VMware Cloud Foundation 9

Authentication & Authorization

Introduction & Best Practices

Bob Plankers (bob.plankers@broadcom.com)
Product Management & Marketing, VCF

October 31, 2025

vmware by Broadcom

These slides correspond to the
“Authentication and Authorization Best Practices in VCF 9”
video on the VCF YouTube Channel

https://www.youtube.com/@VMwareCloudFoundation

vmware by Broadcom

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only.

This document is not intended to provide advice and is provided “AS IS.”

Broadcom 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 requirements and effectiveness of implementations.

Based on a

TRUE STORY

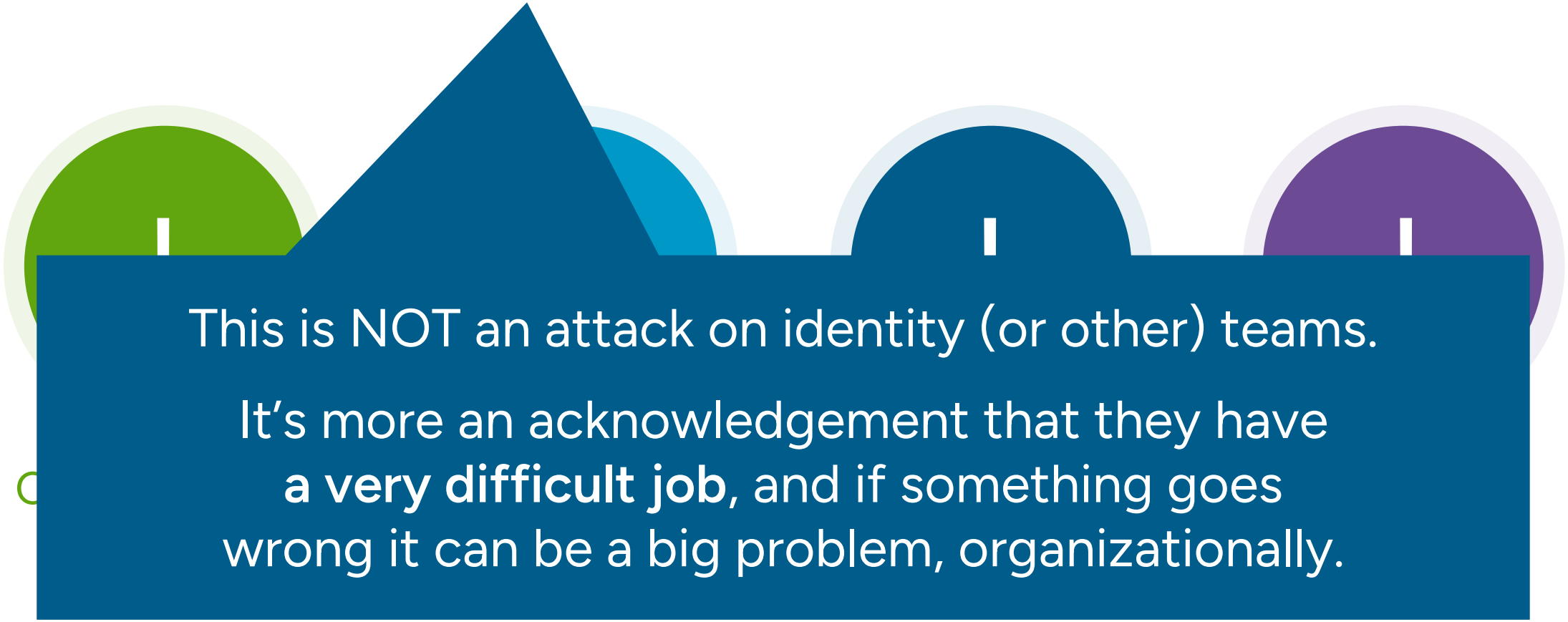
ZERO TRUST

Means **less trust**, not more trust.

vmware by Broadcom

Things Your Identity Provider Can Do To You

Immense Amounts of Trust Placed in Identity Providers



Things Your Identity Provider Can Do To You

Immense Amounts of Trust Placed in Identity Providers

Change Group Membership

Reset User Passwords

Disable MFA and Other Controls

Cover Their Tracks

Identity Providers Have To Trust a Lot of Things, Too

Organizations are Complicated

Provisioning, Monitoring, EDR Systems

Other People They Didn't Choose

Human Resources

Help Desk & Support Staff

Underlying Infrastructure (What?! :)

vmware by Broadcom

VCF Admins already have privileged access to **all organizational data**

vmware by Broadcom

IdP admins are implicit admins **of everything** in the organization

(so are backup admins, among others)

Insider Threat Mitigation

A holistic insider threat mitigation program combines physical security, personnel awareness, and information-centric principles.

Infrastructure is different because infrastructure is **more important**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. **Isolate from primary corporate/enterprise IdPs.**

Options for Isolating Authentication & Authorization

VMware Cloud Foundation Security & Compliance

Separate cloud IdP tenant?

Separate instance on-premises and clustered?

Separate on-premises instance per site?

Options for Isolating Authentication & Authorization

VMware Cloud Foundation Security & Compliance

Separate cloud IdP tenant?

Separate instance on-premises and clustered?

Separate on-premises instance per site?

Options for Isolating Authentication & Authorization

VMware Cloud Foundation Security & Compliance

This level of isolation only really useful if the rest of everything is independent, too.

?

Separate cloud IdP tenant?

Separate instance on-premises and clustered?

Separate on-premises instance per site?

Options for Isolating Authentication & Authorization

VMware Cloud Foundation Security & Compliance

This level of isolation only really useful if the rest of everything is independent, too.

May reach a point where even admins are going to start duplicating their passwords.

Remember: the password vault is an attackable trust relationship, too.

?

eparate on-emises instance per site?

“Reducing audit scope”

How Do You Reduce Trust?

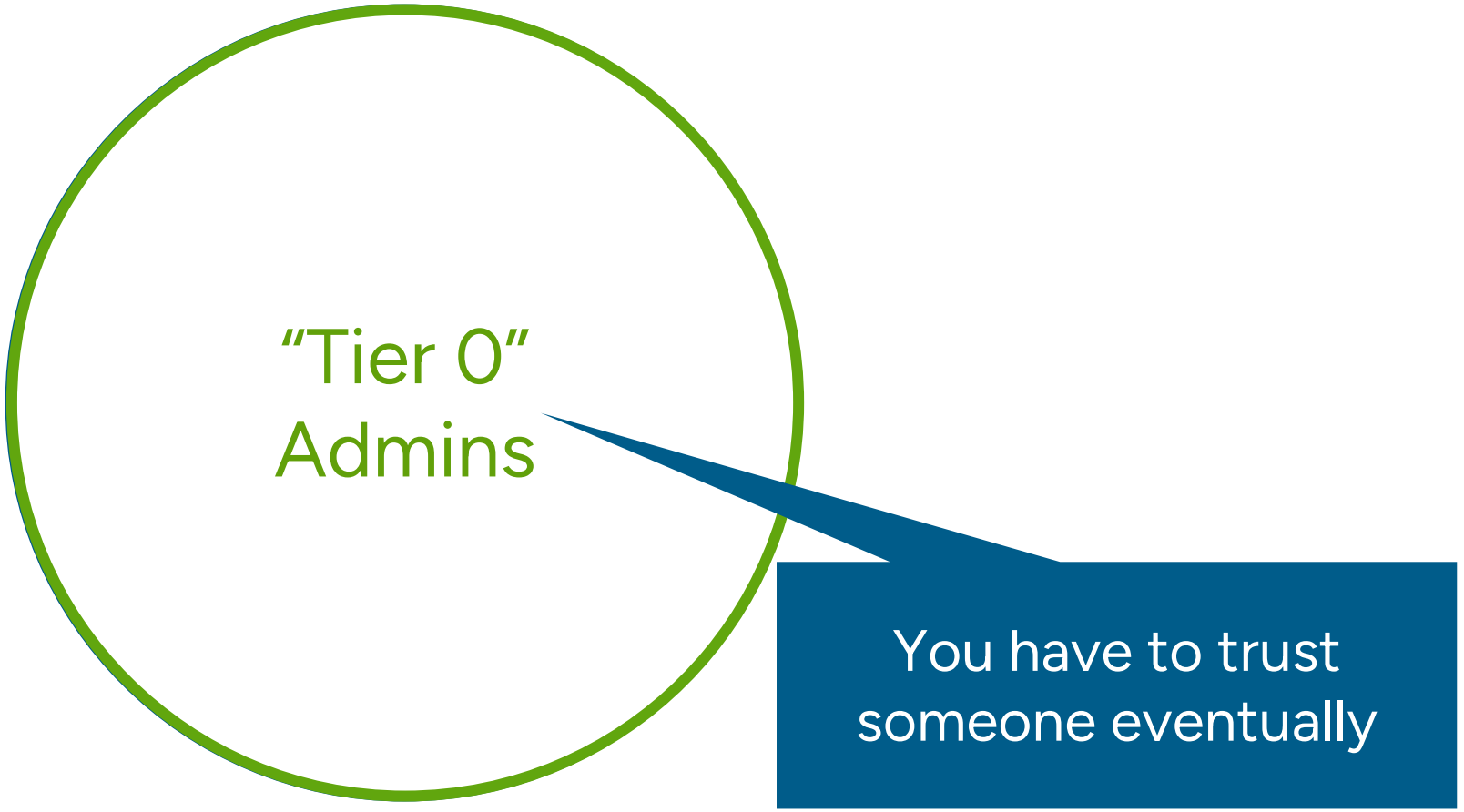
Reduce Overall Trust, Not Require More

How Do You Reduce Trust?

Reduce Overall Trust, Not Require More

How Do You Reduce Trust?

Reduce Overall Trust, Not Require More



Separation of Duties

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. **Isolate from primary corporate/enterprise IdPs.**

Starting to be mandated in regulations, such as the UK Telecommunications Security Code of Practice (M10.30, M11.19, M11.20)

Also called for in third-party defensive guidance for IT infrastructure (Mandiant et al)

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. **If reasonable, do authorization inside vSphere/VCF, not inside your IdP.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. **If reasonable, do authorization inside vSphere/VCF, not inside your IdP.**

Frankly, probably not worth it if you have an isolated IdP.

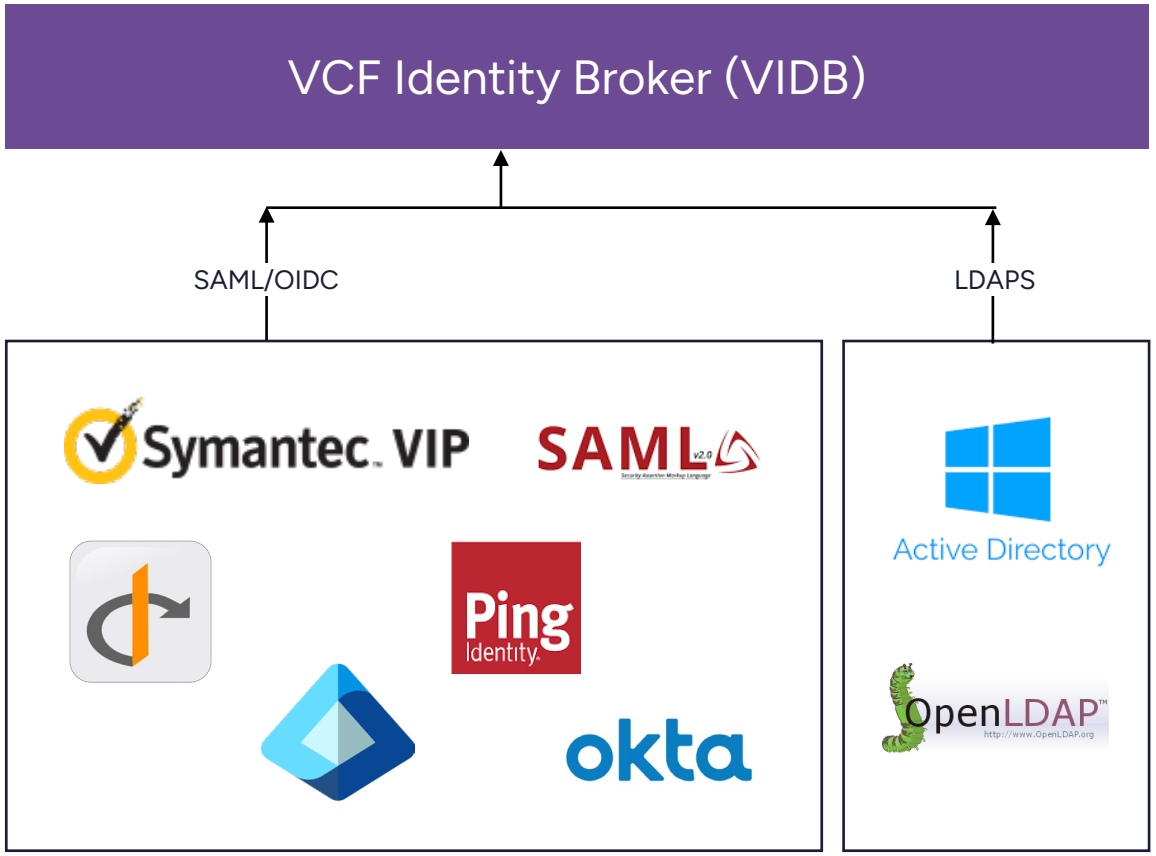
Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. **Use the Identity Broker (VIDB) to introduce MFA.**

Modern Identity Broker Simplifies Configuration

Single Sign-On for VCF Administrator Access Across VCF



Embedded (in vCenter), standalone, and clustered appliance deployment models

Automatic configuration for vCenter, NSX, Operations, and Automation

One IdP configuration for VCF management components, but Automation has multitenancy

Supports any SAML, OIDC, and AD/LDAPS-based IdP

Do not put your infrastructure on the Internet.

Use the cloud services' local proxies instead.

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. **Restrict access to vCenter & VCF Operations to only those who need it.**

Should you put vCenter in/on the same network as ESX management?

Should you put VCF Operations in/on the same network as ESX management?

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. **Restrict direct access to ESX. Drive access through vCenter & RBAC model.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. Restrict direct access to ESX. Drive access through vCenter & RBAC model.
6. **Restrict access to other connected infrastructure systems' management interfaces, too.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. Restrict direct access to ESX. Drive access through vCenter & RBAC model.
6. Restrict access to other connected infrastructure systems' management interfaces, too.
7. **Reduce permissions for service accounts to the minimum needed.**

Know Exactly What Permissions Were Used

vSphere Privilege Recorder

Docs / VMware vSphere / vSphere Security

Using Privilege Recorder

Add to Library | RSS | Download PDF | Feedback

Updated on 06/08/2023

In vSphere, privileges are fine-grained access controls that can be grouped into roles and map them to users or g
you identify the minimum set of privileges required to run a vCenter Server workflow.

To run a specific set of operations, it is very difficult to determine the minimal set of privileges that are required b
not have one-one mapping with the specific workflow which usually consists of multiple calls to different APIs op
object. As a result, the user either has more access or too little access to the environment. With the aim to keep t
privilege recorder feature helps you identify the minimum set of privileges required to run a vCenter Server work
and query the privileges that were checked while performing an operation. Privilege recorder is implemented usi

Note:

This feature is available as an API, and it supports only workflows run by a script. There is no UI suppo

Querying the ListAPI allows you to retrieve lists of privilege checks along with the corresponding sessions, users,
operation IDs (opIDs). You can use the appropriate filters to obtain privileges for a particular workflow.

For example, assume that user A needs to create a VM. Creating a VM requires a certain set of privileges. User A
from the system administrator. The system administrator can enable the privilege recorder and execute the creat
privilege check is performed, the data for the privileges that were checked during the Create VM operation is sto
PrivilegeID, sessionID, OpID, and so on. In this example, this system admin will use the filters to get privileges for
system administrator can now create a role with minimum required privileges and assign it to the user.

Enable Privilege Recorder using the vSphere Client

You can enable privilege recorder by using vSphere Client or adding the configuration to vpxd.cfg. [Read more]

Parent topic: vSphere Permissions and User Management Tasks

Developer Center

Overview | API Explorer | Code Capture

```
curl -X POST 'https://vcenter-1.8.fcotr.org/api/vcenter/authorization/privilege-checks?action=list' -H 'vmware-api-session-id: <valid-vapi-ses
```

Response

```
VcenterAuthorizationPrivilegeChecksListResult {
  "items": (Array<VcenterAuthorizationPrivilegeChecksInfo>, required)
  [
    VcenterAuthorizationPrivilegeChecksInfo {
      "object": (Object, required)
        VapiStdDynamicID (domain-c8) {
          "id": (string, required) "domain-c8",
          "type": (string, required) "vim.ClusterComputeResource",
        }
      "principal": (Object)
        VcenterAuthorizationPrivilegeChecksPrincipal (administrator) {
          "domain": (string, required) "vsphere.local",
          "name": (string, required) "administrator",
        }
      "privilege": (string, required) "System.Read"
```

vmware by Broadcom

vCenter will log the permission you are missing, so…

Create a role with no permissions, try the thing, then adjust the permissions. Repeat until done.

Remember that if it’s a backup system to try restores, too.

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. Restrict direct access to ESX. Drive access through vCenter & RBAC model.
6. Restrict access to other connected infrastructure systems' management interfaces, too.
7. Reduce permissions for service accounts to the minimum needed.
8. **Enable IdP advanced features like conditional access, geographic location, phishing-resistant MFA (number matching), and device hygiene.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. Restrict direct access to ESX. Drive access through vCenter & RBAC model
6. Restrict access to other connected infrastructure systems' management interfaces, too.
7. Reduce permissions for service accounts to the minimum needed.
8. Enable IdP advanced features like conditional access, geographic location, phishing-resistant MFA (number matching), and device hygiene.
9. **Ensure access logs are being retained in your IdP, for as long as possible/funded.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from primary corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use the Identity Broker (VIDB) to introduce MFA.
4. Restrict access to vCenter & VCF Operations to only those who need it.
5. Restrict direct access to ESX. Drive access through vCenter & RBAC model
6. Restrict access to other connected infrastructure systems' management interfaces, too.
7. Reduce permissions for service accounts to the minimum needed.
8. Enable IdP advanced features li… …g-resistant MFA (number matchi…
9. **Ensure access logs are being retained in your IdP, for as long as possible/funded.**

Initial breaches are often years earlier

vmware by Broadcom

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. **If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. **If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.**

Entra ID administrators have it enabled by default, even if you didn't turn SSPR on.

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. **If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.**

Entra ID administrators have it enabled by default, even if you didn't turn SSPR on.

It also does not follow your defined authentication method policies for admins, allowing email and SMS.

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. **Audit infrastructure IdPs against published best practices.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. **Lower authentication token lifetimes.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. **Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastructure components or IdPs (user provisioning systems, HR systems, automated password reset systems, configuration management systems, etc.).**

Authentication & Authorization Best Practices

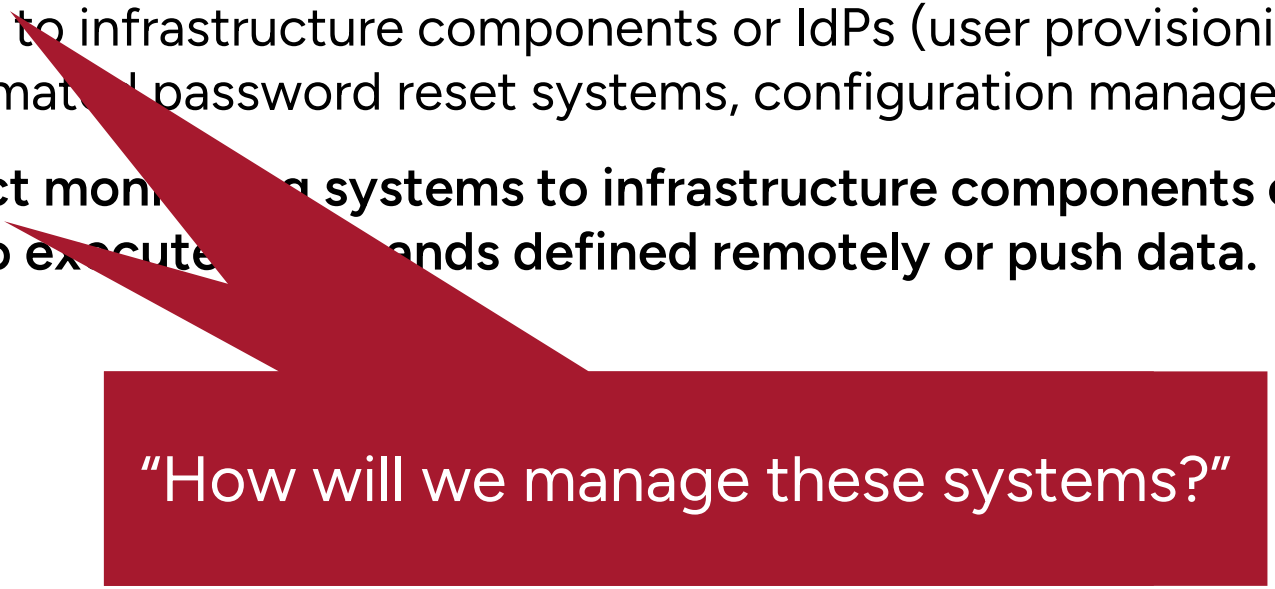
VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastructure components or IdPs (user provisioning systems, HR systems, automated password reset systems, configuration management systems, etc.).
14. **Do not connect monitoring systems to infrastructure components or IdPs in a manner that allows them to execute commands defined remotely or push data.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastructure components or IdPs (user provisioning systems, HR systems, automated password reset systems, configuration management systems, etc.).
14. **Do not connect monitoring systems to infrastructure components or IdPs in a manner that allows them to execute commands defined remotely or push data.**



vmware by Broadcom

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastructure components or IdPs (user provisioning systems, HR systems, automated password reset systems, configuration management systems, etc.).
14. Do not connect monitoring systems to infrastructure components or IdPs in a manner that allows them to execute commands defined remotely or push data.
15. **Do not allow staff outside the VCF administration team the ability to reset infrastructure administrator authenticators. Reset authenticators in person for privileged accounts.**

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastr tems, HR systems, automated pass ystems, etc.).
14. Do not connect monito n a manner that allows them to exec
15. **Do not allow staff outside the VCF administration team the ability to reset infrastructure administrator authenticators. Reset authenticators in person for privileged accounts.**

Attackers are also impersonating Help Desk staff. How would one of your users know it's the real Help Desk?

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastr tems, HR systems, automated pass ystems, etc.).
14. Do not connect monito n a manner that allows them to exec
15. **Do not allow sta y to reset infrastructure administrat privileged accounts.**

Attackers are also impersonating Help Desk staff. How would one of your users know it's the real Help Desk?

How does your answer change if you consider the attacker might have the same information your users do?

Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

10. If using Microsoft Entra ID, disable Seamless SSO. Disable SSPR for administrators.
11. Audit infrastructure IdPs against published best practices.
12. Lower authentication token lifetimes.
13. Do not connect systems which can alter accounts, passwords, or authentication configurations to infrastructure components or IdPs (user provisioning systems, HR systems, automated password reset systems, configuration management systems, etc.).
14. Do not connect monitoring systems to infrastructure components or IdPs in a manner that allows them to execute commands defined remotely or push data.
15. Do not allow staff outside the VCF administration team the ability to reset infrastructure administrator authenticators. Reset authenticators in person for privileged accounts.
16. **Consider carefully where you store “break glass” authentication information.**

Non-Technical Topics

When Implementing Change

Organizational Resistance

"Not how we do things around here."

"We've always done it this way."

"If it ain't broke don't fix it."

"We don't have staff or time for this."

"Why do you think you're special?"

Ownership

"Who maintains the infrastructure IdP?"

"Who is funding this?"

Exceptions

“What about app admins that need access?”

“Infosec will need admin rights.”

Just in case...

But I need the console...

What if...?

Someone will need to say no.

Just for now...

Have boot media...

“I don’t want to have to wake you up...”

vmware by Broadcom

Remember That They're Trying to Solve Problems, Too

"For security and compliance reasons we only grant access in limited cases."

Pre-Existing Written Policy

High-Level Risk Acceptance

VCF Automation

Remember That They're Trying to Solve Problems, Too

"For security and compliance reasons we only grant access in limited cases."

Pre-Existing Written Policy

Include access control as well as application standards to help avoid the need for this type of access.

Include a design review so technological solutions can be found.

Acceptance

Automation

Rememb roblems, Too

"For security in limited cases."

"Okay, fine, you can have access, but only if your VP accepts the risk, in writing, every X days."

1 Pre-Existing Written Policy

2 High-Level Risk Acceptance

3 VCF Automation

vmware by Broadcom

Rememb roblems, Too

"For security in limited cases."

"Okay, fine, you can have access, but only if your VP accepts the risk, in writing, every X days."

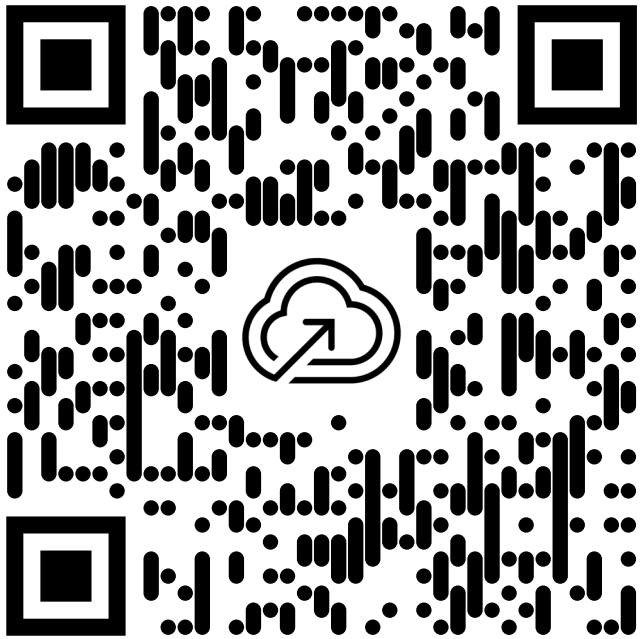
Remember That They're Trying to Solve Problems, Too

"For security and compliance reasons we only grant access in limited cases."

Security Hardening & Compliance Resources

https://brcm.tech/vcf-security

https://github.com/vmware/vcf-security-and-compliance-guidelines/



vmware by Broadcom

VMware Cloud Foundation 9

Thank You