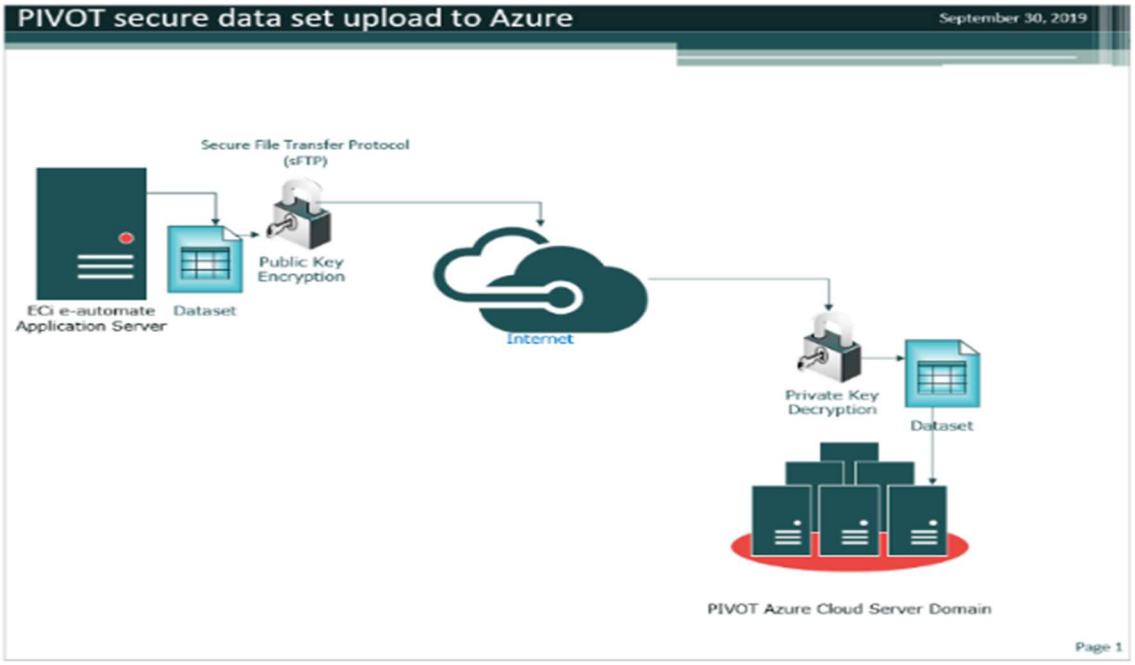
PIVOT Data Integration Tool Functionality

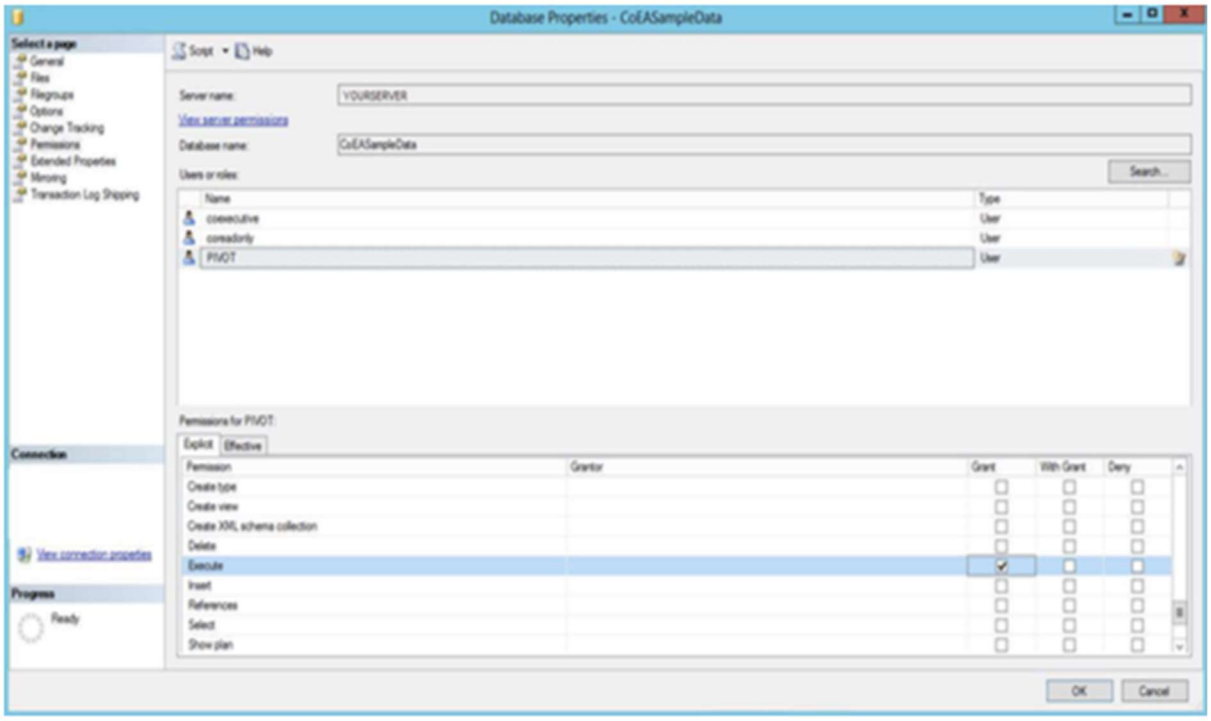
The PIVOT on premise data integration tool is built as a Windows 32-bit application to create specific data sets from your e-automate database. Utilizing Secure File Transfer Protocol (sFTP), data sets are automatically uploaded to the PIVOT cloud servers hosted on Microsoft Azure. After datasets are uploaded the PIVOT data integration monitoring process initiates the data merge on all data sets. Server requirements for the PIVOT data integration tools match up to the specification of ECi's e-automate applications prerequisites.

The PIVOT data integration tool was intended to be installed on a Windows e-automate application server. Our tools utilize the built-in function of Microsoft PowerShell. PowerShell is the default in the Windows Server installation process. This Windows feature is required and needs to be installed if the default installation process was modified.



During the installation of the PIVOT on-premise application you will notice the setup of Microsoft Task Scheduler will need to be completed by your Network Administrator. This is to allow the PIVOT application to send your e-automate data sets on a regular schedule. It is necessary to provide a Windows local account or Windows Active Directory account and credentials with local rights to run scheduled tasks. This account doesn't need to be an Administrator or Domain Administrator account type. This will allow Task Scheduler to run in background utilizing the "Run whether user is logged on or not" function.

PIVOT Data Integration Tool Functionality, con't.



This data integration tool application accesses SQL data by sending a standard query to the host server. The creation of a SQL Server user account and password is required to embed the SQL credentials into the PIVOT data integration tool, which will allow the automatic processing of data sets. Many of the data analytics require both SQL queries and SQL stored procedures and the execute permission within the database properties must be granted within the SQL Server Management Studio.

3 reasons why Azure's infrastructure is secure

With the challenges of recruiting security experts to maintain secure infrastructure, there is not a clear return on investment. To keep pace in this ever-changing security landscape, it's important that they can protect their infrastructure while also lowering their costs and reducing complexity. Azure in uniquely positioned to help with these challenges.

Microsoft Azure provides a secure foundation across physical, infrastructure, and operational security. Customers like Smithfield and Merrill Corporation choose Azure to be their trusted cloud due to its platform security. Microsoft invests over a billion dollars every year into security, including the security of the Azure platform, so that your data and business assets can be protected.

A few months ago, we started an Azure security blog series with a blog on our layered approach to physical security. We shared the 3 ways that Azure improves your security at the RSA conference. Today, we will discuss the network infrastructure, firmware and hardware, and continuous testing and monitoring that make up Azure's secure infrastructure. At the end of this blog, we will discuss some of the security services you can use to further secure your network.

1. Secure network infrastructure

Adopting cloud helps you reduce infrastructure costs while scaling resources and being agile. Even though the network is shared, Microsoft has several mechanisms in place to ensure Azure's network and our customers' networks remain segregated and secure.

Management (Microsoft-managed) networks and customer networks are isolated in Azure to improve performance and ensure the traffic moving through the platform is secure. The management networks are managed by Microsoft and are only available for devices and administrators to connect to Azure. When devices or administrators want to connect to Azure, controls such as just-in-time access and privileged access workstations limit accessibility to help ensure unauthorized individuals do not gain access to the Azure network. In addition, network cabling, the equipment to support and secure the network, and the integration of systems for monitoring the network are managed by Microsoft.

The customer networks are segregated from management networks to protect them from attacks targeting management networks. Customer networks are separated from each other using networking virtualization methods, so customers cannot gain access to other customers' networks.

Data on the Azure platform is always encrypted in transit, except for data that moves within customer controlled networks (such as Azure Virtual Networks and ExpressRoute). It is the responsibility of the customer to encrypt data within a network that he or she controls.

Azure's secure network also has built-in mechanisms to protect against distributed denial-of-service (DDoS) attacks. DDoS attacks try to disrupt access to services by generating so much traffic that it exceeds capacity. DDoS protections are built into the Azure platform to help ensure attacks do not bring down our services. These protections continuously monitor traffic and use scrubbers and customer traffic profiling to detect and then deflect these attacks. Microsoft's experience safeguarding some of the largest services on the Internet, such as Xbox and O365, gives us the ability to scale protection from attacks.

Microsoft isolates networks, ensures the confidentiality of data, and actively works to combat against DDoS attacks so that you can reallocate datacenter security resources into another area in your enterprise.

2. Secure hardware and firmware

Security controls are integrated into the firmware and hardware of Azure to ensure its secure by default and continues to be secure throughout its lifetime.

Microsoft recently announced Project Cerberus to ensure the security of our firmware. Cerberus is a microcontroller, a chip made up of CPU, memory, and programmable input/output, that protects against unauthorized access and malicious updates. The microcontroller also makes it possible to secure the pre-boot, boot-time, and runtime integrity of the firmware. Our hardware has access to the boot environment before the OS loads to ensure malicious code is detected and stopped. Our firmware goes through regular code reviews. We monitor the security of the hardware and firmware to ensure that any threats are detected and mitigated before it can impact your business.

One of our most recent advancements in hardware is confidential computing, which uses Hyper-V and Intel SGX chip-enabled servers to segregate execution and data from the underlying operation system and operators. Azure can encrypt data in use, in transit, and at rest. Azure is the first cloud platform to support both software and hardware-based Trusted Execution Environments (TEEs). Trusted Execution Environments are a portion of memory on a server where customer

data is stored. Only systems have access to it to prevent unauthorized administrators or processes from gaining access to this data.

3. Secure testing and monitoring

Microsoft has over 3,500 cybersecurity experts who work on your behalf 24x7x365. This number includes over 200 professionals who identify potential vulnerabilities through red and blue team exercises. The red team tries to compromise Azure's infrastructure, and the blue team defends against attacks made by the red team. At the end of each red and blue team exercise, the team codifies what they've learned into the Azure operational security process, so the team becomes more effective at continuous detection and response.

Microsoft employs cybersecurity experts to protect your infrastructure, so your resources can be available for other business initiatives.

We've just discussed the ways that Microsoft can help secure Azure's infrastructure. However, there are services for your network that you will still be responsible for setting up in Azure. For example, the same way you need to configure network access controls, load balancers, or network virtual appliances on-premises, you will need to do this in Azure. A service called Azure ExpressRoute helps you establish a secure connection from your on-premises environment to Azure.

In addition to taking advantage of the basic DDoS protections automatically enabled in the platform, you can use a new service, Azure DDoS Protection Standard, for further protection against layer 3-7 attacks. For example, it can protect against volumetric attacks like UDP floods, amplification floods, or attacks that target IPv4 and IPv6. Layer 3 and Layer 4 attacks are detected and are sent to the scrubbers. Scrubbers determine if the traffic is malicious or not and if it's safe to travel through the network. At Layer 7, we can protect against attacks targeting HTTP and SQL protocols.

Microsoft's scale of investments across infrastructure, hardware, and experts are unparalleled. Microsoft provides a secure infrastructure for our datacenters, composed of segregated networks, well-maintained hardware and firmware, and industry-leading operational security processes so that you can have more resources available to deliver business value.