VMware Sovereign Cloud Technical Guidance for VMware Cloud Provider Partners
# Table of Contents

**Introduction** ......................................................................................................................... 4
  - *Legal Disclaimer* .................................................................................................................. 4
  - *Audience* ............................................................................................................................. 4
  - *Scope* .................................................................................................................................. 5

**What is a VMware Sovereign Cloud?** .................................................................................. 6
  - *VMware Sovereign Cloud Terminology* ................................................................................ 6
  - *VMware Security Domains* .................................................................................................. 7

**Interoperability Stack (Bill of Materials)** ........................................................................... 8

**Security and Compliance Guidance** .................................................................................... 8

**Governance, Risk, and Compliance Mapping** ........................................................................ 9

**VMware Sovereign Cloud Criteria** ........................................................................................ 10

**Data Sovereignty and Jurisdictional Control** ........................................................................ 10

**Data Access and Integrity** ....................................................................................................... 10
  - *Data Centers* ....................................................................................................................... 11
  - *Storage options* ................................................................................................................. 11
  - *Backup* ............................................................................................................................... 12
  - *Disaster Recovery (DR)* ...................................................................................................... 13
  - *Data Replication* .................................................................................................................. 13
  - *Network Connectivity Options* ............................................................................................. 13

**Data Security & Compliance** .................................................................................................. 15
  - *Security Controls* ................................................................................................................ 15
  - *Data and Environment Auditing* .......................................................................................... 17
  - *Zero Trust Security Posture* ................................................................................................ 18
  - *Optional Additions for further Zero Trust Security* ................................................................. 19
  - *Encryption* .......................................................................................................................... 20
  - *Catalog of Hardened and Trusted images* ............................................................................ 21
  - *Infrastructure isolation “air-gapped”* .................................................................................... 23
  - *Data Access Controls* .......................................................................................................... 23
  - *Role-based Access Control (RBAC)* ...................................................................................... 24
  - *Attribute-based Access Control (ABAC)* .............................................................................. 25
Data Independence and Interoperability ................................................................. 26
  Prevention of Cloud Vendor Lock-in ............................................................... 26
  Application Portability and Independence ...................................................... 26
  Ability to support and manage hybrid cloud .................................................. 30

Next Steps .......................................................................................................... 30
  Operationalization ......................................................................................... 30
Introduction
The VMware Sovereign Cloud Technical Guidance for VMware Cloud Provider Partners is a technical reference point for deploying all components needed to build and maintain a VMware Sovereign Cloud. The intent of the technical guidance is to document a verified stack along with other components that will define a technical approach to building a Sovereign Cloud.

VMware’s Sovereign Cloud Initiative recognizes VMware Cloud Verified partners that meet VMware’s definition of a Sovereign Cloud. Partners who implement the VMware Sovereign Cloud guidance will be better able to protect the sovereignty of their customers workloads and data.

While the definition of what a Sovereign Cloud is, continues to evolve and is truly based on the Sovereign Nation or entity where the workloads/data/people will reside, technical guidance is needed to make our VMware Cloud Providers successful in serving their customers. This guidance will be flexible enough to allow different configurations and implementations to comply with the entity that is providing the requirements of their Sovereign Cloud.

VMware Cloud Providers benefit from clear guidelines around data sovereignty, data residency, data access, jurisdiction, control, and much more to provide customers with the assurance that their most sensitive data is managed securely. With sovereign cloud capabilities, customers benefit from the scale of a multi-tenant, hybrid cloud environment while maintaining security, access, and control like a traditional on-premises, legacy computing environment.

Legal Disclaimer
This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided “AS IS”. VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Audience
This document is intended for VMware Cloud Provider architects and technical leads responsible for planning and performing the implementation and maintenance of a VMware Sovereign Cloud environment.
Scope
This document addresses the following aspects:

What is a VMware Sovereign Cloud?
The core proposition of a VMware Sovereign Cloud is to provide enforcement of data and workload residency, extend data sovereignty protections beyond the immediate platform where possible and to enable secure, audited connectivity and data transaction between resident, sovereign and non-sovereign data classifications.

Interoperability stack
Provides a list of all the components comprising the software stack. This will be a foundation of the VMware Cloud Verified software stack and a list of other components required to build a VMware Sovereign Cloud.

Note: Versions of the provided software stack should be verified against the VMware Product Interoperability Matrices to ensure compatibility and support. This is the authoritative resource for interoperability between the VMware software components.

Security and Compliance guidance
To align to the VMware Sovereign Cloud definition, a compliant solution must comply with all relevant security guidelines outlined in the product-specific documentation. System administrators and implementation teams for VMware Sovereign Cloud Foundation use the Security and Compliance Configuration Guides for the different components of the stack that make of a VMware Sovereign Cloud to assess and implement user-defined configurations. Default configurations that address compliance are not subject of the configuration guide because they do not require additional configuration. In some cases, default configurations must be evaluated to ensure the default parameter aligns with the policy and procedures of your organization. Guidance for auditors who evaluate a VMware Sovereign Cloud environment can use the references in this guide to evaluate both default and user-defined configurations.

Default configurations
Security configurations based on compliance requirements that are configured by default in VMware Sovereign Cloud. According to the different regulatory requirements, the parameter values might require changes, but by secure design these configurations are included in the current implementation.

User-defined configurations
Additional input by the organization is required to identify, select, and set configurations based on a target regulation.
What is a VMware Sovereign Cloud?
A VMware Sovereign Cloud aims to maintain the sovereignty of data in all possible ways for any entity (country, region, enterprise, government, institution, etc.).

Table 1. Criteria for a VMware Sovereign Cloud

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Data Sovereignty and Jurisdictional Control   | • Data should reside locally  
• The cloud should be managed and governed locally, all data processing – including API calls – should happen within the country/geography  
• The data should be accessible only to residents of the same country, and the data should not be accessible under foreign laws or from any outside geography.  
• Enforcement of data and workload residency  
• Extend data sovereignty protections beyond the immediate platform where possible and to enable secure, audited connectivity and data transaction between resident, sovereign and non-sovereign data classifications. |
| Data Access and Integrity                     | • Two data center locations  
• Backup services, Disaster Recovery, Micro Segmentation, and multiple storage options are required |
| Data Security and Compliance                  | • Security Controls  
• Relevant industry or governmental certifications  
• Zero Trust Security  
• Encryption |
| Data Independence and Interoperability        | • Workload migration with bi-directional workload portability  
• Modern Application architecture using Containers  
• Support for hybrid cloud deployments |

VMware Sovereign Cloud Terminology
Here are some terms that are specific to Sovereign Cloud that should be understood before determining what is needed in your design.

• **Data residency** - Refers to the physical location in which data is stored and processed, by extension this includes the systems on which that data resides. Controls within a Sovereign Cloud platform over workload placement, data storage and processing ensure that the resident status of the data is always preserved.

• **Data sovereignty** - Refers to data being subject to the laws of the jurisdiction it is collected in. This generally implies that the data is generated within the geography of the jurisdiction and that it will remain there.

• **Data localization** – The process of storing and processing data where it is first collected and to persistently maintain its resident and sovereign status, effectively creating compute and data silos along jurisdictional boundaries.

• **Security domains** - A security domain is a conceptual grouping of systems, network connections, supporting infrastructure, people, and operation processes that fall within a common security boundary. Security domains typically represent a common authentication and authorization boundary (e.g., an LDAP realm), such that being granted access to one system in a security domain leads to the explicit or implicit granting of access to other systems in that domain. A security domain can represent a network connectivity area with a common security posture with protections located at the domain boundary, security domains can optionally be further subdivided into smaller connectivity areas using subnets and micro-segmentation.
VMware Security Domains
All VMware Sovereign Clouds must include two prescribed security domains: Resident domain and Sovereign domain. These domains encompass both management and workload domains in vSphere as well as all supporting infrastructure and management elements.

Figure 1. Sovereign Cloud Security Domains
Interoperability Stack (Bill of Materials)

The Bill of Materials table lists the defined set of software components for Cloud Providers to implement a VMware Sovereign Cloud. While VMware Cloud Providers are free to choose and pick other versions or different combinations of VMware Cloud Provider Program software products, the specified stack is what defines a VMware Sovereign Cloud.

Table 1. Bill Of Materials

<table>
<thead>
<tr>
<th>Component</th>
<th>Version and Build</th>
<th>Core/Optional</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Cloud Verified Certification</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware Cloud Foundation™</td>
<td>Enterprise</td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware NSX-T™ Data Center</td>
<td>Advanced or Enterprise</td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>Tanzu Basic</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>Tanzu Greenplum (Tanzu Data Services)</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>Data Management for VMware Tanzu (DMS)</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware Cloud Director™ App Launchpad™</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware Tanzu Application Catalog</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware vCloud® Usage Meter™</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware vSAN™</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware Cloud Director</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
<tr>
<td>VMware Cloud Director Availability</td>
<td></td>
<td>Core</td>
<td></td>
</tr>
</tbody>
</table>

Security and Compliance Guidance

For VMware Sovereign Cloud implementations, a best practice would be to transfer security over to a dedicated team (post-deployment) to augment and monitor the security posture. It is the responsibility of each security, compliance, and audit teams in your organization to verify that configurations meet their compliance requirements. The attack vectors and compliance guidelines are constantly evolving, which requires constant monitoring and risk management processes.

It is important to note that the VMware Sovereign Cloud security guidance is not enough on its own. Each organization needs to assess their own risk posture and identify applicable controls using a series of supporting security architecture, technology, processes, and people to evaluate the environment.

Super users of the system inherit various technologies and typically work with security specialists to implement controls effectively. VMware Sovereign Cloud deployments benefit from post-implementation security health checks to enhance the organizations security posture as it relates to the requirements of the sovereign entity where the VMware Sovereign Cloud resides.
Governance, Risk, and Compliance Mapping
This guidance describes the security configurations that can support Governance, Risk, and Compliance (GRC) considerations. Due to the variety of compliance standards and different organizational business needs, due care should be taken to identify and map VMware Sovereign Cloud configurations against a targeted regulation.

Organizations expect to keep data safe. They must often comply with one or more regulations from government standards to private standards such as:

- National Institute of Standards and Technology (NIST)
- Federal Risk and Authorization Management Program (FedRAMP)
- Payment Card Industry (PCI)
- International Organization for Standardization number 27001 (ISO27001)
- International Organization for Standardization number 27032 (ISO27032)
- British Standards Institution (BSI)
- Internet Engineering Task Force (IETF)

Security Versus Compliance
The VMware Sovereign Cloud approaches security and compliance concepts in a practical manner. Security supported by the VMware Sovereign Cloud reduces the risk of data theft, cyber-attack, or unauthorized access. While compliance is the proof that a security control is in place, typically within a defined timeline. Security and compliance work with a broader set of considerations including people, processes, and technology. Security is primarily outlined in the design decisions and highlighted within the technology configurations. Compliance is focused on mapping the correlation between security controls and specific requirements. A compliance mapping provides a centralized view to list out many of the required security controls. Those controls are further detailed by including each security control’s respective compliance citations as dictated by a domain such as NIST, PCI, FedRAMP, HIPAA, and so forth.
VMware Sovereign Cloud Criteria
This section provides architectural and design guidance that will allow a Verified Cloud Provider to determine or classify a VMware Sovereign Cloud implementation. It is important to continually review the criteria that defines what a Sovereign Cloud is as the requirements that you need to meet are constantly evolving.

The following main criteria and their implementation will be reviewed in this technical whitepaper:

- **Data sovereignty and jurisdictional control**
- **Data access and integrity**
- **Data security and compliance**
- **Data independence and interoperability**

Data Sovereignty and Jurisdictional Control
Ensuring data sovereignty and jurisdictional control requires both logical and physical design considerations specific to the Sovereign Entity that is dictating the regulations and standards for their Sovereign Cloud. The general requirement is to make sure that all data is resident within the physical boundaries of the Sovereign territory where the Sovereign Cloud has been implemented.

Therefore, the data remains subject to the exclusive jurisdictional control and authority of the governmental bodies in the sovereign territory where the data was collected. Foreign governmental bodies or legal entities located outside the sovereign territory are unable to assert any jurisdiction or authority over any part of the data that resides in the Sovereign Cloud.

Data Access and Integrity
Being able to access the data in a VMware Sovereign Cloud needs to be secure, redundant, and reliable. It is crucial to make sure that your VMware Sovereign Cloud is available to your customers so they can access their data quickly and securely. As a cloud provider you will want to consider the following topics in your design criteria: Data Centers, Storage, Backup, Disaster and Recovery (DR), Data Center Connectivity, and Secure Networking.
Data Centers
A VMware Sovereign Cloud requires that there be at least two data centers located in the jurisdiction where the data is collected.

The data centers that the Cloud Provider is hosting the VMware Sovereign Cloud from must be at least a Tier III or higher classification for uptime (99.982% availability or higher). If this was a public or commercially hosted environment the Backup, DR, and High Availability configuration could be something stored in a public cloud somewhere. However, in this case because of the issue of Data Access and Integrity in a Sovereign Cloud configuration there needs to be a second location within the Sovereign Security Domain structure that provides these services.

Deploying VMware Cloud Foundation in two different locations can be managed from a single SDDC Manager Console, see Multi-Instance Management for more information.

If you are deploying VMware Cloud Foundation for your instance of VMware Sovereign Cloud you will want to reference the current VMware Cloud Foundation Compliance Kit in order to secure your environment.

Storage options
It is very important to have flexible and secure storage options. In the case of a VMware Sovereign Cloud, it is a requirement to be able to provide file, block, and object storage for both structured and unstructured data. VMware vSAN is a required component in the VMware Sovereign Cloud configuration. It provides all these storage types (object storage access is accomplished with a 3rd party solution in conjunction with vSAN Direct) and with it comes security and high availability.
You can use [VMware vSAN Documentation](#) to configure your storage environment.

**Note:** VMware vSAN Encryption is discussed later in this guide. However, it is necessary to ensure a secure storage environment for your VMware Sovereign Cloud.

### Backup

Data integrity is vital for Cloud Providers to be successful in supporting customers and in a VMware Sovereign Cloud it is just as important. So having a proper backup strategy is required if you are implementing such a solution. Whatever third-party solution is used to back up the data in a Sovereign Cloud, here are some things to consider in your design.

- **Application backup** - The choice of backup solution(s) will to some extent depend on the applications and platform services that the provider offers to customers, examine the application portfolio being offered to customers and select a backup solution that offers the desired level of application support coverage.

  In addition to offering virtual machine-level backup solutions, it is strongly recommended that application-aware backup solutions are also provided as they generally offer more granular backup and restore capabilities for applications and databases.

  This is useful for rolling back recent transactions while preserving data that was created after a backup was last made, restore operations can also typically be executed non-disruptively as the application can remain online.

- **Hosting of VMware Sovereign Cloud components** - All components in a VMware Sovereign Cloud must be hosted entirely within the local geographical jurisdiction, this extends to backups and remote replications.
• **Immutable storage** - Immutable storage technology ensures that data, once stored, cannot be modified, or deleted. This capability is useful in environments where trust in the integrity of data is of very high importance, typically for compliance and legal reasons. Once the data is stored it becomes a permanent record what cannot be altered by either the data owner or the provider as this is prevented by the technology itself. Note that the concept of immutable storage can apply to primary storage, backup solutions and removeable media, customers may require immutable storage in any of these forms.

**Disaster Recovery (DR)**

Disaster recovery is an essential capability of a cloud hosting platform being used by customers who require Sovereign Cloud services. The nature of the data and applications being hosted and their importance to the nation means that customers will want to recover quickly and reliably in the event of a disaster. Cloud Providers offering a Sovereign Cloud implementation should provide cross-site protection, replication, and fail-over services within the jurisdiction to give their customers the tools they need to achieve their business continuity goals and to preserve sovereign data integrity.

The design of a DR solution in a VMware Sovereign Cloud should consider the different security domains and data classifications that the platform is composed of. This may mean implementing multiple DR solution instances in a single platform to maintain isolation between different security classifications. The replication traffic between sites must be encrypted. The connectivity between the sites should be redundant, take diverse routes, and not depend on any entities that are controlled by foreign entities.

A VMware Sovereign Cloud provides two products that provide DR protection for customer workloads: VMware Cloud Director Availability and VMware Site Recovery Manager (SRM).

**Configuration References**

Please see the following documents for disaster recovery configuration references depending on which product is used.

- Site Recovery Manager for VMware Cloud Foundation
- VMware Cloud Director Availability

**Data Replication**

Data replication functionality is significant for data with certain classifications at the database or application level that has national importance. Cloud Providers can implement replicated storage volumes for the purpose of virtual machine and container persistent storage placement while services such as DBaaS can be configured in clustered or replicated multi-node configurations depending on the database technology involved. However, keep in mind that this data that is replicated should be only replicated in the jurisdiction of the Sovereign Cloud instance and any connectivity to this replicated data should maintain a low latency connection for either synchronous or asynchronous replication which ensures data availability.

**Network Connectivity Options**

Securing network traffic is necessary both within the data center environment in which the platform is hosted as well as for end-to-end connectivity scenarios, a breach of network security at any stage risks invalidating the sovereign status of the data that is hosted on the platform. Consider the following recommendations when designing a VMware Sovereign Cloud:

- **Physical** – All network cables, switches and other network hardware appliances connected to the Sovereign Cloud should be physically secured and made inaccessible to any person who is not specifically authorized to operate the Sovereign Cloud. This physical protection applies within the data center which is already presumed to be secure and where other non-sovereign services are hosted. This also applies to customer and provider owned hardware on which network links are terminating for connectivity into the Sovereign Cloud. All hardware related to the Sovereign Cloud must be isolated in dedicated data halls, cabinets, or cages in their entirety and these must be locked. This approach ensures traceability of actions within the Sovereign Cloud to known and authorized entities. The only network elements that should be exposed to other areas of the data center are uplink connections and devices that link the Sovereign domain of the platform to the outside world.
- **Firewalls** – A VMware Sovereign Cloud will already include edge and distributed firewall capabilities within the platform. The provider will likely include additional firewall appliances, possibly at the insistence of certain customers. As a minimum, the VMware Sovereign Cloud will include an edge firewall in the Sovereign domain which represents the primary ingress/egress point for the entire Sovereign Cloud, an edge firewall in the Resident domain to control traffic flow between the Resident and Sovereign domains and an edge firewall for each tenant virtual data center. Some customers may introduce additional firewall layers using virtual appliances or physical firewall appliances hosted in the provider data center.

- **Micro-segmentation** – NSX-T provides an additional layer of network security with its distributed firewall capability which enables secure micro-segmentation of the workloads. Micro-segmentation provides firewalling capabilities that apply at the interface level, network packets are inspected and filtered as they enter or leave an interface on a virtual machine, providing maximum protection and the ability to enforce zero-trust network environments. Providers and customers can use micro-segmentation to create restrictive scopes of network communication appropriate to their application and apply firewall rules directly to those groups. Micro-segmentation with zero-trust enforcement is a requirement of the Sovereign domain, it ensures that no workload can communicate with another workload without being explicitly allowed by a firewall rule. Zero-trust is a requirement of the Sovereign domain as this is the only domain that allows direct connectivity to external systems and is therefore an attack surface, zero-trust mitigates the risk of lateral attack in the unlikely event of a workload being compromised from outside. Zero-trust is not a requirement of the Resident domain; however, this feature should be available to customers should they decide to implement it.

- **Network isolation** – There are multiple layers of network isolation required in a VMware Sovereign Cloud. Cloud Providers are free to introduce additional isolation if desired. The Resident domain of a VMware Sovereign Cloud is isolated from the outside world, no inbound connections are possible thanks to two layers of edge firewall and a lack of routing to enable access from the outside world (any component or connection that is not in the Resident Domain or a trusted connection in the Sovereign Domain). One useful advantage of this topology is that in the event of a suspected or confirmed attack, the link between the Resident domain which hosts sovereign data and the Sovereign domain where the attack lands can be severed or isolated. Overall application and data isolation is achieved by preventing unrelated applications from communicating with one-another in the Sovereign domain and access to data sources in the Resident domain being constrained only to the appropriate application.

- **Encrypted Network Tunnels (VPNs)** – NSX-T provides IPSEC VPN which allows a Cloud Provider to secure traffic flows between environments.

In that regard, the [NSX-T Data Center 3.1 Security Configuration Guide](#) is essential for a secure VMware Sovereign Cloud.

![Figure 4. Example of a Physical vs Logical Security Separation with NSX](image-url)
Data Security & Compliance

Securing a customer's data and then making sure those security measures remain in compliance with the requirements or criteria of what makes a VMware Sovereign Cloud should be handled by a separate security team in the Cloud Providers organization. This is because it requires constant focus, adjustment, and evolution to stay up to date on the ever-changing landscape that is defining what a Sovereign Cloud is.

The goal of this section is to layout the technical guidance to secure the data of your customer and then make sure it stays compliant with industry standards as well as the governmental entities that are the ruling authority over the implemented Sovereign Cloud.

Security Controls

The foundation of a VMware Sovereign Cloud software stack starts with VMware Cloud Foundation. The following security concepts are treated as guiding principles to develop a secure VMware Cloud Foundation environment that leverages capabilities available across all products. These principles do not only result in the configurations identified in this guidance but are also inherent in product capabilities. Please refer to the Sovereign Cloud Technical Whitepaper to understand the principles that should be leveraged to maintain a robust secure environment. Organizations that leverage these guidelines can expand these capabilities across the Software-Defined Data Center to include people, process, and technology controls. Each organization must tailor these principles and prioritize how they approach them.

VMWare Cloud Foundation

The VMware Cloud Foundation Security and Compliance Kit should be used to implement the customers defined security controls.

This kit includes the following documents that should be used to secure the environment and then also to audit the implementation on a regular basis.

Table 2. VMware Cloud Foundation Security & Compliance Documents

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Document Description</th>
<th>Intended Audience</th>
</tr>
</thead>
</table>
| Security and Compliance Configuration for VMware Cloud Foundation | User defined configurations can be performed post deployment of VMware Cloud Foundation for Standard Architecture. | System Integrator  
Cloud Administrator  
Infrastructure Administrator |
| VMware Cloud Foundation Audit Guide | Procedures to validate both default and user defined configurations with a preface composed by an independent, third-party auditor introducing the audit content and its applicability to control testing of a Software-Defined Data Center. | Security Professional Auditor |
VMware vSphere

The components of a vSphere environment are secured out of the box by several features such as authentication, authorization, a firewall on each ESXi host, and so on. You can modify the default setup in many ways. For example, you can set permissions on vCenter objects, open firewall ports, or change the default certificates. You can take security measures for different objects in the vCenter object hierarchy, for example, vCenter Server systems, ESXi hosts, virtual machines, and network and storage objects.

The guiding principles that are provided in the Securing the vSphere Environment document will help you ensure the proper security of your Sovereign Cloud.

VMware Cloud Director

Security threats to VMware Cloud Director can be broadly categorized as either internal threats that originate within the system and its tenants, or external threats that originate outside the system. This latter category includes threats to the infrastructure created to host a VMware Cloud Director server group and threats to the installed VMware Cloud Director software.

The VMware Cloud Director Security Guide provides details on how to provide data access control for your Sovereign Cloud.

VMware NSX-T Data Center

Due to the critical role NSX Data Center plays within an organization, configuration of the product along with secure topology will reduce the risk an organization may face. This document is intended to provide configuration information and topology recommendations to ensure a more secure deployment.

The NSX-T Data Center 3.1 Security Configuration Guide is essential for a secure Sovereign Cloud.

VMware vSAN

You can encrypt data-in-transit in your vSAN cluster and encrypt data-at-rest in your vSAN datastore. vSAN can encrypt data in transit across hosts in the vSAN cluster. Data-in-transit encryption protects data as it moves around the vSAN cluster. vSAN can encrypt data at rest in the vSAN datastore. Data-at-rest encryption protects data on storage devices in case a device is removed from the cluster.

Learn how to encrypt your vSAN environment using the Using Encryption in a vSAN Cluster document.

VMware Tanzu

vSphere with Tanzu leverages vSphere security features and provisions Tanzu Kubernetes clusters that are secure by default. vSphere with Tanzu is an add-on module to vSphere that can leverage the security features that are built into vCenter Server and ESXi.

Find more guidance on securing your Tanzu Basic components in the following guides:

vSphere with Tanzu Security

vSphere Security

Deploy a Confidential vSphere Pod

Using Pod Security Policies with Tanzu Kubernetes Clusters
Data and Environment Auditing

A key benefit of a VMware Sovereign Cloud is the ability to provide enhanced audit and compliance reporting, the output of which should be made available to customers on-demand and to official accreditors if this is a requirement in the jurisdiction. Security events such as suspected or attempted breaches should be reported to customers as well as the actions taken by the provider in response to those events. This not only provides openness to customers around the effectiveness of the provider’s security measures and procedures but enables them to adjust their own security strategies in response to what could be repeated and persistent attacks.

The VMware Cloud Provider Platform includes products that can assist in gathering audit information and provide continuous monitoring of the environment.

VMware vRealize Operations

VMware vRealize Operations (vROPS) is a monitoring and capacity analytics product that can be expanded to include compliance management packs that monitor metrics relevant to compliance in various industries. In addition to compliance monitoring, ongoing capacity and resource utilization monitoring and alerting, using these capabilities helps to prevent outages and service degradation by warning in advance of eventual capacity exhaustion. vROPS is a requirement of a VMware Sovereign Cloud.

Please see the vRealize Operations Configuration Guide for more information on this topic.

For Auditing of the environment please see the Auditing Users and the Environment using vRealize Operations Document.

VMware vRealize Log Insight

VMware vRealize Log Insight (vRLI) is a centralized logging product that collects, filters, and helps analyze log output from VMware products and syslog sources, helping to bring all diagnostics and audit data together in a central repository. It is a requirement of VMware Sovereign Cloud to implement vRLI and to configure all VMware components for use with it. This is especially important for components such as Cloud Director and NSX-T as one handles customer-facing self-service activities and the other handles network connectivity and security.

The configuration guide for a Secure vRealize Log Insight Environment is especially helpful in making sure your Sovereign Cloud has a secured environment for centralized logging.

VMware vRealize Network Insight

VMware vRealize Network Insight (vRNI) is used for performing network traffic pattern analysis and auditing on a one-off or continual basis. vRNI can identify traffic flows between both virtual and physical network nodes, build profiles of ‘normal’ activity and identify unusual or concerning network traffic.

For technical guidance on installation and configuration of vRNI please see the Using VMware vRealize Network Insight guide.

Using output from these products gives providers a rich and comprehensive source of detailed audit information that can be used to generate audit reports for specific customers and independent auditors.

Usage Metering

As a Cloud Provider, the act of collecting usage from your customers is what helps you determine which services and products are being used and how. In a VMware Sovereign Cloud, usage metering is essential as it gives you insight into which services are being used and which ones may need some extra marketing to your customers. Usage Metering also helps you as a Cloud Provider to know how much licensing may be needed for certain products. In a VMware Sovereign Cloud depending on the requirements of the sovereign entity defining the Cloud, the data that is sent back to VMware could compromise Sovereignty of the data. Therefore, when designing this feature of a VMware Sovereign Cloud you will need to consider if offline reporting is needed. vCloud Usage Meter is able to collect data offline so that only the appropriate data can be sent back to VMware.

vCloud Usage Meter

vCloud Usage Meter works in conjunction with vCloud Usage Insight, which is a service that aggregates the data collected from vCloud Usage Meter instances, and automatically pre-fills it into the Commerce Portal. To automatically report and
pre-fill your aggregated monthly product consumption data from vCloud Usage Meter into the Commerce Portal, you must register your vCloud Usage Meter instances with Commerce Portal.

For VMware Sovereign Cloud environments, it may be necessary to deploy vCloud Usage Meter in Offline Mode. Offline reporting is downloading the usage data from Usage Meter in raw format and then uploading it to Usage Insight manually. In this mode, there is no automatic data transfer from Usage Meter to Usage Insight. Please see the document entitled How to Deploy vCloud Usage Meter to learn more about how to switch Usage Meter to offline mode.

By downloading the usage data, providers can see what data has been collected by Usage Meter. They need to apply a script to unpack the downloaded raw data file to see the collected data in json format. This is valuable in a VMware Sovereign Cloud because it allows the provider to validate that the data being sent will not compromise the Sovereign Cloud Status. Please refer to the article How to Download Product Consumption for vCloud Usage Meter Running in Offline Mode to understand how to implement this feature and what you can expect to see when the data is downloaded. Providers can also refer to Usage Meter Data Privacy and Sharing Guidelines whitepaper to learn what data Usage Meter collects.

**Zero Trust Security Posture**

Micro-segmentation with zero-trust enforcement is a requirement of the Sovereign domain in a VMware Sovereign Cloud. This ensures that no workload can communicate with another workload without being explicitly allowed by a firewall rule. The Sovereign domain is the only domain that allows direct connectivity to external systems and is therefore an attack surface. zero-trust mitigates the risk of lateral attack in the unlikely event of a workload being compromised from outside.

The Resident domain of a Sovereign Cloud is isolated from the outside world, no inbound connections are possible thanks to two layers of edge firewall and a lack of routing to enable access from the outside world. When designing a VMware Sovereign Cloud, the outside world refers to any system or network that is not part of the platform itself where a total security equivalence cannot be assured. This includes the public internet but can also include the customer’s own on-premises networks and the service provider’s own internal systems and networks if these have not been secured physically and logically in equivalent ways. Overall application and data isolation is achieved by preventing unrelated applications from communicating with one-another in the Sovereign domain and access to data sources in the Resident domain being constrained only to the appropriate application.

**VMware NSX-T Data Center**

Using NSX-T in your Sovereign Cloud environment will satisfy the requirement for a Zero Trust Security posture as it protects the data in transit, and it also provides for micro/macro segmentation. Using the NSX-T Datacenter Distributed Firewall Documentation you will be able to understand how to install, configure, and manage segmentation for the applications in your VMware Sovereign Cloud.

![Figure 5. Illustrating a Zero Trust Implementation](image)
A VMware Sovereign Cloud Zero Trust Security Posture is based on developing five pillars of trust. These pillars are device trust, user trust, transport/session trust, application trust, and data trust. While Micro-segmentation is the only required configuration to achieve a Zero Trust Security Posture in the VMware Sovereign Cloud, there are other optional products that could be used to enhance your security in your environment.

The multi-layered approach includes adding security around the data and the application, making sure the transport or access is secure, and having a strong knowledge about the user and the device used to request access. Security checks at each layer enable you to extract audit logs and build analytics. And with logs and analytics, you can achieve automation and orchestration in which all applications and data are equally protected, and no users or devices are trusted by default.

Optional Additions for further Zero Trust Security
There are additional VMware products that can assist in implementing a Zero Trust Security posture beyond what is listed in the current Bill of Materials for a VMware Sovereign Cloud. These are listed below.

VMware SASE Platform (Secure Access Service Edge)
The Secure Access Service Edge (SASE) combines VMware SD-WAN Gateways, VMware Secure Access, our zero trust network access (ZTNA) solution, secure web gateway (SWG) and cloud security access broker (CASB) solutions, and VMware NSX Firewall, our next-gen firewall functionality—all delivered through VMware SASE points of presence (PoPs). These networking and security services can be delivered in an intrinsic or sequenced manner to branch edges, mobile users, campuses, and IoT devices.

![Figure 6. SASE Architecture](image-url)
Carbon Black EDR
Using Carbon Black EDR for Endpoint Security will help you to ensure a Zero Trust Security Posture from all your devices. Please use the Carbon Black User Guide to understand how to manage Carbon Black EDR, install sensors on endpoints, and using Carbon Black EDR to monitor file activity and threats on your endpoints.

![Figure 7. Illustration of the Carbon Black EDR Data Flow](image)

VMware Horizon
Using VMware Horizon in conjunction with Carbon Black Cloud you can publish Desktops and Applications that are very secure and is part of your Zero Trust security posture. The VMware Horizon Documentation will show you how to architect, install, and manage this part of your environment. It further describes how to create and deploy pools of desktops and applications that run on Microsoft Remote Desktop Services (RDS) hosts. It includes information about configuring policies, entitling users and groups, and configuring remote application features.

Workspace ONE
Using Workspace ONE will provide secure access to applications and workstations while maintaining your Zero Trust security posture. Using this VMware Workspace ONE Documentation you will learn how you can configure and manage a Workspace ONE digital workspace that includes the VMware Workspace ONE Intelligent Hub app for mobile devices and app management.

Encryption
Providers will need to use encryption to protect the data and communications that take place in a VMware Sovereign Cloud. To accomplish this, you will use both vSphere Virtual Machine Encryption, Storage Encryption, and Network Encryption to secure all workloads, data, and communications.

Data at-rest Encryption
Encrypting data at-rest can be achieved at the virtual machine and storage levels using virtual machine and vSAN encryption.

vSphere Virtual Machine Encryption
Encryption is applied to the virtual disk files attached to the virtual machine as well as the memory swap file and snapshots.

vSphere Encryption relies on a compliant KMS server to generate and manage keys, vCenter requests the private key for a virtual machine when it powers on the virtual machine and so the KMS becomes a critical dependency. Referencing the Virtual Machine Encryption documents will help direct you in implementing encryption for your sensitive workloads. You will need to consider which Key Provider is needed. Understanding the different components of Virtual Machine Encryption and how to implement it will also be covered.

vSAN Encryption
vSAN can perform data at rest encryption in your datastores. Encrypting your vSAN datastores in your Sovereign Cloud is a requirement. Data-at-rest encryption protects data on storage devices in case a device is removed from the cluster. The document called vSAN Data-At-Rest Encryption will help you to learn how Data-At-Rest Encryption works, design considerations, and how to manage it after the initial configuration.

Data in-flight Encryption

Data in motion, also referred to as data in transit or data in flight, is digital information that is in the process of being transported between locations either within or between computer systems. All data that goes over your internal network or the internet is potentially vulnerable. Encrypting data in-flight means that you encrypt data when it’s being transmitted over a network.

Data in motion includes the following scenarios: data moving from an Internet-capable endpoint device to a web-facing service in the cloud; data moving between virtual machines within and between cloud services and data that is traversing trusted private networks and an untrusted network such as the Internet. Once the data arrives at its destination, it becomes data-at-rest.

NSX-T Data Center Encryption

NSX-T Data Center provides the ability to encrypt data that is in transit between different sites/locations by using IPSec VPN. The Internet Protocol Security (IPSec) profiles provide information about the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IPSec tunnel. NSX-T Data Center provides system-generated IPSec profiles that are assigned by default when you configure an IPSec VPN or L2 VPN service.

To implement an IPSec VPN’s for your VMware Sovereign Cloud you can refer to the NSX-T Data Center VPN documentation. Here you will be able to confirm your knowledge on IPSec VPN’s, how to configure them, and how to manage the policies required to ensure the security of your data as it is traveling across your networks. Encrypting your data as it moves from point to point is a vital design consideration in a Sovereign Cloud. You will want to monitor and audit your encryption on a regular if not continual basis.

Catalog of Hardened and Trusted Images

Virtual workloads that are deployed or provisioned into a VMware Sovereign Cloud need to be trusted. This means that the configuration and purpose of all images used to provision virtual machines must be known and verified. There are many ways to secure a virtual machine in a way that acceptable to the customer or the Cloud Provider.

Implementing Operating System updates, applications installation, and virtual machine access all need to be handled in a way so as not to deviate from the Security Hardening Best Practices that have been implemented. These Best Practices need to be documented and updated on a regular basis. There also needs to be a process put in place that will allow for monitoring of these images against a set of defined standards to ensure the trust and security of provisioned workloads is maintained.

A separate audit should be performed on these images on a regular basis.

Please refer to the VMware vSphere Security Configuration Guide to perform security hardening of a virtual machine. In using this guide, you will find a spreadsheet that will provide you with a checklist of items that should be configured to provide the best possible security.

Please seek out the Microsoft Operating System Security site to secure your windows images. If you use a form of Linux or Unix operating systems, you will need to seek out the best practice guides for those operating systems.
VMware Tanzu Application Catalog (TAC)

VMware Tanzu Application Catalog is a service that combines content and tools to allow IT organizations to consume open source and commercial applications customized to their specific requirements, across multiple platforms. In a Sovereign Cloud this can be useful when decoupling the application and data from the underlying infrastructure. The Tanzu Application Catalog Documentation will show how to get started using the TAC to provide secure, tested, pre-built applications in a resilient way.

[Diagram of Tanzu Application Catalog Example]

**Figure 8. Tanzu Application Catalog Example**
VMware Cloud Director App Launchpad

App Launchpad is a VMware Cloud Director service extension which service providers can use to create and publish catalogs of deployment-ready applications. Tenant users can then deploy the applications with a single click. Using App Launchpad in your VMware Sovereign Cloud will help in providing tested, secure, and trusted images for provisioning.

As a service provider, you install App Launchpad in your data center. App Launchpad supports the use of applications from the Bitnami applications catalog that is available in the VMware Marketplace. You can also create catalogs of your custom, in-house applications and configure App Launchpad to work with these catalogs. Following the guidance in the VMware Cloud Director App Launchpad Documentation you will be able to install and configure the product in your datacenter. You will also be able to integrate with other catalogs you have already built.

![Figure 9. Architecture of App Launchpad](image)

Infrastructure isolation “air-gapped”

An air-gapped environment ensures that all the applications, networks, and resources in the environment are physically isolated from external inputs to prevent potential security risks.

In this context, if you need to operate with artifacts that are not within your network, you have to mirror them to the air-gapped environment so that your teams are able to consume them under secure conditions.

Data Access Controls

The whole purpose of a Sovereign Cloud is to protect the data that lives there. So, the design of how you will control the access to data that lives in your VMware Sovereign Cloud is one of the most important considerations you will have to make. You must limit personnel of those who operate the Sovereign Cloud to specific individuals or teams that meet the following requirements:

1. Have the applicable sovereign territory-specific security clearances for the applicable sovereign territory
2. Have full privilege access auditing and management.
Note: While external intrusion from unauthorized entities is a primary focus of the design, there is a real threat from internal entities that are acting with or without mal intent. Therefore, it is imperative to have a solid design in place that includes monitoring and auditing to prevent from losing control over your data.

There are different ways to control access to your data, Role-based Access Control and Attribute-based Access Control.

**Role-based Access Control (RBAC)**

Role-based Access Control (RBAC) is the most common model in which an entity’s ability to interact with systems, applications and data is prescribed by an assigned list of granular permissions allowing specific actions to be performed that are appropriate to the role of the authenticated entity.

The RBAC model is a foundation in the VMware Sovereign Cloud software stack. However, there are many other methods of authentication and authorization that protect access to the data that is being accessed. Below you will find a list of products that are part of the Bill of Materials for the VMware Sovereign Cloud and the references you will need to configure the RBAC in a way that maintains the security of the data in your environment.

**vSphere**

In vSphere, authentication and authorization govern access. vCenter Single Sign-On supports authentication, which means it determines whether a user can log in to vSphere components at all. Each user must also be authorized to view or manipulate vSphere objects.

vSphere supports several different authorization mechanisms, which is discussed in Understanding Authorization in vSphere. The focus of this document is how the vCenter Server permission model works and how to perform user management tasks.

Following vCenter Server Security Best Practices will help you ensure the integrity of your Sovereign Cloud. This document touches on general best practices for vCenter Server access, how to secure network connectivity, password requirements and lockout behavior, and other general security best practices for vCenter.

**Cloud Director**

A VMware Cloud Director tenant organization can contain an arbitrary number of users and groups. An Organization Administrator can create users locally or import them from an external directory service (LDAP) or identity provider (OAuth, SAML). Imported users can be members of one or more groups. A user that is a member of multiple groups gets assigned all the roles assigned to those groups. Each organization is created with a default set of rights and a set of predefined roles that include combinations of those rights. A System Administrator can grant additional rights to an organization, and organization administrators can use those rights to create custom roles that are local to the organization. Permissions within an organization are controlled through the assignment of rights and roles to users and groups.

No unauthenticated user is allowed to access any VMware Cloud Director functionality through the Web console, Tenant Portal, or VMware Cloud Director API. Each user authenticates using a username and password. You can configure password retry and account lockout policies globally and per organization.

The [VMware Cloud Director Security Guide](#) provides details on how to provide data access control for your Sovereign Cloud.

**NSX-T Data Center**

In NSX-T Data Center 3.1, you can log in to NSX Manager using a local user account, a user account managed by VMware Identity Manager (vIDM), or a user account managed by a directory service such as Active Directory over LDAP or OpenLDAP. You can also assign roles to user accounts managed by vIDM or a directory service to implement role-based access control.

Use this guide on [NSX-T Data Center 3.1 Authentication and Authorization](#) to secure your network environment. In this guide you will learn how to manage local user accounts, how to integrate with a VMware Identity manager or LDAP, and how to use RBAC to secure access.
VMware Tanzu Basic

As a vSphere administrator, you need privileges to configure a Supervisor Cluster and to manage namespaces. You define permissions on namespaces to determine which DevOps engineers can access them. As a DevOps engineer, you authenticate with the Supervisor Cluster by using your vCenter Single Sign-On credentials and can access only the namespaces for which you have permissions.

Find out more in the vSphere with Tanzu Authentication document understand how to manage permissions for your Tanzu environment and which authentication methods will be needed to manage the Kubernetes Clusters.

Attribute-based Access Control (ABAC)

Attribute-based access control (ABAC), also known as policy-based access control, defines an access control paradigm whereby access rights are granted to users using policies which combine attributes together. These policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action. This type of access control requires a 3rd party application which supports SAML 2.0 SSO.
Data Independence and Interoperability

The ability to provide a successful VMware Sovereign Cloud for your customers will rely on a balance of security, flexibility, reliability, and performance. The data that resides in the Sovereign Cloud needs to be able remain useful despite the advancement of the hardware and software that supports it. Therefore, the data needs to be able to interoperate with all other components in the Sovereign Cloud and it also needs to be able to remain independent of the underlying infrastructure.

Prevention of Cloud Vendor Lock-in

The ability to migrate workloads in and out of the VMware Sovereign Cloud prevents Cloud Vendor Lock-in. This is a scenario where a workload has been provisioned at one site and then due to incompatibility with any other supporting infrastructure is not unable to move out of its current location. This could result in the application/service being stuck and unable to take advantage of other useful features that another Cloud Provider may offer.

VMware Cloud Director Availability

Any VMware Cloud Director Availability version can migrate vSphere workloads to a private cloud site backed by VMware Cloud Director by using the native integrations with VMware Cloud Director and VMware vCenter Server®. [VMware Cloud Director Availability Documentation](#) shows how to use the Disaster Recovery-as-a-Service (DRaaS) solution. VMware Cloud Director Availability provides replication and failover capabilities for VMware Cloud Director™ and vCenter Server workloads both at the virtual machine and at the vApp level. You will be able to understand how to migrate workloads in and out of your Sovereign Cloud.

Application Portability and Independence

Application portability is the ability of an application to be portably installed, deployed, accessed, and managed – regardless of delivery model. The term defines an application’s flexibility when used on multiple platforms or instantly accessed from the Internet, a desktop or network. Data independence helps you to keep data separated from all programs that make use of it. You can use this stored data for computing and presentation. In many systems, data independence is an essential function for components of the system.

VMware Tanzu

VMware Tanzu provides a full stack of capabilities for modernizing your applications and infrastructure to continuously deliver better software to production. The VMware Tanzu portfolio simplifies multi-cloud operations and allows developers to easily access the resources they need to build modern applications.

VMware Tanzu allows you to containerize your workloads to run in the cloud, while increasing security and manageability. You can refactor existing software to be delivered continuously and resiliently. You run and manage your applications consistently everywhere, on a secure and scalable infrastructure with a conformant Kubernetes runtime. You can get VMware Tanzu either in the form of one of the VMware Tanzu Editions, or by selecting from the individual products to meet your requirements.

A VMware Sovereign Cloud utilizes VMware Tanzu Basic, VMware Tanzu Application Catalog, Data Management for VMware Tanzu (DMS), VMware Tanzu Greenplum (Tanzu Data Services), and VMware Cloud Director App Launchpad.
VMware Tanzu Basic
With VMware Tanzu Basic Edition you can embed Kubernetes in vSphere 7 or deploy your own management cluster on vSphere 6.7U3 or vSphere 7. Using the VMware Tanzu Basic Documentation, you will find out how to successfully install, configure, and manage K8’s on vSphere.

VMware Tanzu Application Catalog (TAC)
VMware Tanzu Application Catalog is a service that combines content and tools to allow IT organizations to consume open source and commercial applications customized to their specific requirements, across multiple platforms. In a Sovereign Cloud this can be useful when decoupling the application and data from the underlying infrastructure. The Tanzu Application Catalog Documentation will show how get started using the TAC to provide secure, tested, pre-built applications in a resilient way.
Data Management for VMware Tanzu (DMS)
Data Management for VMware Tanzu (DMS) is a VMware solution that offers a data-as-a-service toolkit for on-demand provisioning and automated management of PostgreSQL and MySQL databases on vSphere infrastructure. DMS provides both a graphical user interface and a REST API in the toolkit, enabling both administrators and developers to get the most out of the service. Please refer to the Data Management for VMware Tanzu Documentation to understand the following benefits:

• Data Management for VMware Tanzu simplifies management for administrators by operating as a fleet management tool; it provides a centralized view of an organization’s data service instances running on multi-cloud infrastructure.
• Database users can benefit from DMS’s self-service capabilities to create new data service instances, or to operate on existing instances safely and securely, without requiring infrastructure or database expertise.
• Data Management for VMware Tanzu also provides full automation for provisioning data service instances, backups, security patches, and periodic updates of the data service engine.

VMware Tanzu Greenplum (Tanzu Data Services)
Tanzu Greenplum is a massively parallel processing (MPP) database server that supports next generation data warehousing and large-scale analytics processing.

By automatically partitioning data and running parallel queries, it allows a cluster of servers to operate as a single database supercomputer performing tens or hundreds of times faster than a traditional database. It supports SQL, MapReduce parallel processing, and data volumes ranging from hundreds of gigabytes to hundreds of terabytes. Look at the VMware Tanzu Greenplum for Kubernetes Documentation to get a feel for installing, configuring, and managing this in your environment.
VMware Cloud Director App Launchpad

App Launchpad is a VMware Cloud Director service extension which service providers can use to create and publish catalogs of deployment-ready applications. Tenant users can then deploy the applications with a single click. Using App Launchpad in your VMware Sovereign Cloud will help with Data portability and independence.

As a service provider, you install App Launchpad in your data center. App Launchpad supports the use of applications from the Bitnami applications catalog that is available in the VMware Marketplace. You can also create catalogs of your custom, in-house applications and configure App Launchpad to work with these catalogs. Following the guidance in the VMware Cloud Director App Launchpad Documentation you will be able to install and configure the product in your datacenter. You will also be able to integrate with other catalogs you have already built.

Figure 12. Architecture of App Launchpad
Ability to support and manage hybrid cloud

The ability to provide a VMware Sovereign Cloud that is secure, flexible, and consistent, requires that customer the opportunity to move between on-premises environments and cloud-based environments. This of course means that all environments that exist in a Sovereign realm would need to be interoperable and trustworthy. Using VMware Cloud Director Availability allows for this functionality as it will provide the customer the ability to move between cloud environments and the on-premises environment that is being offered. A Cloud provider that is building a VMware Sovereign Cloud needs to design their environment to accommodate this.

VMware Cloud Director Availability

Any VMware Cloud Director Availability version can migrate vSphere workloads to a private cloud site backed byVMware Cloud Director by using the native integrations with VMware Cloud Director and VMware vCenter Server®. [VMware Cloud Director Availability Documentation](#) shows how to use the Disaster Recovery-as-a-Service (DRaaS) solution. VMware Cloud Director Availability provides replication and failover capabilities for VMware Cloud Director™ and vCenter Server workloads both at the virtual machine and at the vApp level. You will be able to understand how to migrate workloads in and out of your Sovereign Cloud. This includes migrating from a cloud site to on-premises and back out to the cloud site.

Next Steps

Operationalization

After a VMware Sovereign Cloud has been designed, implemented, and configured. It is now time to operationalize it in such a way that your customers can make use of it in a way that is beneficial to them. This means that as a Cloud Provider you will need to transform your normal business operations to accommodate the new secure Sovereign environment so that you can stay compliant with the architecture you just built.

Insert here the products that one can refer to which will help them to operationalize their environment.