


# Examples of implementing Azure enterprise scaffold

01/03/2017 • 9 minutes to read • Contributors 

## In this article

[Background](#)

[Scenario 1: line-of-business application](#)

[Scenario 2: customer-facing app](#)

[Next steps](#)

This article provides examples of how an enterprise can implement the recommendations for an [Azure enterprise scaffold](#). It uses a fictional company named Contoso to illustrate best practices for common scenarios.

## Background

Contoso is a worldwide company that provides supply chain solutions for customers. They provide everything from a software as a service model to a packaged model deployed on-premises. They develop software across the globe with significant development centers in India, the United States, and Canada.

The ISV portion of the company is divided into several independent business units that manage products in a significant business. Each business unit has its own developers, product managers, and architects.

The Enterprise Technology Services (ETS) business unit provides centralized IT capability and manages several datacenters where business units host their applications. Along with managing the datacenters, the ETS organization provides and manages centralized collaboration (such as email and websites) and network/telephony services. They also manage customer-facing workloads for smaller business units who don't have operational staff.

The following personas are used in this article:

- Dave is the ETS Azure administrator.
- Alice is Contoso's Director of Development in the supply chain business unit.

Contoso needs to build a line-of-business app and a customer-facing app. It has decided to run the apps on Azure. Dave reads the [prescriptive subscription governance](#) article and is ready to implement the recommendations.

## Scenario 1: line-of-business application

Contoso is building a source code management system (BitBucket) to be used by developers across the world. The application uses infrastructure as a service (IaaS) for hosting and consists of web servers and a database server. Developers access servers in their development environments, but they don't need access to the servers in Azure. Contoso ETS wants to allow the application owner and team to manage the application. The application is only available while on Contoso's corporate network. Dave needs to set up the subscription for this application. The subscription will also host other developer-related software in the future.

### Naming standards and resource groups

Dave creates a subscription to support developer tools that are common across all the business units. Dave needs to create meaningful names for the subscription and resource groups (for the application and the networks). He creates the following subscription and resource groups:

Item	Name	Description
Subscription	Contoso ETS DeveloperTools Production	Supports common developer tools
Resource Group	bitbucket-prod-rg	Contains the application web server and database server
Resource Group	corenetworks-prod-rg	Contains the virtual networks and site-to-site gateway connection

## Role-based access control

After creating his subscription, Dave wants to ensure that the appropriate teams and application owners can access their resources. Dave recognizes that each team has different requirements. He uses the groups that have been synchronized from Contoso's on-premises Active Directory to Azure Active Directory and provides the right level of access to the teams.

Dave assigns the following roles for the subscription:

Role	Assigned to	Description
<a href="#">Owner</a>	Managed ID from Contoso's on-premises Active Directory	This ID is controlled with just-in-time (JIT) access through Contoso's Identity Management tool and ensures that subscription owner access is fully audited
<a href="#">Security Reader</a>	Security and risk management department	This role allows users to look at the Azure Security Center and the status of the resources
<a href="#">Network Contributor</a>	Network team	This role allows Contoso's network team to manage the Site to Site VPN and the Virtual Networks
<i>Custom role</i>	Application owner	Dave creates a role that grants the ability to modify resources within the resource group. For more information, see <a href="#">Custom roles in Azure RBAC</a>

## Policies

Dave has the following requirements for managing resources in the subscription:

- Because the development tools support developers across the world, he doesn't want to block users from creating resources in any region. However, he needs to know where resources are created.
- He is concerned with costs. Therefore, he wants to prevent application owners from creating unnecessarily expensive virtual machines.
- Because this application serves developers in many business units, he wants to tag each resource with the business unit and application owner. By using these tags, ETS can bill the appropriate teams.

He creates the following policies via [Azure Policy](#):

Field	Effect	Description
location	audit	Audit the creation of the resources in any region
type	deny	Deny creation of G-Series virtual machines
tags	deny	Require application owner tag

Field	Effect	Description
tags	deny	Require cost center tag
tags	append	Append tag name <b>BusinessUnit</b> and tag value <b>ETS</b> to all resources

## Resource tags

Dave understands that he needs to have specific information on the bill to identify the cost center for the BitBucket implementation. Additionally, Dave wants to know all the resources that ETS owns.

He adds the following [tags](#) to the resource groups and resources.

Tag name	Tag value
ApplicationOwner	The name of the person who manages this application
CostCenter	The cost center of the group that is paying for the Azure consumption
BusinessUnit	<b>ETS</b> (the business unit associated with the subscription)

## Core network

The Contoso ETS information security and risk management team reviews Dave's proposed plan to move the application to Azure. They want to ensure that the application isn't exposed to the internet. Dave also has developer apps that in the future will be moved to Azure. These apps require public interfaces. To meet these requirements, he provides both internal and external virtual networks, and a network security group to restrict access.

He creates the following resources:

Resource type	Name	Description
Virtual Network	internal-vnet	Used with the BitBucket application and is connected via ExpressRoute to Contoso's corporate network. A subnet ( <code>bitbucket</code> ) provides the application with a specific IP address space
Virtual Network	external-vnet	Available for future applications that require public-facing endpoints
Network Security Group	bitbucket-nsg	Ensures that the attack surface of this workload is minimized by allowing connections only on port 443 for the subnet where the application lives ( <code>bitbucket</code> )

## Resource locks

Dave recognizes that the connectivity from Contoso's corporate network to the internal virtual network must be protected from any wayward script or accidental deletion.

He creates the following [resource lock](#):

Lock type	Resource	Description
CanNotDelete	internal-vnet	Prevents users from deleting the virtual network or subnets, but does not prevent the addition of new subnets

## Azure Automation

Dave has nothing to automate for this application. Although he created an Azure Automation account, he won't initially use it.

### Azure Security Center

Contoso IT service management needs to quickly identify and handle threats. They also want to understand what problems may exist.

To fulfill these requirements, Dave enables the [Azure Security Center](#) and provides access to the Security Reader role.

## Scenario 2: customer-facing app

The business leadership in the supply chain business unit has identified various opportunities to increase engagement with Contoso's customers by using a loyalty card. Alice's team must create this application and decides that Azure increases their ability to meet the business need. Alice works with Dave from ETS to configure two subscriptions for developing and operating this application.

### Azure subscriptions

Dave logs into the Azure Enterprise Portal and sees that the supply chain department already exists. However, as this project is the first development project for the supply chain team in Azure, Dave recognizes the need for a new account for Alice's development team. He creates the "R&D" account for her team and assigns access to Alice. Alice logs in via the Azure portal and creates two subscriptions: one to hold the development servers and one to hold the production servers. She follows the previously established naming standards when creating the following subscriptions:

Subscription use	Name
Development	Contoso SupplyChain ResearchDevelopment LoyaltyCard Development
Production	Contoso SupplyChain Operations LoyaltyCard Production

### Policies

Dave and Alice discuss the application and identify that this application only serves customers in the North American region. Alice and her team plan to use Azure's Application Service Environment and Azure SQL to create the application. They may need to create virtual machines during development. Alice wants to ensure that her developers have the resources they need to explore and examine problems without pulling in ETS.

For the **development subscription**, they create the following policy:

Field	Effect	Description
location	audit	Audit the creation of the resources in any region

They don't limit the type of SKU a user can create in development, and they don't require tags for any resource groups or resources.

For the **production subscription**, they create the following policies:

Field	Effect	Description
location	deny	Deny the creation of any resources outside of the US datacenters
tags	deny	Require application owner tag
tags	deny	Require department tag

Field	Effect	Description
tags	append	Append tag to each resource group that indicates production environment

They don't limit the type of SKU a user can create in production.

## Resource tags

Dave understands that he needs to have specific information to identify the correct business groups for billing and ownership. He defines resource tags for resource groups and resources.

Tag name	Tag value
ApplicationOwner	The name of the person who manages this application
Department	The cost center of the group that is paying for the Azure consumption
EnvironmentType	<b>Production</b> (Even though the subscription includes <b>Production</b> in the name, including this tag enables easy identification when looking at resources in the portal or on the bill)

## Core networks

The Contoso ETS information security and risk management team reviews Dave's proposed plan to move the application to Azure. They want to ensure that the Loyalty Card application is properly isolated and protected in a DMZ network. To fulfill this requirement, Dave and Alice create an external virtual network and a network security group to isolate the Loyalty Card application from the Contoso corporate network.

For the **development subscription**, they create:

Resource type	Name	Description
Virtual Network	internal-vnet	Serves the Contoso Loyalty Card development environment and is connected via ExpressRoute to Contoso's corporate network

For the **production subscription**, they create:

Resource type	Name	Description
Virtual Network	external-vnet	Hosts the Loyalty Card application and is not connected directly to Contoso's ExpressRoute. Code is pushed via their Source Code system directly to the PaaS services.
Network Security Group	loyaltycard-nsg	Ensures that the attack surface of this workload is minimized by only allowing in-bound communication on TCP 443. Contoso is also investigating using a web application firewall for additional protection.

## Resource locks

Dave and Alice confer and decide to add resource locks on some of the key resources in the environment to prevent accidental deletion during an errant code push.

They create the following lock:

Lock type	Resource	Description
-----------	----------	-------------

Lock type	Resource	Description
CanNotDelete	external-vnet	To prevent people from deleting the virtual network or subnets. The lock does not prevent the addition of new subnets

## Azure Automation

Alice and her development team have extensive runbooks to manage the environment for this application. The runbooks allow for the addition/deletion of nodes for the application and other DevOps tasks.

To use these runbooks, they enable [Automation](#).

## Azure Security Center

Contoso IT service management needs to quickly identify and handle threats. They also want to understand what problems may exist.

To fulfill these requirements, Dave enables Azure Security Center. He ensures that the Azure Security Center is monitoring the resources and provides access to the DevOps and security teams.

## Next steps

- To learn about creating Resource Manager templates, see [Best practices for creating Azure Resource Manager templates](#).