounts it easier for users to manage their identities and will increase the security capabilities in your environment.

SSO with Azure Active Directory

By leveraging Azure AD for SSO you'll also have the ability to combine multiple data sources into an intelligent security g security graph enables the ability to provide threat analysis and real-time identity protection to all accounts in Azure AD, accounts that are synchronized from your on-premises AD. By using a centralized identity provider, you'll have centralize security controls, reporting, alerting, and administration of your identity infrastructure.

As Contoso Shipping integrates its existing Active Directory instance with Azure AD, you will make controlling access con across the organization. Doing so will also greatly simplify the ability to sign into email and Office 365 documents withou to reauthenticate.

Multi-factor authentication

Multi-factor authentication (MFA) provides additional security for your identities by requiring two or more elements for f authentication. These elements fall into three categories:

Something you know would be a password or the answer to a security question. **Something you possess** could be a m that receives a notification or a token-generating device. **Something you are** is typically some sort of biometric property fingerprint or face scan used on many mobile devices.

Using MFA increases security of your identity by limiting the impact of credential exposure. An attacker who has a user's would also need to have possession of their phone or their security token generator in order to fully authenticate. Authen with only a single factor verified is insufficient, and the attacker would be unable to use only those credentials to authent benefits this brings to security are huge, and we can't emphasize enough the importance of enabling MFA wherever poss

Azure AD has MFA capabilities built in and will integrate with other third-party MFA providers. MFA should be used for u Global Administrator role in Azure AD, because these are highly sensitive accounts. All other accounts can also have MFA

For Contoso Shipping, you decide to enable MFA any time a user is signing in from a non-domain-connected computer - includes the mobile apps your drivers use.

Providing identities to services

It's usually valuable for services to have identities. Often, and against best practices, credential information is embedded i configuration files. With no security around these configuration files, anyone with access to the systems or repositories ca these credentials and risk exposure.

Azure AD addresses this problem through two methods: service principals and managed identities for Azure services.

Service principals

To understand service principals, it's useful to first understand the words **identity** and **principal**, because of how they are the identity management world.

An **identity** is just a thing that can be authenticated. Obviously, this includes users with a user name and password, but it include applications or other servers, which might authenticate with secret keys or certificates.

A **principal** is an identity acting with certain roles or claims. Usually, it is not useful to consider identity and principal sepa think of using 'sudo' on a Bash prompt in Linux or on Windows using "run as Administrator." In both those cases, you are logged in as the same identity as before, but you've changed the role under which you are executing. Groups are often al considered principals because they can have rights assigned.

A **service principal** is an identity that is used by a service or application. And like other identities, it can be assigned roles

Managed identities for Azure services

The creation of service principals can be a tedious process, and there are a lot of touch points that can make maintaining difficult. Managed identities for Azure services are much easier and will do most of the work for you.

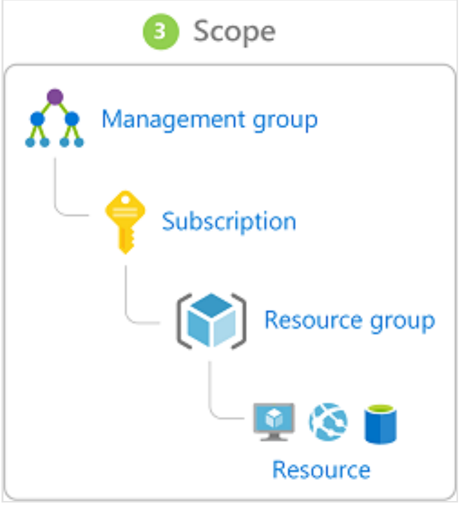
A managed identity can be instantly created for any Azure service that supports it—and the list is constantly growing. Wh create a managed identity for a service, you are creating an account on your organization's Active Directory (a specific organization's Active Directory instance is known as an "Active Directory Tenant"). The Azure infrastructure will automatic care of authenticating the service and managing the account. You can then use that account like any other Azure AD acco including allowing the authenticated service secure access of other Azure resources.

Role-based access control

Roles are sets of permissions, like "Read-only" or "Contributor", that users can be granted to access an Azure service insta

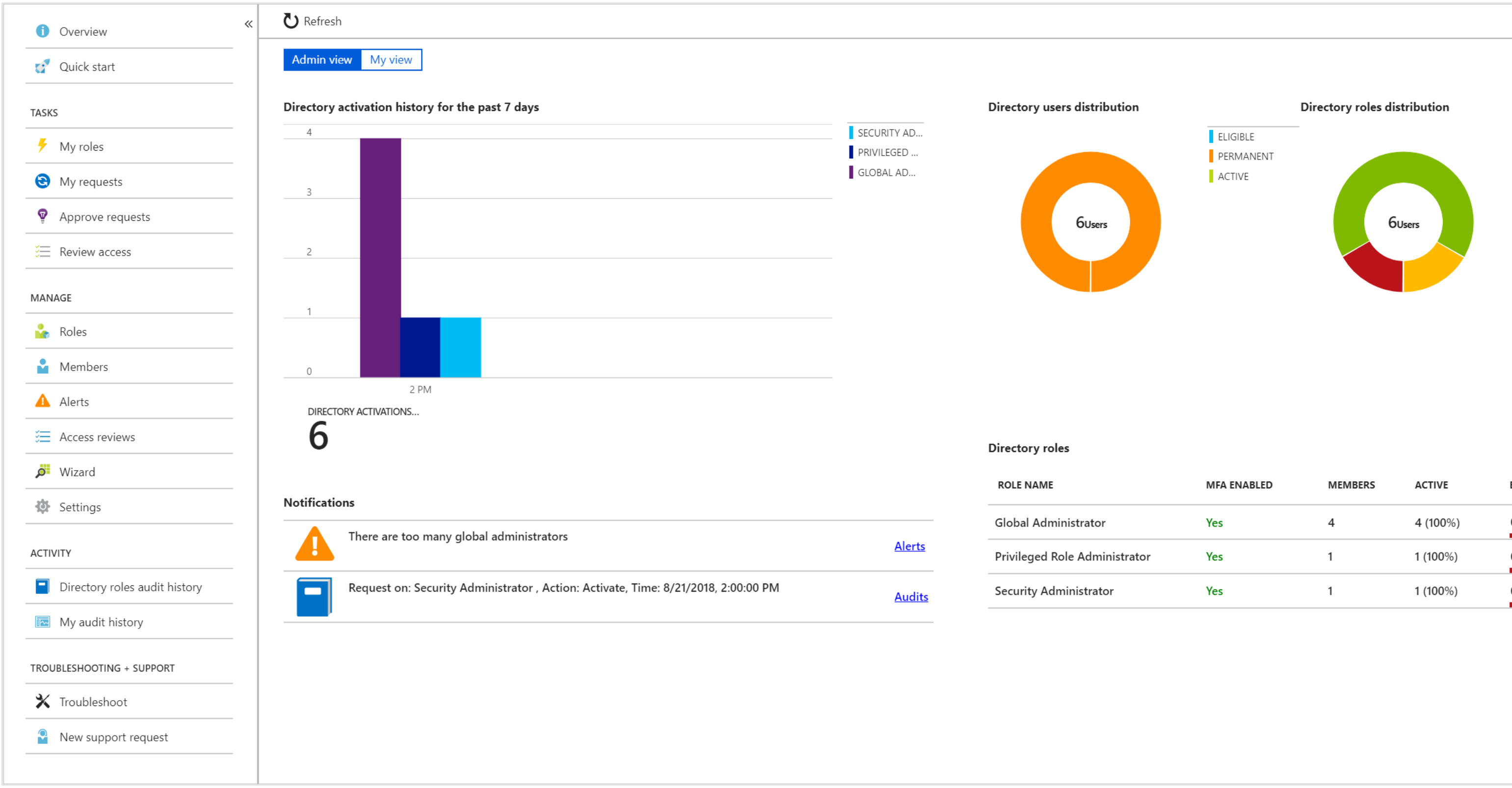
Roles can be granted at the individual service instance level, but they also flow down the Azure Resource Manager hierar

Here's a diagram that shows this relationship. Roles assigned at a higher scope, like an entire subscription, are inherited b scopes, like service instances.



Privileged Identity Management

In addition to managing Azure resource access with role-based access control (RBAC), a comprehensive approach to infra protection should consider including the ongoing auditing of role members as their organization changes and evolves. A Privileged Identity Management (PIM) is an additional, paid-for offering that provides oversight of role assignments, self- and just-in-time role activation and Azure AD and Azure resource access reviews.



Notifications

There are too many global administrators — Alerts

Request on: Security Administrator , Action: Activate, Time: 8/21/2018, 2:00:00 PM — Audits

Directory roles

ROLE NAME	MFA ENABLED	MEMBERS	ACTIVE
Global Administrator	Yes	4	4 (100%)
Privileged Role Administrator	Yes	1	1 (100%)
Security Administrator	Yes	1	1 (100%)

based access configuration, we can always be sure who has the ability to see and manipulate our data and infrastructure.

Next unit: Encryption

Continue >